УДК 343.982: 343.137.5 DOI: 10.37025/1992-4437/2022-38-2-36

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
Р. М. Кобець, *студент,*
Київський національний університет
ім. Тараса Шевченка, м. Київ
ORCID: https://orcid.org/0000-0002-9894-5541

ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ WI-FI РОУТЕРІВ ПІД ЧАС ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Мета статті полягає у висвітленні теоретико-прикладних підходів до правового забезпечення дій працівників слідчих та оперативних підрозділів під час виявлення та розслідування кримінальних правопорушень зі встановлення особи, яка перебувала на місці події, за допомогою технічних можливостей WI-FI роутера. ***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 WI-FI роутера. 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 у практику послідовності дій працівників слідчих та оперативних підрозділів під час виявлення та розслідування кримінальних правопорушень. ***Наукова новизна***. Запропоновано послідовність дій слідчо-оперативної групи зі встановлення особи, яка вчинила кримінальне правопорушення, якщо на місці події виявлено WI-FI роутер (комп'ютерну техніку), та обґрунтовано типові процесуальні стадії їх виконання. ***Висновки***. Розглянуто дії слідчо-оперативної групи зі встановлення особи, яка вчинила кримінальне правопорушення, якщо на місці події виявлено WI-FI роутер (комп'ютерну техніку), особливість яких полягає в необхідності використання спеціальних знань. Профіль і кваліфікація фахівця, якого необхідно залучити до огляду або тимчасового доступу до WI-FI роутера (комп'ютерної техніки), визначається залежно від мети і завдань слідчої (розшукової) дії, зважаючи на встановлені первинні дані про характер кримінального правопорушення. Проаналізовано підхід, який застосовується до поняття електронних доказів у кримінальному процесуальному та інших галузях національного процесуального права, із чого випливає, що скриншот, у контексті його використання в правовому полі, не оригінал документа, а лише форма відображення (копія, статичний файл зображення) електронного документа, який фіксується на цифровий носій, що засвідчується електронним підписом особи, яка його подає. Для наочного розгляду суб'єктами кримінального процесу відповідної інформації скриншот слід подавати в роздрукованому вигляді як паперову копію документа – електронний доказ, засвідчений підписом та із зазначенням дати. Надані науково-методичні рекомендації у процесі викладення основного матеріалу можуть становити методологічне підґрунтя ефективного виявлення та розслідування кримінальних правопорушень зазначеної спрямованості.

Ключові слова: кримінальне правопорушення; виявлення та розслідування кримінального правопорушення; слідчо-оперативна група; спеціальні знання; спеціаліст; протокол; WI-FI роутер; MAC-адреса; скриншот; девайс.

Вступ

Боротьба з кримінальною протиправністю (Ponomarenko, 2020; Novozhylov, 2021; Poluliashchenko, 2022) чи не найважливіший напрям діяльності держави, що зумовлює потребу постійно вдосконалювати роботу правоохоронних органів (Dudchenko, 2019; Voluiko, & Druchek, 2020; Filipenko, 2021; Solntseva, 2021). Водночас набуває ваги розроблення способів реалізації науково-технічних досягнень (Kloosterman, Mapes, Geradts, van Eijk, Koper, van den Berg, Verheij, van der Steen, & van Asten, 2015; Tymoshenko, Kozachenko, Kyslenko, Horodetska, Chubata, & Barhan, 2022) у боротьбі з кримінальною протиправністю (Yukhno, 2021), розширюючи можливості їх використання у запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні (Areshonkov, 2020; Teplytskyi, 2020). Разом із тим «використання спеціальних знань поряд із застосуванням сучасних науково-технічних пристроїв є неодмінною умовою

проведення огляду місця події. Їх використання потрібно не тільки у ході виявлення, фіксації та вилучення слідів, а й для загальної оцінки обстановки місця події, проведення попередніх досліджень на місці події, направлених на пояснення фактів виникнення певних слідів, місць їх розташування та часу виникнення тощо, що може свідчити про механізм події в цілому» (Pyrih, 2020).

Правові та криміналістичні основи фіксування криміналістично значущої інформації розробляли, зокрема, П. П. Артеменко, В. П. Бахін, В. Г. Гончаренко, А. В. Іщенко, О. В. Золотар, 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 доказів 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. Проте сьогодні бракує досліджень із проблематики виявлення на місці події електронних (цифрових) слідів, зокрема у WI-FI роутерів, для встановлення особи під час виявлення та розслідування кримінальних правопорушень, що й зумовлює актуальність обраної тематики, визначаючи подальші напрями наших розроблень.

Мета й завдання дослідження

Мета статті – висвітлити теоретико-прикладні підходи до правового забезпечення дій працівників слідчих та оперативних підрозділів під час виявлення та розслідування кримінальних правопорушень зі встановлення особи, яка перебувала на місці події, за допомогою технічних можливостей WI-FI роутера.

Для досягнення цієї мети потрібно вирішити такі завдання:

визначити особливості дій слідчо-оперативної групи зі встановлення особи, яка вчинила кримінальне правопорушення, якщо на місці події виявлено WI-FI роутер (комп'ютерну техніку);

проаналізувати підхід, який застосовується до поняття електронних доказів у кримінальному процесуальному й інших галузях національного процесуального права, розглянути питання використання скриншота у правовому полі як електронного документа;

надати відповідні науково-методичні рекомендації в контексті цього дослідження.

Виклад основного матеріалу

У разі виявлення факту кримінального правопорушення, наприклад у приватному чи багатоквартирному будинку, слідчо-оперативна група (далі – СОГ), що прибула на місце події, передусім здійснює першочергові заходи та невідкладні слідчі (розшукові) дії (*Ministerstvo vnutrishnikh sprav Ukrainy,* 2017, Lypen 07, Instruktsii z orhanizatsii vzaiemodii), серед них – огляд місця події, а саме огляд приміщень на наявність матеріальних слідів кримінального правопорушення, зокрема засобів, знарядь його вчинення, навколишніх предметів, вивчає матеріальну обстановку. Такі дії з пошуку слідів й інших речових доказів на місці події допоможуть встановити особу, що вчинила кримінальне правопорушення.

