НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИВЧЕННЯ ПРОБЛЕМ
ЗЛОЧИННОСТІ ІМЕНІ АКАДЕМІКА В. В. СТАШИСА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ
Лабораторія «Використання сучасних досягнень науки і техніки
у боротьбі зі злочинністю»

# ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Матеріали міжнародного науково-практичного круглого столу,
присвяченого Всеукраїнському тижню права
м. Харків, 12 грудня 2022 року

*Електронне наукове видання*

Харків
«Право»
2022

DOI: https://doi.org/10.31359/978-966-998-460-9
УДК [343.1+343.98]:004(061)
В43



Рекомендовано до друку та поширення через мережу Інтернет вченою радою
Науково-дослідного інституту вивчення проблем злочинності
імені академіка В. В. Сташиса Національної академії правових наук України
*(протокол № 9 від 28 грудня 2022 року)*

**Використання** цифрової інформації в розслідуванні кримінальних правопо-
В43 рушень: матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), Г. К. Авдєєва, М. О. Соколенко. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Лаб. «Використання сучас. досягнень науки і техніки у боротьбі зі злочинністю». – Харків : Право, 2022. – 104 с. – DOI: https://doi.org/10.31359/978-966-998-460-9.
ISBN 978-966-998-460-9

Видання містить матеріали міжнародного науково-практичного круглого столу, на якому було розглянуто найбільш важливі сучасні проблеми цифровізації криміналістики, судової експертизи і кримінального процесу. Викладено матеріали обговорень таких наукових і практичних проблем: формування цифрової криміналістики та її роль у розслідуванні кримінальних правопорушень; впровадження інноваційних методів і застосування цифрових технологій у криміналістиці та судовій експертизі; цифрова інформація в розслідуванні кримінальних правопорушень; місце цифрових доказів у розслідуванні воєнних злочинів; проблеми використання цифрової інформації в кримінальному провадженні.

Для працівників органів правопорядку, науковців, викладачів, аспірантів і студентів юридичних навчальних закладів і широкого кола осіб, яких цікавлять сучасні проблеми криміналістики, кримінального процесу і судової експертизи.

**УДК [343.1+343.98]:004(061)**

*Організаційний комітет і редакційна колегія можуть не підтримувати позицію автора, проте ми поважаємо право кожного учасника конференції на висловлювання своїх ідей, критичних зауважень, інших суджень.*



ISBN 978-966-998-460-9

**ЗМІСТ**

# ВІТАЛЬНЕ СЛОВО ДИРЕКЦІЇ НДІ ВИВЧЕННЯ ПРОБЛЕМ ЗЛОЧИННОСТІ ІМЕНІ АКАДЕМІКА В. В. СТАШИСА НАПрН УКРАЇНИ УЧАСНИКАМ «КРУГЛОГО СТОЛУ»

**Владислава Батиргареєва,**
доктор юридичних наук, професор, директор Науково-дослідного інституту вивчення проблем злочинності ім. акад. В. В. Сташиса НАПрН України,
м. Харків, Україна

*Якби печерній людині показали наші технології, вона б прийняла це за магію. А якщо показати сучасній людині магію, вона прийме її за технологію.*
Компанія Red Barrels Studio

*Злочини, що не вдалося розкрити: чи можливо таке в майбутньому?*
В. Батиргареєва

Я вітаю учасників «круглого столу» з одного із центрів активного супротиву ворогу – з міста-героя Харкова. Тема війни і тема цифри сьогодні є визначальними темами нашого суспільства. Ще деякий час тому соціальними робінзонами нас хотів зробити COVID-19, ізолювавши людей в їх оселях. Сьогодні ж розв'язана РФ загарбницька війна хоче зробити з нас вигнанців, примушуючи залишати власні домівки, власну країну. У такій обстановці нам важливо зберегти соціально корисні зв'язки, перелаштувати всі сфери життєдіяльності суспільства у відповідності до викликів і небезпек, що нас оточують щодня. Зберегти основний контекст суспільних відносин та не випасти із фрейму соціалізації нам якраз і допомагає цифрова трансформація матриці соціальності, якою охоплено всі сфери життя та діяльності людини. Отже, науково-технічний прогрес в «особі» цифрової трансформації, без перебільшення, можна вважати оболонкою буття сучасної людини.

Ще на зорі розвитку епохи телеграфу і телефону всесвітньовідомий винахідник Томас Едісон зазначив, що первинною умовою прогресу людства є незадоволеність. Вочевидь, й інноваціям у сфері протидії зло-

чинності сприяє саме невдоволеність станом боротьби з цим ганебним явищем. Це природно викликає прагнення всіляко підсилити заходи із запобігання злочинам та бажання підвищити ефективність їх розслідування, адже у такий спосіб можна значно оптимізувати роботу органів кримінальної юстиції, тим самим забезпечивши невідворотність притягнення злочинців до кримінальної відповідальності та їх покарання.