Але трапляється, що виявлені сліди не мають достатньої криміналістичної інформації для швидкої ідентифікації та встановлення особи, яка вчинила кримінальне правопорушення. Тому одним із допоміжних (альтернативних) способів убачається використання технічних можливостей WI-FI роутера в разі його виявлення під час огляду приміщень та його обстеження на місці події. Адже у WI-FI роутері можуть зберігатися електронні (цифрові, деякі фахівці їх ще називають віртуальними) сліди (Naidon, 2019; Hrebenkova, 2021b; Kalancha, & Harkusha, 2021; Tymoshenko, Kozachenko, Kyslenko, Horodetska, Chubata, & Barhan, 2022) пристрою (девайса), наприклад стільникового радіотелефону, якщо ним користувалась особа, яка вчинила кримінальне правопорушення. Тобто в WI-FI роутері передбачено технічну функцію, за допомогою якої в цьому пристрої автоматично зберігається MAC-адреса девайса, що підключався до нього. За цим електронним ідентифікатором можна в подальшому встановити особу, яка перебувала на місці події. Виявлені та задокументовані електронні (цифрові) сліди в WI-FI роутері за правильного їх процесуального оформлення набуватимуть статусу доказів.

Отже, пропонуємо розглянути версію, відповідно до якої під час огляду місця події члени групи СОГ висловили припущення, що особа, яка вчинила кримінальне правопорушення, тривалий час спілкувалась із потерпілим (у приміщенні виявили пляшки від алкоголю, недокурок, увімкнений WI-FI роутер тощо), а він, можливо, користувався роутером.

Якщо виявлено WI-FI роутер (комп'ютерну техніку), *дії слідчо-оперативної групи на місці події зі встановлення особи, яка вчинила кримінальне правопорушення, мають провадитись у такій послідовності.*

Насамперед для забезпечення збереження інформації на цьому пристрої слід вжити заходів, аби особи, які перебувають у цей час у приміщенні, його не торкалися, і щоб будь-хто не від'єднав пристрій від електричної мережі. Водночас не варто

до приїзду згідно з кримінальним процесуальним законодавством України (*Verkhovna Rada Ukrainy,* 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 71) спеціаліста в цій сфері (Nadizhko, 2020; Pyrih, 2020; Senchenko, & Yushchenko, 2021) проводити власними силами будь-які дії з роутером (комп'ютерною технікою).

Спеціаліст допоможе професійно розібратися в особливостях комп'ютерного обладнання і носіїв інформації, а також запобігти умисному або випадковому її знищенню, зазначить, яка інформація підлягає копіюванню. Профіль і кваліфікація фахівця, якого необхідно залучити до огляду та тимчасового доступу до WI-FI роутера (комп'ютерної техніки), визначається залежно від мети і завдань слідчої (розшукової) дії, зважаючи на первинні дані про характер кримінального правопорушення. У цьому випадку зазвичай залучають працівника Департаменту кіберполіції Національної поліції України (*Ministerstvo vnutrishnikh sprav Ukrainy*, 2017, Lypen 07, Instruktsii z orhanizatsii vzaiemodii, rozd. XV). Спеціалізовану пересувну лабораторію та працівників Експертної служби МВС України зазвичай залучають до огляду місця події (*Ministerstvo vnutrishnikh sprav Ukrainy*, 2017, Lypen 07, Instruktsii z orhanizatsii vzaiemodii, rozd. III, p. 14) за окремими видами вчинених кримінальних правопорушень (*Ministerstvo vnutrishnikh sprav Ukrainy*, 2015, Lystopad 03, Instruktsiia pro poriadok zaluchennia).

На початковій стадії проведення слідчих (розшукових) дій, таких як обшук, а також виїмка, огляд слідчому або оперативному працівнику у складі СОГ на місці події, якщо виявлено WI-FI роутер, необхідно:

1. Прибувши на місце проведення слідчої (розшукової) дії заборонити всім особам, що перебувають у приміщенні, у якому вчинено кримінальне правопорушення, торкатися до роутерів (комп'ютерної техніки), носіїв інформації, вмикати і вимикати пристрої й енергоживлення, інакше такі дії можуть розцінюватися як спроба знищити докази, що слід відобразити в протоколі огляду або тимчасового доступу.

2. Провести фото-, відеозйомку приміщення, у якому здійснюється огляд або тимчасовий доступ до комп'ютерного обладнання (роутера).

3. У процесі огляду або тимчасового доступу до роутера (комп'ютерної техніки) спеціаліст у присутності понятих має:

встановити та зафіксувати такі дані: вид роутера, його модель, адресу, S/N номер, MAC ID, пароль від WI-FI (Wirelless Password (WPS) або PIN, ім'я користувача та пароль (Username, Password). Ця інформація міститься на звороті роутера (див. рис. 1);

Рис. 1
Загальні дані роутерів різних моделей,
що містяться на їх звороті

здійснити вхід до інтерфейсу роутера. Для автентифікації входу до інтерфейсу роутера необхідно в пошуковій колонці ввести пароль: http://192.168.0.1 або http://192.168.1.1. За таким паролем можна зайти в інтерфейс роутера, використовуючи ноутбук, та здійснити візуальний огляд відображеної інформації на екрані комп'ютера з подальшим її фіксуванням. Далі вводиться ім'я користувача: admin і пароль: admin (див. рис. 2);

встановити MAC-адреси пристроїв, які підключались до роутера.

Дії зі встановлення MAC-адреси пристроїв, які підключались до роутера, розглянемо на прикладі інтерфейсу роутера на зразок ASUS RT-N10. Для цього:

1. Після введення пароля доступу до роутера на екран (дисплей) комп'ютера виводять загальну картинку інтерфейсу роутера та здійснюють огляд і фіксування відповідної інформації (див. рис. 3).

2. На екрані (дисплеї) комп'ютера, обираючи необхідну функцію управління роутером, вста-

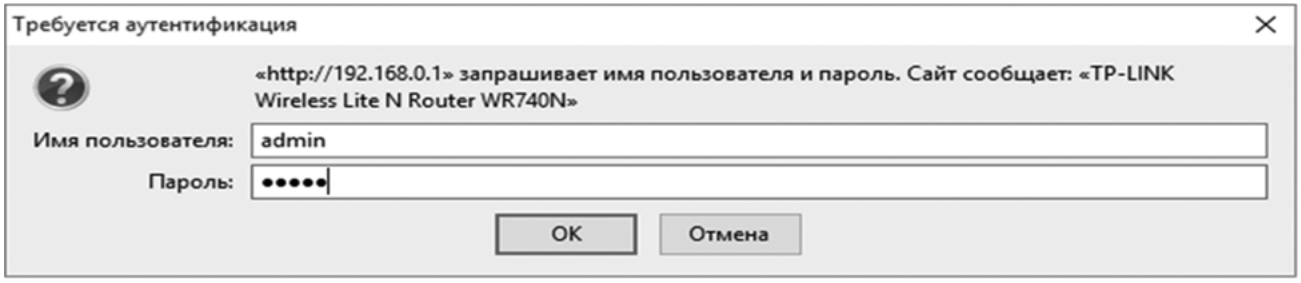

Рис. 2
Скриншот екрана (дисплея) комп'ютера з інформацією про введення пароля

Рис. 3
Скриншот екрана (дисплея) комп'ютера, на якому міститься інформація з роутера

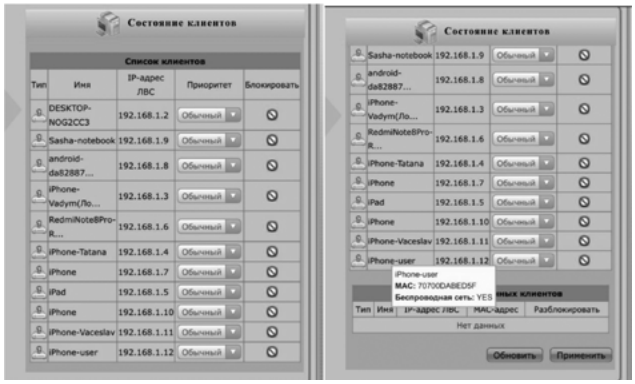

Рис. 4
Скриншот екрана (дисплея) комп'ютера зі списком користувачів, які підключались до роутера

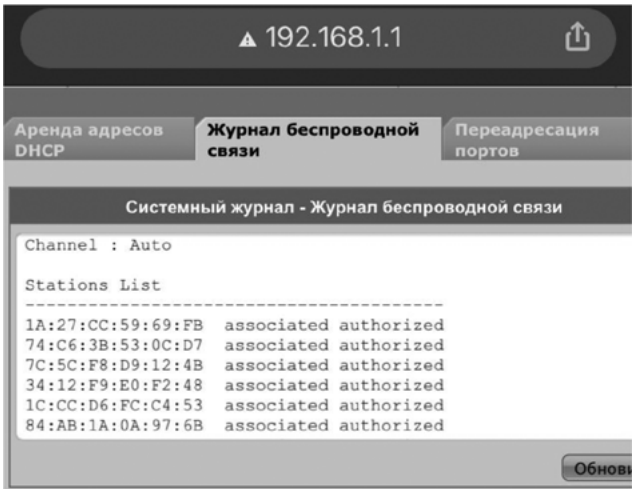

Рис. 5
Скриншот екрана (дисплея) комп'ютера із системним журналом, у якому міститься інформація про MAC-адреси девайсів, що підключалися до роутера

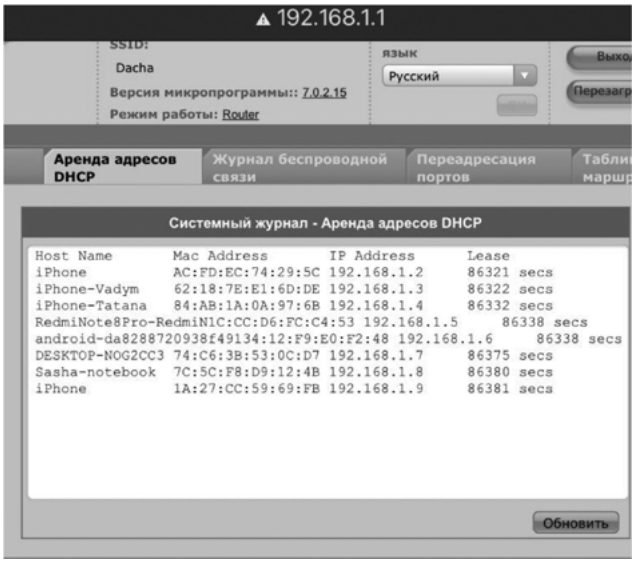

Рис. 6
Скриншот екрана (дисплея) комп'ютера із системним журналом, у якому міститься інформація про дату та час підключення користувача до мережі

новлюють і фіксують MAC-адреси девайсів, які підключались до цього пристрою (див. рис. 4 і 5).

3. Виявлені MAC-адреси вивчають і аналізують. Визначають невідомі MAC-адреси, що не належать встановленим особам (користувачам).

Залежно від виробника роутера визначають дату, час підключення невідомого користувача до мережі, а також часовий проміжок його підключення (див. рис. 6).