Засновник кібернетики та теорії штучного інтелекту Норберт Вінер якось сказав, що ми змінили своє оточення настільки радикально, що тепер маємо змінювати себе, щоб жити в цьому новому оточенні. Дійсно, в інформаційному суспільстві як постіндустріальній фазі розвитку цивілізації головними продуктами виробництва стають інформація та знання. І цей факт накладає свій відбиток на одвічне протистояння прогресу і хаосу за вектором «злочинність-суспільство». Тому не втрачає й дотепер своєї актуальності запитання: «чи є ідеальні злочини або ж існують лише неідеальні засоби їх розкриття?» Якою б не була відповідь, можемо констатувати, що нові технології та методи, які можуть бути використані у протистоянні зі злочинністю, з'являються майже кожного дня. Сьогодні найважливішим напрямом оптимізації та підвищення ефективності слідчої, судової та експертної діяльності слід вважати комп'ютеризацію та можливості впровадження цифрових інформаційних технологій, що виявляються наслідком рушійного впливу глобалізації сучасного світу і новою главою в історії криміналістики. Важливість звернення до новинок технічного прогресу у протидії злочинності підсилюється ще й тим, що остання в цьому плані «модернізується» швидше, ніж відповідні можливості органів кримінальної юстиції. Фактично на розв'язання цієї проблеми ще понад 20 років тому наголошувалося у Законі України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 р.: «У сфері правоохоронної діяльності якісно нова організація специфічних режимів зберігання та оброблення інформації, зв'язок з міжнародними правоохоронними органами забезпечать реалізацію активної, наступальної стратегії в боротьбі з правопорушеннями, корупцією, організованою злочинністю, застосування нових інформаційних технологій у розкритті злочинів». Однак, повторимося, для органів кримінальної юстиції й досі залишається актуальною проблема використання новітніх технологій з метою виявлення, фіксації та збереження криміналістично значущої інформації (припустимо, за допомогою фотозйомки, аудіо- або відеозапису), висування версій, планування й організації розслідування злочинів,

дистанційного провадження слідчих (розшукових) дій, ведення електронного документообігу, функціонування криміналістичних обліків, користування законодавчою базою й іншими базами даних, автоматизованого пошуку відомостей щодо різних об'єктів, включаючи й інтегровані банки даних та ін.

Водночас останніми роками фахівці в галузі боротьби зі злочинністю працюють над розв'язанням завдання щодо запровадження електронних доказів у кримінальному процесі як самостійного процесуального джерела. І є дуже непростою справою визнати за цифровою інформацією самостійне доказове значення. До того ж постійно точаться суперечки з проводу необхідності дотримання балансу між входженням до орбіти кримінального процесу цифрових об'єктів як процесуальних доказів та непорушністю права особи на privacy. У зв'язку з цим конче потрібною у кримінальному процесі є сувора регламентація процедури проведення, припустимо, обшуків, пов'язаних із доступом до інформації, котра міститься на електронних носіях. Напевно, вже настав час введення до контексту кримінального процесу поняття «обшук цифрового пристрою», що стане новою сторінкою і в історії криміналістичної науки.

Важливо відзначити, що діяльність Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України так само пов'язана з розробкою інноваційних методів у справі боротьби зі злочинністю. Так, фахівцями нашої криміналістичної лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю», що розпочала свою роботу ще у вересні 1995 р., розроблено, зокрема, автоматизоване робоче місце слідчого «Інсайт», інформаційно-пошуковий модуль АІПС «Кліше», методика ідентифікації людини за параметрами мовних сигналів; алгоритми автоматизованої цифрової фотозйомки, цифрового відео- та звукозапису; алгоритми ідентифікації людини на основі біометричних ознак, автоматизовані інформаційні системи «Слідча практика», «Слідчий прецедент», «Профіль вбивці» та багато іншого. У зв'язку з цим проведення цьогорічного «круглого столу» під назвою «Використання цифрової інформації в розслідуванні кримінальних правопорушень» є важливим заходом для обміну знань та досвіду між науковцями та практичними працівниками. Отже, сподіваємося, що робота наукового форуму стане відчутним внеском у розв'язання такої злободенної потреби, якою є стабілізація у протидії злочинності, особливо в умовах запровадження у країні воєнного

стану. І в осяжному майбутньому ми зможемо з упевненістю констатувати, що не залишиться жодного злочину, який не вдасться розкрити…

Від імені колективу нашого Інституту бажаємо учасникам наукового заходу творчого натхнення, плодотворної дискусії, нових звершень та відчуття близької Перемоги !

# ПРОБЛЕМИ ВИКОРИСТАННЯ ЗАСОБІВ ЦИФРОВОЇ КРИМІНАЛІСТИКИ ПРИ РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

**Авдєєва Галина Костянтинівна,**
кандидат юридичних наук, старший науковий співробітник,
провідний науковий співробітник лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України,
м. Харків, Україна

У 70-х роках минулого сторіччя на тлі розвитку комп'ютерної техніки і інформаційних технологій зародився новий напрямок криміналістики – комп'ютерна криміналістика, завданнями якого було, в основному, збирання та дослідження слідів несанкціонованого проникнення до комп'ютерів, їх систем чи мереж без дозволу власника та вчинення дій, які змінюють чи припиняють режим їх роботи.

На початку 1990-х р. набули розвитку цифрові та мережеві технології і це докорінно змінило способи виявлення, вилучення і дослідження доказів, які мали вигляд цифрових слідів. Комп'ютерна криміналістика трансформувалася в цифрову, і на сьогодні вона охоплює роботу не лише з комп'ютерною інформацією, а й з будь-якою інформацією у цифровому вигляді, яка міститься не тільки на різноманітних цифрових пристроях та носіях цифрової інформації, а й у телекомунікаційних мережах. Цифрова криміналістика суттєво доповнює традиційні методи розслідування злочинів та, зокрема, дозволяє за допомогою супутникових знімків встановити місцезнаходження злочинців (таким чином було виявлено і ліквідовано ватажка терористичного угрупування «Аль-Каїда» Усама бен Ладена).

Важливість і актуальність розвитку цифрової криміналістики в усьому світі підтверджується тим, що у 2012 р. був навіть прийнятий спеціальний міжнародний стандарт ISO/IEC 27037:2012 [1], який містить настанови щодо роботи із цифровими доказами. Дотримуючись цього стандарту, журналісти-розслідувачі інтернет-видання Bellingcat на основі аналізу цифрової інформації (телефонних розмов, відеозаписів, супутникових знімків та ін.) встановили, що до авіакатастрофи с пасажирським Boeing-777 MH17 причетні військові РФ.

Сучасними завданнями цифрової криміналістики слугують пошук і аналіз цифрових слідів, аналіз даних (в т.ч. – метаданих[1]), збирання доказової інформації у цифровому середовищі. Найбільш складними і масштабними є завдання щодо пошуку у відкритому доступі та аналізу потенційних джерел доказів – величезної кількості загальнодоступних відео- та аудіо-записів, фото- та супутникових знімків, текстів, звітів, публікацій в соціальних мережах. Для допомоги у вирішенні таких складних завдань Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини у 2020 р. представлений Протокол Берклі (Практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права), який містить стандарти і методологічні підходи до «збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах». [2, с. 6]. Розробники Протоколу наголошують на важливості встановлення достовірності доказової інформації та забезпеченні її збереження.

У Протоколі Берклі викладені алгоритми пошуку, накопичення, аналізу та збереження цифрової інформації з відкритих джерел із дотриманням принципів об'єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини та ін. Автори Протоколу надають рекомендації щодо визначення меж вирішуваного завдання з метою економії часу та забезпечення особистої безпеки свідків і потерпілих, а також – для безпеки апаратного і програмного забезпечення.

З 24 лютого 2022 р. в Україні зафіксовано вже понад 40 тисяч воєнних злочинів, скоєних військовими РФ. [3]. Після звільнення раніше окупованих РФ територій України (частин Київської, Чернігівської, Сумської, Харківської, Херсонської та Луганської областей) виявлено значні руйнування цивільної інфраструктури, катівні зі слідами тортур, масові поховання цивільних осіб та військових зі слідами катувань, тіла закатованих громадян України та ін. Це свідчить про порушення військовими РФ прав громадян України, закріплених у Розділі І Європейської Конвенції про захист прав людини і основоположних свобод (ЄКПЛ) та її протоколах №№ 1, 4, 6, 7, 12 і 13. [4, с. 116]. Це, насамперед, право на життя (ст. 2 Конвенції); заборона катувань (ст. 3 Конвенції); заборона

[1] Метадані – це дані, що характеризують або пояснюють інші дані.

рабства (ст. 4 Конвенції); заборона дискримінації (ст. 14 Конвенції); право на власність (ст. 1 Протоколу № 1); право на освіту (ст. 2 Протоколу № 1); право на свободу і особисту недоторканність (ст. 5 Конвенції), право на справедливий суд (ст. 6 Конвенції); заборона покарання без закону (ст. 7 Конвенції); право на ефективний засіб правового захисту (ст. 13 Конвенції) та ін. [5].

Лідери багатьох країн світу закликали притягнути вище керівництво РФ до кримінальної відповідальності за воєнні злочини. Але через те, що на сьогодні ані Україна, ані РФ не ратифікували Римський статут, Міжнародний кримінальний суд (МКС) не зможе дати юридичну оцінку злочину агресії РФ проти України. Тому Україна ініціює створення спеціального міжнародного трибуналу для доведення вини кожного з представників військово-політичного керівництва РФ.