На завершальній стадії огляду або тимчасового доступу до роутера (комп'ютерної техніки) необхідно:

1. Визначити за допомогою спеціаліста з огляду на використання комп'ютера як засобу вчинення кримінального правопорушення або джерела доказів (Hutsaliuk, & Antoniuk, 2020), де в роутері (комп'ютерній техніці) зберігається потрібна інформація, яка підлягає копіюванню.

2. Здійснити на місці події, зважаючи на те, що є багато моделей роутерів, які під час їх від'єднання від електричної мережі втрачають змінні дані,

у присутності понятих фіксування відповідної інформації. Для цього виведена на екран (дисплей) комп'ютера потрібна інформація з роутера має бути записана 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, що засвідчений електронним підписом особою, яка здійснює ці процесуальні дії, що прирівняний до власноручного підпису (*Verkhovna Rada Ukrainy*, 2017, Zhovten 05, Pro elektronni dovirchi posluhy, st. 18, ch. 4; *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).

3. Оформити протокол огляду або тимчасового доступу, у якому поетапно фіксують усі дії спеціаліста (рекомендується під його диктовку та у присутності понятих):

зазначають розміщення роутера, комп'ютерної техніки, їх взаємне розміщення і щодо навколишніх предметів;

описують зовнішній вигляд роутера, комп'ютерної техніки, порядок з'єднання різних вузлів і деталей між собою із зазначенням наявних особливостей (кольору, штампів, написів тощо);

записують серії та номери пристрою (пристроїв), інші ідентифікаційні ознаки;

описують процедуру копіювання інформації з роутера (комп'ютерної техніки);

заносять усі заяви присутніх під час огляду або тимчасового доступу, що стосуються технічних і процесуальних моментів слідчої (розшукової) дії, що проводиться.

До протоколу додають: схеми плану приміщень із приміткою, де був розміщений роутер; матеріали фото-, відеозйомки, що проводились під час слідчої (розшукової) дії; скриншоти з екрана (дисплея) комп'ютера, на якому відображені MAC-адреси девайсів, що підключались до роутера; цифровий носій інформації (диск), на якому зафіксовано скриншоти.

Протокол підписують слідчий та інші учасники слідчої (розшукової) дії (спеціалісти, поняті, особа, у якої проведено огляд та тимчасовий доступ), а також інші присутні (представники адміністрації, технічного персоналу), що мають стосунок до роботи комп'ютерної мережі (під час слідчої (розшукової) дії в службових приміщеннях).

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

4. У робочому приміщенні роздрукувати з цифрового носія інформації (диску) скриншоти виведених на екран (дисплей) комп'ютера MAC-адрес девайсів, які підключались до роутера за певний проміжок часу, що нас цікавить.

У контексті порушеної нами проблематики розглянемо питання використання скриншота (англ. *screenshot* – знімок екрана) – зображення (статичний файл зображення), яке відбиває те, що бачить користувач на екрані монітора комп'ютера, планшета, смартфона в конкретний момент часу), у правовому полі як електронного документа (Kozytska, 2020; Hrebenkova, 2021a; Siemko, & Krakhmalov, 2021).

Відповідно до норм кримінального процесуального законодавства України, документом (що являє собою спеціально створений із метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження – st. 99, ch. 1) можуть вважатись, зокрема: матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі комп'ютерні дані); складені в порядку, передбаченому КПК України, протоколи процесуальних дій та додатки до них, а також носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (st. 99, ch. 2). Водночас оригіналом документа є сам документ, а оригіналом електронного документа – його відображення, якому надається таке саме значення, як документа (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 99, ch. 3).

Нормами цивільного процесуального законодавства України поняття «електронні докази» витлумачено як «інформація в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, електронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), вебсайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатися, зокрема, на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет)» (st. 100, ch. 1). Разом із тим наголошено, що «учасники справи мають право подавати електронні докази в паперових копіях, посвідчених у порядку, передбаченому законом. Паперова копія електронного доказу не вважається письмовим доказом» (st. 100, ch. 3). До того ж зазначено:

«1. Суд оцінює докази за своїм внутрішнім переконанням, що ґрунтується на всебічному, повному, об'єктивному та безпосередньому дослідженні наявних у справі доказів.

2. Жодні докази не мають для суду заздалегідь встановленої сили. Суд оцінює належність, допустимість, достовірність кожного доказу окремо, а також достатність і взаємний зв'язок доказів у їх сукупності.

3. Суд надає оцінку як зібраним у справі доказам в цілому, так і кожному доказу (групі однотипних доказів), який міститься у справі, мотивує відхилення або врахування кожного доказу (групи доказів)» (*Verkhovna Rada Ukrainy*, 2004, Berezen 18, Tsyvilnyi protsesualnyi kodeks Ukrainy, st. 89, ch. 1–3).

Із зазначеного випливає, що скриншот, у контексті його використання в правовому полі, не оригінал документа, а лише форма відображення (копія, статичний файл зображення) електронного документа, який фіксується на цифровий носій, що засвідчується електронним підписом особи, яка його подає. Для наочного розгляду суб'єктами кримінального процесу відповідної інформації скриншот слід подавати в роздрукованому вигляді як паперову копію документа – електронний доказ, засвідчений підписом та із зазначенням дати.

Після оформлення протоколу на місці події провадять подальші слідчі (розшукові) дії зі встановлення місцезнаходження девайсів за їх MAC-адресою. Для цього (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 159, ch. 2, st. 162, ch. 1, p. 7) слідчий (оперативний працівник) готує клопотання, що його погоджує прокурор, про отримання тимчасового доступу до інформації (документів), які знаходяться в операторів і постачальників електронних комунікаційних послуг і містять інформацію про зв'язок, абонента, надання електронних комунікаційних послуг, зокрема й отримання послуг, їх тривалість, зміст, маршрути передавання тощо (трафіку), щоб отримати ухвалу слідчого судді суду першої інстанції. 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.