Докази військових злочинів накопичуються в спеціально створеному окремому онлайн-архіві. [6]. За допомогою американської системи розпізнавання осіб Clearview AI, яка використовує базу даних з 10 млрд фотопортретів (в т.ч. – з соціальних мереж), встановлено особи окремих злочинців-військових РФ за їх фотознімками та фотороботами. Незалежна міжнародна комісія з розслідування порушень в Україні також задокументувала випадки позасудових страт, незаконного позбавлення волі, катувань, жорстокого поводження, зґвалтувань та інших видів сексуального насильства, скоєних в районах, окупованих Збройними силами РФ, у чотирьох областях (Київській, Чернігівській, Харківській та Сумській) за період з 24 лютого та у березні 2022 р. [7].

У судочинстві країн ЄС, США та, зокрема, в Міжнародному кримінальному суді використання цифрових доказів регулюється правовими нормами, основою яких слугують принципи роботи з цифровими доказами, викладені у Протоколі Берклі та матеріалах Наукової робочої групи з цифрових доказів (SWGDE). [8]. В кримінальному процесуальному законодавстві України, на жаль, взагалі відсутнє визначення терміну «цифрові докази», не визначений порядок їх збирання, зберігання, аналізу та використання у кримінальному провадженні. Тому судами України вони іноді не визнаються допустимими доказами [9], а напрацювання у цьому напрямі науковців і юристів ЄС та США використовуються, в основному, журналістами-розслідувачами.

Успіх розслідування воєнних злочинів, скоєних військовими та військово-політичним керівництвом РФ, певною мірою залежить від ефектив-

ності використання цифрових доказів у кримінальному провадженні. Тому вкрай важливим є внесення змін і доповнень до кримінального процесуального законодавства України щодо визначення поняття «цифрові докази», регламентації процесів їх збирання, зберігання, фіксації, а також – визначення їх допустимості і достовірності.

**Список використаних джерел**


1. ISO/IEC 27037:2012 Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html

2. Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. Організація Об'єднаних Націй, 2020. Переклад. 119 с. С. 6. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

3. РФ скоїла в Україні понад 40 тисяч воєнних злочинів. Медіакомпанія DW. Bonn, Germany. URL: https://www.dw.com/uk/rf-skoila-v-ukraini-ponad-40-tisac-voennih-zlociniv-ofis-prezidenta/a-63103928?maca=ukr-rss-ukrnet-ukr-all-3816-xml

4. Сенаторова О. В. Права людини і збройні конфлікти: навчальний посібник. Київ: Видавництво «ФОП Голембовська О. О.», 2018. 208 с. С. 116.

5. The European Convention on Human Rights. Council of Europe. URL: https://www.coe.int/en/web/human-rights-convention

6. Russia's war crimes. URL: https://war.ukraine.ua/russia-war-crimes/

7. Звіт Незалежної міжнародної комісії з розслідування порушень в Україні. Генеральна Асамблея ООН. 18.10.2022. URL: https://www.ohchr.org/sites/default/files/2022–10/A-77–533-AUV-UA.pdf

8. Positions and Considerations of Scientific Working Group on Digital Evidence. URL: https://www.swgde.org/documents/positions-and-considerations

9. Судді Верховного Суду поділилися актуальною судовою практикою з питання доказування на підставі електронних доказів. Верховний суд України: офіційний сайт. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1155803/

# ЦИФРОВА ІНФОРМАЦІЯ В РОЗСЛІДУВАННІ ЗЛОЧИНІВ

**Булулуков Олег Юрійович,**
кандидат юридичних наук, доцент
кафедри криміналістики Національного юридичного університету
імені Ярослава Мудрого, м. Харків, Україна

**Коновалова Віолетта Омелянівна,**
доктор юридичних наук, професор, заслужений діяч науки України,
головний науковий співробітник «Використання сучасних досягнень
науки і техніки у боротьбі зі злочинністю» Науково-дослідного
інституту вивчення проблем злочинності імені академіка В. В. Сташиса
НАПрН України, дійсний член (академік) Національної академії
правових наук України,
м. Харків, Україна

У розслідуванні злочинів використання цифрової інформації набуває широкого застосування. Цей процес є природнім і обумовлений розвитком науково-технічного прогресу та новими способами вчинення злочинів. Використання злочинцями комп'ютерів, комп'ютерних програм, смартфонів та мережи інтернет призвело до виникнення низки питань, пов'язаних із використанням цифрової інформації як доказу вчинення злочину. Щодо зазначеної інформації в літературі існує думка, що «використання цифрових джерел доказової інформації залишається майже неврегульованим у національному кримінальному процесуальному законодавстві. Такий стан справ, безумовно, перешкоджає ефективному використанню сучасних технологій та джерел інформації» [1, с. 301]. Однак, не зважаючи на існуючи проблеми неврегульованості даного питання законодавством України, цифрова інформація все більше використовується в кримінальних провадженнях у якості доказу.