У разі визначення конкретного місця, дати, часу з'єднання технічного засобу (стільникового радіотелефону) з роутером провадять (*Verkhovna Rada Ukrainy*, 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, st. 268) таку негласну слідчу (розшукову) дію, як установлення місцезнаходження радіообладнання (радіоелектронного засобу), що може дати можливість установити місцезнаходження технічного засобу, який був підключений до мережі (роутера) у момент вчинення кримінального правопорушення. Порядок її проведення внормовано положеннями кримінального процесуального законодавства України (*Verkhovna Rada Ukrainy,* 2012, Kviten 13, Kryminalnyi protsesualnyi kodeks Ukrainy, hl. 21). Загальні засади та єдині вимоги до організації проведення негласних слідчих (розшукових) дій слідчими органів досудового розслідування або за їх дорученням чи дорученням прокурора уповноваженими оперативними підрозділами, а також використання їх результатів у кримінальному провадженні окреслено відповідною Інструкцією (*Heneralna prokuratura Ukrainy, Ministerstvo vnutrishnikh sprav Ukrainy, Sluzhba bezpeky Ukrainy, Administratsiia Derzhavnoi prykordonnoi sluzhby Ukrainy, Ministerstvo finansiv Ukrainy, Ministerstvo yustytsii Ukrainy,* 2012, Lystopad 16, Instruktsii pro orhanizatsiiu provedennia).

Наукова новизна

Запропоновано послідовність дій слідчо-оперативної групи зі встановлення особи, яка вчинила кримінальне правопорушення, якщо на місці події виявлено WI-FI роутер (комп'ютерну техніку), та обґрунтовано типові процесуальні стадії їх виконання.

Висновки

1. Розглянуто дії слідчо-оперативної групи зі встановлення особи, яка вчинила кримінальне правопорушення, якщо на місці події виявлено WI-FI роутер (комп'ютерну техніку), особливість яких полягає в необхідності використання спеціальних знань. Профіль і кваліфікація фахівця, якого необхідно залучити до огляду або тимчасового доступу до WI-FI роутера (комп'ютерної техніки), визначається залежно від мети і завдань слідчої (розшукової) дії, зважаючи на встановлені первинні дані про характер кримінального правопорушення.

2. Проаналізовано підхід, який застосовується до поняття електронних доказів у кримінальному процесуальному та інших галузях національного процесуального права, із чого випливає, що скриншот, у контексті його використання в правовому полі, не оригінал документа, а лише форма відображення (копія, статичний файл зображення) електронного документа, який фіксується на цифровий носій, що засвідчується електронним підписом особи, яка його подає. Для наочного

розгляду суб'єктами кримінального процесу відповідної інформації скриншот слід подавати в роздрукованому вигляді як паперову копію документа – електронний доказ, засвідчений підписом та із зазначенням дати.

3. Надані науково-методичні рекомендації у процесі викладення основного матеріалу можуть становити методологічне підґрунтя ефективного виявлення та розслідування кримінальних правопорушень зазначеної спрямованості.

References

Areshonkov, V. V. (2020). Tekhnichne zabezpechennia tekhniko-kryminalistychnykh doslidzhen u rozsliduvanni zlochyniv [Technical safety of technical-forensic research in crime investigation]. *Aktualni problemy derzhavy i prava, 88*, 3–10 [in Ukrainian].
DOI: https://doi.org/10.32837/apdp.v0i88.3049

Dudchenko, O. (2019). Sutnist pravookhoronnoi systemy. *Pidpryiemnytstvo, hospodarstvo i pravo*, *8*, 144–149 [in Ukrainian].
DOI: https://doi.org/10.32849/2663-5313/2019.8.27

Filipenko, A. S. (2021). Dosvid orhanizatsii diialnosti pravookhoronnykh orhaniv v yevropeiskykh derzhavakh [Experience in organizing the activities of law enforcement agencies in European countries]. *Analitychno-porivnialne pravoznavstvo, 4*, 208–212 [in Ukrainian].
DOI: https://doi.org/10.24144/2788-6018.2021.04.36

Heneralna prokuratura Ukrainy, Ministerstvo vnutrishnikh sprav Ukrainy, Sluzhba bezpeky Ukrainy, Administratsiia Derzhavnoi prykordonnoi sluzhby Ukrainy, Ministerstvo finansiv Ukrainy, Ministerstvo yustytsii Ukrainy. (2012, Lystopad 16). *Instruktsii pro orhanizatsiiu provedennia nehlasnykh slidchykh (rozshukovykh) dii ta vykorystannia yikh rezultativ u kryminalnomu provadzhenni*: zatv. nakazom No 114/1042/516/1199/936/1687/5. https://zakon.rada.gov.ua/laws/show/v0114900-12#Text [in Ukrainian].

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. (2021a). Nalezhnist i dopustymist elektronnykh vidobrazhen yak dzherel dokaziv u kryminalnomu provadzhenni [Appropriateness and permissibility of electronic mapping as sources of evidence in criminal proceedings]. *Yurydychnyi naukovyi elektronnyi zhurnal, 12*, 335–338 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2021-12/84

Hrebenkova, M. S (2021b). 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

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

Kalancha, I. H., & Harkusha, A. M. (2021). Kopiia elektronnoi informatsii yak dokaz u kryminalnomu provadzhenni: protsesualnyi ta tekhnichnyi aspekty [Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects]. *Yurydychnyi naukovyi elektronnyi zhurnal, 8*, 336–339 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2021-8/77

Kloosterman, A., Mapes, A., Geradts, Z., van Eijk, E., Koper, C., van den Berg, J., Verheij, S., van der Steen, M., & van Asten, A. (2015). The interface between forensic science and technology: how technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system. *Philosophical transactions of the Royal Society of London. Series B, Biological sciences, 370*(1674), 20140264.
DOI: https://doi.org/10.1098/rstb.2014.0264

Kozytska, O. H (2020). Shchodo poniattia elektronnykh dokaziv u kryminalnomu provadzhenni [On The concept of electronic evidence in criminal proceedings]. *Yurydychnyi naukovyi elektronnyi zhurnal, 8*, 418–421 [in Ukrainian].
DOI: https://doi.org/10.32782/2524-0374/2020-8/103

Ministerstvo vnutrishnikh sprav Ukrainy. (2015, Lystopad 03). *Instruktsiia pro poriadok zaluchennia pratsivnykiv orhaniv dosudovoho rozsliduvannia politsii ta Ekspertnoi sluzhby Ministerstva vnutrishnikh sprav Ukrainy yak spetsialistiv dlia uchasti v provedenni ohliadu mistsia podii*: zatv. nakazom No 1339. https://zakon.rada.gov.ua/laws/show/z1392-15#Text [in Ukrainian].

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].

Nadizhko, M. M. (2020). Vykorystannia spetsialnykh znan u sudovo-ekspertnii diialnosti: teoretyko-pravovi aspekty [Use of specific knowledge in forensic activity: theoretical and legal aspects]. *Kryminalistychnyi visnyk, 33*(1), 25–36 [in Ukrainian].
DOI: https://doi.org/10.37025/1992-4437/2020-33-1-25

Naidon, Ya. (2019). Poniattia ta klasyfikatsiia virtualnykh slidiv kiberzlochyniv [Concept and classification of virtual traces of cybercrime]. *Pidpryiemnytstvo, hospodarstvo i pravo, 5*, 304–307 [in Ukrainian].
DOI: https://doi.org/10.32849/2663-5313/2019.5.56

Novozhylov, V. S. (2021). Zakhyst vid kryminalnykh pravoporushen yak zavdannia kryminalnoho provadzhennia [Protection from criminal offences as the objective of criminal procedure]. *Electronic Kyiv-Mohyla Academy Institutional Repository, 8*, 42–53 [in Ukrainian].
DOI: https://doi.org/10.18523/2617-2607.2021.8.42-53

Poluliashchenko, M. V. (2022). Vidpovidnist kryminalno-pravovoi normy pro vtiahnennia nepovnolitnikh u protypravnu diialnist faktoram kryminalizatsii [Compliance with criminal law on involvementof minors in illegal activity factorsof criminalization]. *Visnyk Luhanskoho derzhavnoho universytetu vnutrishnikh sprav imeni E. O. Didorenka, 1*(97), 123–134 [in Ukrainian].
DOI: https://doi.org/10.33766/2524-0323.97.123-134

Ponomarenko, Yu. A. (2020). Shchodo zmistu protypravnosti yak oznaky kryminalnoho pravoporushennia [On the content of unlawfulness as a sign of a criminal offence]. *Pytannia borotby zi zlochynnistiu, 39*, 46–53 [in Ukrainian].
DOI: https://doi.org/10.31359/2079-6242-2020-39-46

Pyrih, I. V. (2020). Fiksatsiia rezultativ doslidnytskoi diialnosti spetsialistiv na mistsi podii [Fixing results of research activities of specialists at the scene of crime]. *Kryminalistyka i sudova ekspertyza, 65,* 220–229.
DOI: https://doi.org/10.33994/kndise.2020.65.21

Senchenko, N. M., & Yushchenko, M. S. (2021). Uchast eksperta u kryminalnomu provadzhenni [Expert participation in criminal proceedings]. *Analitychno-porivnialne pravoznavstvo, 3*, 227–231 [in Ukrainian].
DOI: https://doi.org/10.24144/2788-6018.2021.03.42

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: https://doi.org/10.20998/2227-6890.2021.1.07

Solntseva, Kh. V. (2021). Shliakhy zaprovadzhennia natsionalnoi kontseptsii intehrovanoi orhanizatsii politseiskoi diialnosti [Ways of implementation of the national concept of the integrated organization of police activity]. *Problemy zakonnosti, 155*, 146–165 [in Ukrainian].
DOI: https://doi.org/10.21564/2414-990X.155.243856

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. (2020). 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

Tymoshenko, Y. P., Kozachenko, O. I., Kyslenko, D. P., Horodetska, M. S., Chubata, M. V., & Barhan, S. S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga, 11*(51), 149–160 [in Ukrainian].
DOI: https://doi.org/10.34069/AI/2022.51.03.14

Verkhovna Rada Ukrainy. (2004, Berezen 18). *Tsyvilnyi protsesualnyi kodeks Ukrainy*: Zakon Ukrainy No 1618-IV. https://zakon.rada.gov.ua/laws/show/1618-15#Text [in Ukrainian].

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

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].

Voluiko, O., & Druchek, O. (2020). Poniattia pravookhoronnoi diialnosti ta pravookhoronnykh orhaniv u svitli kontseptsii natsionalnoi bezpeky Ukrainy [The term of law enforcement activities and law enforcement bodies in view of the Soncept of the National Security of Ukraine]. *Pidpryiemnytstvo, hospodarstvo i pravo, 10*, 95–100 [in Ukrainian].
DOI: https://doi.org/10.32849/2663-5313/2020.10.16

Yukhno, O. O. (2021). Kryminalistychne zabezpechennia diialnosti ustanov sudovykh ekspertyz ta orhaniv dosudovoho rozsliduvannia i diznannia u protydii zlochynnosti [Forensic support of the activities of forensic science institutions and pre-trial investigation and inquest bodies in counteraction to crime]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky, 23*(1), 61–74 [in Ukrainian].
DOI: https://doi.org/10.32353/khrife.1.2021.04

Список використаних джерел

Арешонков, В. В. (2020). Технічне забезпечення техніко-криміналістичних досліджень у розслідуванні злочинів [Technical safety of technical-forensic research in crime investigation]. *Актуальні проблеми держави і права, 88*, 3–10.
DOI: https://doi.org/10.32837/apdp.v0i88.3049