У процесі розслідування кримінальних проваджень встановлено, що «електронні пристрої (телефони, смартфони, комп'ютери, портативні пристрої геолокації (GPS, Glonass), цифрові фотоапарати, відеореєстратори, веб-камери, мережеві маршрутизатори, платіжні системи та інші цифрові пристрої все частіше використовуються злочинцями і, як наслідок, сліди неправомірних дій залишаються в інформаційному про-

сторі» [2, с. 169]. Зазначені цифрові сліди у вигляді цифрової інформації виявляють в процесі проведення слідчих (розшукових) дій щодо окремих носіїв такої інформації. На нашу думку використання цифрової інформації в розслідуванні може відбуватися у різний спосіб.

Так, під час розслідування окремих видів кримінальних правопорушень на слідчу ситуацію з метою її зміни здійснюється вплив засобами криміналістичної тактики. Зазначений вплив здійснюється шляхом прийняття та реалізації тактичних рішень різного виду. Вказане може сприяти отриманню доказової інформації при: а) визначенні джерел її отримання; б) подоланні протидії з боку зацікавлених осіб; в) наявності випадків її приховуванні; г) можливості її приховування надалі; д) виникненні певних труднощів при згадці і інтерпретації інформації у окремих осіб і ін. На прийняття рішень у вказаних ситуаціях впливає цифрова інформація, що сприяє вибору напряму тактичного впливу.

Як приклад розглянемо злочини, пов'язані із навмисним заподіянням шкоди здоров'ю людині.

Тактичні рішення при розслідуванні вказаних злочинів, формуються і отримують свою попередню структуру на етапі планування проведення слідчих (розшукових) дій. Саме на цьому етапі здійснюється аналіз ситуації та визначаються дії особи що здійснює розслідування. Під час аналізу встановлюється можливість отримання цифрової інформації, що може бути джерелом доказів причетності підозрюваного до вчинення злочину. Акцент на виявленні цифрової інформації робиться у зв'язку з її надійним способом фіксації на електронних носіях. І такими носіями можуть бути камери відеоспостереження, що знаходяться біля місця події, відеореєстратори автомобілів, відео з телефонів чи камер випадкових свідків і ін. У більшості випадків розслідування навмисного заподіяння шкоди здоров'ю починається з допиту потерпілого. Допит потерпілого здійснюється відразу після того, коли з'являється така можливість. При допиті потерпілого, що знаходиться у важкому стані, коли результат лікування невідомий, рекомендується застосовувати додатковий спосіб фіксації – відео або звукозапис з обов'язковою участю лікаря. Досить часто потерпілий при допиті намагається виправдати винну особу, заявляючи про заподіяння тілесних ушкоджень унаслідок своєї необережної поведінки. У таких випадках прийняття рішення щодо демонстрації відео отриманого з камер спостереження дозволить вплинути на допитуваного і отримати від нього правдиві свідчення. Використання цифро-

вої інформації при допиті може сприяти встановленню не тільки обставин заподіяння тілесних ушкоджень потерпілому, але відновити окремі деталі події про які потерпілий забув розповісти.

У контексті цифрової інформації важливе інформаційне навантаження мають і інші слідчі (розшукові) дії.

Так, після допиту потерпілого важливим є допит свідків події, до яких ми відносимо і медичний персонал, який надавав первинну допомогу потерпілому. Також важливим є огляд (обшук) носіїв цифрової інформації, якими у даному випадку можуть бути: смартфони, планшети, комп'ютери та відеорегістратори автомобілів. Отримана цифрова інформація може містити відомості щодо мотивів злочину та поведінки потерпілого і підозрюваного як до моменту вчинення злочину, так і після його вчинення.

У криміналістичній літературі існують різні точки зори з приводу можливості отримання цифрової інформації зі смартфонів та комп'ютерів що належать особам на праві власності. Мова йде про «процесуальні гарантії щодо захисту громадян від надмірної зацікавленості з боку правоохоронних органів під час проведення процесуальних дій» [3, с. 178]. На нашу думку доступ до особистого листування і іншої приватної інформації може бути набутим тільки в процесі обшуку. Іншим є питання отримання інформації із відкритих джерел. Йдеться про соціальні мережі де люди мають свої профілі і багато хто з них щодня публікує свій контент. Доступ до таких джерел відкритий і будь-хто може отримати інформацію, що є у відкритому доступі щодо окремої особи. Інформація з відкритих джерел може бути систематизована і використана в розслідуванні. Однак, «надання цифровим відомостям з відкритих джерел статусу доказу та перспективи їх використання у судовій залі детермінує особливі підходи до формування кінцевого звіту такої аналітичної діяльності, належної процесуальної фіксації та збереження даних» [4, с. 37].

Відповідно щодо цифрової інформації в розслідуванні злочинів, пов'язаних із навмисним заподіянням шкоди здоров'ю людині. така інформація відносно потерпілого і підозрюваного також може бути отримана з відкритих джерел. Характеристики вказаних осіб, виходячи з їх профілів в соціальних мережах, дають можливість визначити їх соціальний стан, звички, наміри, цілі, нарешті – створити їхні психологічні портрети. Все це буде сприяти встановленню взаємовідносин між ними (якщо

такі мали місце) та оцінці дій кожного з них. Інформація з відкритих джерел також допоможе встановити коло осіб, що можуть як свідки пояснити поведінку потерпілого і підозрюваного, дати пояснення щодо певної події.

Тактично правильно допит підозрюваного необхідно проводити після отримання та аналізу інформації щодо події злочину та інформації, що характеризує особу підозрюваного. Така інформація може міститися у показаннях потерпілого і свідків, у результатах огляду місця події, смартфона та комп'ютера підозрюваного (наприклад, щодо листування з потерпілим), а також в аналізі його профілю в соціальних мережах (цифрова інформація).

**Список використаних джерел**

1. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права.* 2016. № 1. С. 301–305.

2. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2017. № 1. (77). С. 168–175.

3. Метелев О. П. Збирання цифрової інформації як окремий спосіб отримання доказів під час кримінального провадження. *Науковий вісник Ужгородського національного університету. Серія ПРАВО.* 2020. Вип. 60. С. 177–180.

4. Дуфенюк О. Використання відкритих джерел цифрової інформації під час розслідування злочинів. *Інформація та документ у сучасному науковому дискурсі:* матеріали VII Всеукраїнської дистанційної науково-практичної конференції. (Івано-Франківськ, 20 травня 2022 р.). Івано-Франківськ: ІФНТУНГ, 2022. С. 37–41.

# ЩОДО ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ В КРИМІНАЛЬНОМУ ПРОВАДЖЕННЯ: ОКРЕМІ АСПЕКТИ

**Глинська Наталія Валеріївна,**
доктор юридичних наук, старший науковий співробітник, завідувачка відділом дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

Процес стрімкого впровадження інформаційних технологій у всі сфери соціального життя, що спостерігається в останні роки, запустило глобальний процес інформатизації суспільства, всеосяжний перехід до процесу створення, фіксування та передачі інформації в електронному просторі. Відповідно значну долю інформаційного сегменту сучасного кримінального провадження складає саме цифрова інформація, що обумовлює *необхідність формування якісно нового підходу до використання у доказуванні цифрових (електронних) доказів*. Водночас, як констатується сучасною науковою спільнотою та практиками, чинне кримінальне процесуальне законодавство містить лише загальні правила щодо застосування електронних доказів, залишаючи не врегульованими низку питань щодо специфіки порядку їх збирання та способів дослідження. Зазначене унеможливлює повноцінне оперування на практиці цифровою інформацією у процесі доказування обставин вчиненого кримінального правопорушення.

Необхідність не лише доктринального, а й нормативного вирішення питання щодо належного фіксування цифрової інформації сьогодні є вкрай актуальною в умовах об'єктивної потреби розслідування воєнних злочинів та оперування значним масивом інформації із відкритих джерел (як-то контент у соцмережах, відео-, фотоконтент, супутникові знімки, карти та інша онлайн-інформація) як доказами у відповідних провадженнях. Адже сьогодні у роботі органів досудового розслідування є певні складнощі щодо системного розуміння документування відповідної цифрової інформації із джерел відкритого доступу. Проблемність позначеного питання відмічена й суддями Верховного Суду. Так, за словами голови ККС ВС С. Кравченка, до проблемних питань використання електронних доказів належать, зокрема, «..можливість застосування моніторингу та користувацького пошуку в соціальних мережах, резуль-

тати зняття інформації з електронних інформаційних систем, правова оцінка скриншотів, співвідношення оригіналу доказу та його копії»[1].

Однією з «найпопулярніших» актуальних проблем у практиці використання цифрової інформації на підтвердження встановлених фактів є невизначеність щодо концептуального в контексті допустимості доказів питання стосовно співвідношення оригіналу джерела електронного доказу та його копії. Адже принципова відмінність середовищ існування паперових й електронних документів (аналогове та електронне) об'єктивно унеможливлюють застосування ідентичних критеріїв оригінальності таких різновидів документів та стандартів належної процедури їх копіювання. Відповідно за відсутності спеціального правового регулювання таких цифрових критеріїв та стандартів неоднозначним на практиці виявилось питання щодо допустимості використання в доказуванні скопійованої електронної інформації.

Адже з огляду на встановлені законом правила доказування, спрямовані на забезпечення правдивості фактичних даних, на яких може гарантуватися обвинувачення, процесуальним джерелом доказів, за загальним правилом, має бути оригінал документу (ч.3. ст.99 КПК). Оригіналом електронного документа закон визнає його *відображення*, якому надається таке ж значення, як документу. Отже оригіналом електронного документу закон визнає аналоговий документ, доступний для візуального сприйняття.

Втім таке нормативне формулювання на думку сучасних дослідників в контексті електронних документів є таким, що не відповідає природі носія цифрової інформації та не узгоджується із розумінням оригіналу електронного документу, відображеного у Законі України «Про електронні документи та електронний документообіг» (який є спеціальним (профільним), а отже й пріоритетним для врегулювання цифрових відносин в кримінальному провадженні) , з положень якого випливає, зокрема, що «*відображення* даних вважається електронною або паперовою копією електронного документу та потребує засвідчення у порядку, встановленому законом (ч.5,6 ст.7). За загальним правилом, оригіналом електронного документа визнається примірник документа з обов'язковими реквізитами, у т.ч. – з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронні довірчі послуги» (ч.2 ст.7) [2].