Дудченко, О. (2019). Сутність правоохоронної системи. *Підприємництво, господарство і право, 8*, 144–149.
DOI: https://doi.org/10.32849/2663-5313/2019.8.27

Філіпенко, А. С. (2021). Досвід організації діяльності правоохоронних органів в європейських державах [Experience in organizing the activities of law enforcement agencies in European countries]. *Аналітично-порівняльне правознавство, 4*, 208–212.
DOI: https://doi.org/10.24144/2788-6018.2021.04.36

Генеральна прокуратура України, Міністерство внутрішніх справ України, Служба безпеки України, Адміністрація Державної прикордонної служби України, Міністерство фінансів України, Міністерство юстиції України. (2012, Листопад 16). *Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні:* затв. наказом № 114/1042/516/1199/936/1687/5. https://zakon.rada.gov.ua/laws/show/v0114900-12#Text

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. (2021a). Належність і допустимість електронних відображень як джерел доказів у кримінальному провадженні [Appropriateness and permissibility of electronic mapping as sources of evidence in criminal proceedings]. *Юридичний науковий електронний журнал, 12*, 335–338.
DOI: https://doi.org/10.32782/2524-0374/2021-12/84

Гребенькова, М. С. (2021b). 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

Гуцалюк, М. В, & Антонюк, П. Є. (2020). Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні. *Криміналістичний вісник, 1*(33), 37–49.
DOI: https://doi.org/10.37025/1992-4437/2020-33-1-37

Каланча, І. Г., & Гаркуша, А. М. (2021). Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти [Copy of electronic information as evidence in criminal proceedings: procedural and technical aspects]. *Юридичний науковий електронний журнал, 8*, 336–339.
DOI: https://doi.org/10.32782/2524-0374/2021-8/77

Kloosterman, A., Mapes, A., Geradts, Z., van Eijk, E., Koper, C., van den Berg, J., Verheij, S., van der Steen, M., & van Asten, A. (2015). The interface between forensic science and technology: how technology could cause a paradigm shift in the role of forensic institutes in the criminal justice system. *Philosophical transactions of the Royal Society of London. Series B, Biological sciences, 370*(1674), 20140264.
DOI: https://doi.org/10.1098/rstb.2014.0264

Козицька, О. Г. (2020). Щодо поняття електронних доказів у кримінальному провадженні [On The concept of electronic evidence in criminal proceedings]. *Юридичний науковий електронний журнал, 8*, 418–421.
DOI: https://doi.org/10.32782/2524-0374/2020-8/103

Міністерство внутрішніх справ України. (2015, Листопад 03). *Інструкція про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події:* затв. наказом № 1339. https://zakon.rada.gov.ua/laws/show/z1392-15#Text

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

Надіжко, М. М. (2020). Використання спеціальних знань у судово-експертній діяльності: теоретико-правові аспекти [Use of specific knowledge in forensic activity: theoretical and legal aspects]. *Криміналістичний вісник, 33*(1), 25–36.
DOI: https://doi.org/10.37025/1992-4437/2020-33-1-25

Найдьон, Я. (2019). Поняття та класифікація віртуальних слідів кіберзлочинів [Concept and classification of virtual traces of cybercrime]. *Підприємництво, господарство і право, 5*, 304–307.
DOI: https://doi.org/10.32849/2663-5313/2019.5.56

Новожилов, В. С. (2021). Захист від кримінальних правопорушень як завдання кримінального провадження [Protection from criminal offences as the objective of criminal procedure]. *Electronic Kyiv-Mohyla Academy Institutional Repository, 8,* 42–53.
DOI: https://doi.org/10.18523/2617-2607.2021.8.42-53

Полулященко, М. В. (2022). Відповідність кримінально-правової норми про втягнення неповнолітніх у протиправну діяльність факторам криміналізації [Compliance with criminal law on involvementof minors in illegal activity factorsof criminalization]. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка, 1*(97), 123–134.
DOI: https://doi.org/10.33766/2524-0323.97.123-134

Пономаренко, Ю. А. (2020). Щодо змісту протиправності як ознаки кримінального правопорушення [On the content of unlawfulness as a sign of a criminal offence]. *Питання боротьби зі злочинністю, 39*, 46–53.
DOI: https://doi.org/10.31359/2079-6242-2020-39-46

Пиріг, І. В. (2020). Фіксація результатів дослідницької діяльності спеціалістів на місці події [Fixing results of research activities of specialists at the scene of crime]. *Криміналістика і судова експертиза, 65*, 220–229.
DOI: https://doi.org/10.33994/kndise.2020.65.21

Сенченко, Н. М., & Ющенко, М. С. (2021). Участь експерта у кримінальному провадженні [Expert participation in criminal proceedings]. *Аналітично-порівняльне правознавство, 3*, 227–231.
DOI: https://doi.org/10.24144/2788-6018.2021.03.42

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: https://doi.org/10.20998/2227-6890.2021.1.07

Солнцева, Х. В. (2021). Шляхи запровадження національної концепції інтегрованої організації поліцейської діяльності [Ways of implementation of the national concept of the integrated organization of police activity]. *Проблеми законності, 155*, 146–165.
DOI: https://doi.org/10.21564/2414-990X.155.243856

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. (2020). 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

Tymoshenko, Y. P., Kozachenko, O. I., Kyslenko, D. P., Horodetska, M. S., Chubata, M. V., & Barhan, S. S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). *Amazonia Investiga, 11*(51), 149–160.
DOI: https://doi.org/10.34069/AI/2022.51.03.14

Верховна Рада України. (2004, Березень 18). *Цивільний процесуальний кодекс України:* Закон України № 1618-IV. https://zakon.rada.gov.ua/laws/show/1618-15#Text