При цьому в якості оригіналу може бути визнані судом й дублікат документа (документ, виготовлений таким самим способом, як і його

оригінал), а також копії інформації, у тому числі комп'ютерних даних, що міститься в інформаційних (автоматизованих) системах, електронних комунікаційних системах, інформаційно-комунікаційних системах, комп'ютерних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста (ч.4 ст.99 КПК). З огляду на специфіки способів формування електронної інформації з такої нормативної регламентації не зрозумілим залишається процедура виготовлення дублікату електронного документа, а відповідно й порядок верифікації тотожності оригіналу та дублікату електронного документа, а також – у якій формі має бути скопійована інформація під час проведення процесуальних дій: паперовій чи електронній.

Позначена правова невизначеність обумовлює наявність діаметрально протилежних правових позицій ВС. Так, зокрема, у постанові ККС від 11 березня 2020 р. по справі № 149/745/14 490 ВС підтримав визнання недопустимим не лише використання у доказуванні копій відеофонограм, зроблених під час НС(Р)Д, а й протоколів як похідних від них доказів. У той самий час у постанові ККС ВС від 15 січня 2020 р. по справі № 161/5306/16-к визнано можливим подання до суду дублікатів матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі електронних), виготовлених слідчим, прокурором із залученням спеціаліста. У рішенні від 29 березня 2021 р. по справі № 554/5090/16-к ВС висловив позицію про те, що один і той самий електронний документ може існувати на різних носіях. Усі ідентичні за своїм змістом екземпляри електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом і датою створення. Питання ідентифікації електронного документа як оригіналу можуть бути вирішені уповноваженою особою, яка його створила (за допомогою спеціальних програм порахувати контрольну суму файлу або каталогу з файлами – CRC-сума, hash-сума), або за наявності відповідних підстав шляхом проведення спеціальних досліджень.

Видається вирішення як позначеного питання щодо оригінальності електронних доказів та вимог до їх копії, так і інших аспектів можливо лише у спосіб унормування в КПК комплексу питань щодо використання цифрової інформації у кримінальному провадженні з урахуванням специфіки їх інформаційної природи та «унікальних характеристик» [3].

В цьому контексті слід, зокрема, звернути увагу на рекомендації, що сформульовано у Звіті щодо України, підготовленому Офісом Програми

з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Марко Куннапу і пана Марка Юріча, про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них (2016/DGI/JP/3608 3 листопада 2016 року). Відповідно до рекомендацій 9–10 цього Звіту «наявність конкретних критеріїв щодо визначення електронних доказів може й не бути абсолютною необхідністю, проте є дуже цінною. По-перше, запровадження такої дефініції значно спростило б процес розробки конкретних процесуальних заходів. Це особливо важливо, оскільки інші правила КПК, пов'язані з доказами, не відповідають концепції електронних доказів, адже всі наявні процесуальні заходи орієнтовані на доказ як на фізичний або матеріальний об'єкт. По-друге, запровадження поняття «електронних доказів» збільшить правову чіткість і передбачуваність закону. Створення спеціальних законів про електронні докази та відповідні процесуальні заходи дозволять установити правила щодо прийнятності електронних доказів» [4].

**Список використаних джерел**

1. 'Судді ВС обговорили з експертами питання щодо допустимості електронних доказів, отриманих із відкритих джерел (Судова влада України, 7 червня 2022) https://supreme.court.gov.ua/supreme/pres-centr/news/1282146/?fbclid=IwAR38uhyaCGNZyG19U7Wjs3l20JCS3uuPfSCwOeUx4BFW9iWWysF6297brsY .

2. Скрипник А. В. *Використання цифрової інформації в кримінальному процесуальному доказуванні: монографія* (Право, 2022) 122.

3. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування / Д. М. Цехан // Науковий вісник Міжнародного університету. 2013. №5. С. 259.

4. Звіт щодо України, підготовлений Офісом Програми з кіберзлочинності на основі експертної підтримки незалежних експертів Ради Європи пана Марко Куннапу і пана Марка Юріча, про чинне законодавство і проекти законів, що доповнюють різні питання, пов'язані з кіберзлочинністю та електронними доказами, та вносять зміни до них ( 2016/DGI/JP/3608 3 листопада 2016 року). https://rm.coe.int/16806f3743.// Цит. За: Шило О. Г., Шило А. В. 'До питання впровадження в Україні електронного кримінального провадження' *Правові засади діяльності правоохоронних органів*: збірник наукових статей, тез доповідей та повідомлень за матеріалами VII Міжнародної науково-практичної конференції (10–11 грудня 2020 року, Харків) Вип. 36. 109–111.