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

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

Волуйко, О., & Дручек, О. (2020). Поняття правоохоронної діяльності та правоохоронних органів у світлі концепції національної безпеки України [The term of law enforcement activities and law enforcement bodies in view of the Concept of the National Security of Ukraine]. *Підприємництво, господарство і право, 10*, 95–100.
DOI: https://doi.org/10.32849/2663-5313/2020.10.16

Юхно, О. О. (2021). Криміналістичне забезпечення діяльності установ судових експертиз та органів досудового розслідування і дізнання у протидії злочинності [Forensic support of the activities of forensic science institutions and pre-trial investigation and inquest bodies in counteraction to crime]. *Теорія та практика судової експертизи і криміналістики, 23*(1), 61–74.
DOI: https://doi.org/10.32353/khrife.1.2021.04

Стаття надійшла до редакції 23.05.2022

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
R. Kobets, *Student,*
Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine
ORCID: https://orcid.org/0000-0002-9894-5541

USING WI-FI ROUTERS CAPABILITIES DETECTION AND INVESTIGATION OF CRIMINAL OFFENSES

The purpose of the article is to highlight the theoretical and practical approaches to the legal support of the actions of investigative and operative units during the detection and investigation of criminal offenses to identify the person who was at the scene using the technical capabilities of the WI-FI router. ***Methodology***. Given the specifics of the object and the 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 WI-FI router. 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 investigative and operative units during the detection and investigation of criminal offenses. ***Scientific novelty***. The sequence of actions of the investigative team to identify the person who committed a criminal offense, if a WI-FI router (computer equipment) is found at the scene, is proposed, and the typical procedural stages of their implementation are substantiated. ***Conclusions***. The actions of the investigative-operational group to identify the person who committed a criminal offense, if a WI-FI router (computer equipment) was found at the scene, the peculiarity of which is the need to use special knowledge, were considered. The profile and qualifications of the specialist who must be involved in the inspection or temporary access to the WI-FI router (computer equipment) is determined depending on the purpose and tasks of the investigative (search) action, taking into account the established primary data about the nature of the criminal offense. The approach applied to the concept of electronic evidence in criminal procedural and other branches of national procedural law is analyzed, from which it follows that a screenshot, in the context of its use in the legal field, is not an original document, but only a form of display (copy, static image file) of an electronic a document recorded on a digital medium certified by the electronic signature of the person submitting it. For a visual review by the subjects of the criminal process, the screenshot should be submitted in printed form as a paper copy of the document – electronic evidence, certified by a signature and with the date. 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.

Keywords: criminal offense; detection and investigation of a criminal offence; investigative and operational group; expertise; specialist; protocol; WI-FI router; MAC address; screenshot; device.

Н. В. Кобец, *кандидат юридических наук,*
старший научный сотрудник,
доцент кафедры оперативно-разыскной деятельности,
Национальная академия внутренних дел, г. Киев
ORCID: https://orcid.org/0000-0002-2233-0946
email: mv.kobets@ukr.net
Р. Н. Кобец, *студент,*
Киевский национальный университет
им. Тараса Шевченко, г. Киев
ORCID: https://orcid.org/0000-0002-9894-5541

ИСПОЛЬЗОВАНИЕ ВОЗМОЖНОСТЕЙ WI-FI РОУТЕРОВ ВО ВРЕМЯ ОБНАРУЖЕНИЯ И РАССЛЕДОВАНИЯ УГОЛОВНЫХ ПРАВОНАРУШЕНИЙ

Цель статьи заключается в освещении теоретико-прикладных подходов к правовому обеспечению действий сотрудников следственных и оперативных подразделений при выявлении и расследовании уголовных правонарушений по установлению находящегося на месте происшествия лица с помощью технических возможностей WI-FI роутера. ***Методология***. Исходя из специфики объекта и предмета исследования выбран методологический инструментарий. Методологическую основу составляет диалектический подход к анализу проблематики документирования и фиксирования на месте происшествия доказательств, учитывая возможности WI-FI роутера. При исследовании использована система методов научного познания: формальной логики (абстрагирование, логика, индукция, дедукция, синтез) – для выяснения содержания рассматриваемых вопросов; теоретический – в процессе исследования научной и учебно-методической литературы; моделирование – для разработки и внедрения в практику последовательности действий сотрудников следственных и оперативных подразделений при обнаружении и расследовании уголовных правонарушений. ***Научная новизна***. Предложена последовательность действий следственно-оперативной группы по установлению лица, совершившего уголовное правонарушение, если на месте происшествия обнаружен WI-FI роутер (компьютерная техника), и обоснованы типовые процессуальные стадии их выполнения. ***Выводы***. Рассмотрены действия следственно-оперативной группы по установлению лица, совершившего уголовное правонарушение, если на месте происшествия обнаружен WI-FI роутер (компьютерная техника), особенность которых заключается в необходимости использования специальных знаний. Профиль и квалификация специалиста, которого необходимо привлечь к осмотру или временному доступу к WI-FI роутеру (компьютерной технике), определяется в зависимости от целей и задач следственного (разыскного) действия, учитывая установленные первичные данные о характере уголовного преступления. Проанализирован подход, применяемый к понятию электронных доказательств в уголовном процессуальном и других отраслях национального процессуального права, из чего следует, что скриншот, в контексте его использования в правовом поле, не оригинал документа, а только форма отображения (копия, статический файл изображения) электронного документа, фиксируемого на цифровой носитель, удостоверяемый электронной подписью подающего его лица. Для наглядности рассмотрения субъектами уголовного процесса соответствующей информации скриншот следует представлять в распечатанном виде как бумажную копию документа – электронное доказательство, удостоверенное подписью и с указанием даты. Представленные научно-методические рекомендации в процессе изложения основного материала могут составлять методологическую основу эффективного выявления и расследования уголовных правонарушений соответствующей направленности.

Ключевые слова: уголовное правонарушение; выявление и расследование уголовного преступления; следственно-оперативная группа; специальные знания; специалист; протокол; WI-FI роутер; MAC-адрес; скриншот; девайс.