# ПРОБЛЕМИ КОТРОЛЮ ЗА ОНЛАЙН ДИСТРИБУЦІЄЮ ЛІКАРСЬКИХ ЗАСОБІВ

**Гнедик Євген Сергійович,**
кандидат юридичних наук,, молодщий науковий співробітник
Лабораторії дослідження проблем національної безпеки у сфері
громадського здоров'я НДІ вивчення проблем злочинності
імені академіка В. В. Сташиса
НАПрН України, м. Харків, Україна

**Нога Петро Петрович,**
асистент кафедри цивільного, господарського
і фінансового права Полтавського юридичного інституту Національного
юридичного університету імені Ярослава Мудрого,
молодщий науковий співробітник Лабораторії дослідження проблем
національної безпеки у сфері громадського здоров'я НДІ вивчення
проблем злочинності імені академіка В. В. Сташиса НАПрН України,
м. Харків, Україна

В Україні значна кількість незаконних лікарських засобів реалізується саме з використанням мережі Інтернет. Йдеться про так званий «чорний онлайн ринок лікарських засобів», на якому реалізуються фальсифіковані, нестандартні, не зареєстровані в певній країні, а також неякісні лікарські засоби. Це один із найприбутковіших видів злочинного бізнесу. Проблема його функціонування не є новою для світу, ще у 1999 р. за ініціативою Національної асоціації фармацевтів США (National Association of Boards of Pharmacy, NABF), було запроваджено програму верифікації сайтів Інтернет-аптек [1]. США також вживала низку заходів щодо безпеки фармацевтичної діяльності. Та незважаючи на це незаконний продаж в Інтернеті небезпечних ліків є широко розповсюдженим видом діяльності й там. За даними звіту NABF, оприлюдненого у 2015 р., внаслідок аналізу біля 11 тис. веб-сайтів, які здійснювали в США онлайн торгівлю рецептурними лікарськими засобами, було виявлено 96% тих, що не відповідали фармацевтичному законодавству США і стандартам безпеки пацієнтів [2].

Починаючи з 2008 р. Інтерпол координує щорічне проведення у світі операції Pangea (18–25 травня 2021 році було проведено операцію Pangea-XIV, в якій взяли участь 92 країни. Було перевірено 710 тис. упаковок лікарських засобів, вилучено небезпечної продукції на суму 23

млн.доларів США, закрито 113 тис.веб-сайтів, через які здійснювався продаж ліків, заарештовано 277 осіб [3]. Натомість Європол 17 квітня 2020 р.представив звіт «Вірусний маркетинг – фальсифіковані, субстандартні товари і злочини проти інтелектуальної власності під час пандемії COVID-19». У цьому звіті поряд із Туреччиною Україна віднесена до основних країн-транзитерів контрафактної і субстандартної медичної продукції в країни ЄС. За даними звіту 8,1% підозрюваних, які поставляли до ЄС таку продукцію, мали громадянство України, що поступається лише Польщі і Румунії, громадянство яких мали 12,3% і 11,1% осіб відповідно [4]. Підтвердженням гіпотези про наявність в Україні широкого ринку незаконних лікарських засобів, що реалізуються з використанням мережі Інтернет є дані з цієї мережі [5].

Таким чином, маємо констатувати наявність в Україні розгалуженої системи незаконних Інтернет-аптек, що здійснюють продаж лікарських засобів невідомого походження, щодо яких не здійснюється передбачений Законом «Про лікарські засоби» контроль походження, якості, умов зберігання і транспортування та, як наслідок, відсутній кримінально-правовий механізм захисту потерпілих осіб від дій злочинців.

Відсутність в Україні контролю походження і якості лікарських засобів на стрімко зростаючому онлайн ринку створює сприятливі умови для обігу фальсифікованих лікарських засобів. Разом із тим, аналіз судової практики щодо застосування за ст. 321–1 КК «Фальсифікація лікарських засобів або обіг фальсифікованих лікарських засобів» свідчить, що з 29 вироків, постановлених судами І інстанції в України, винесених за цією статтею з 2013 по серпень 2021 рр., лише в одному йдеться онлайн продаж фальсифікованого лікарського засобу [6].

Враховуючи, що широко розповсюджена в Україні незаконна онлайн торгівля ліками є в світі одним із основних каналів реалізації як фальсифікованих, так і незареєстрованих лікарських засобів, можна припустити високий рівень латентності такої діяльності.

Електронна дистанційна роздрібна торгівля лікарськими засобами в Україні вперше була дозволена на підставі Постанови Кабінету Міністрів України від 23 березня 2020 р. №220. Відповідно до цієї Постанови були внесені зміни до Ліцензійних умов провадження господарської діяльності з виробництва лікарських засобів, оптової та роздрібної торгівлі лікарськими засобами, імпорту лікарських засобів (крім активних фармацевтичних інгредієнтів), якими надано дозвіл на здійснення дистанційної роздрібної торгівлі лікарськими засобами у разі встанов-

лення карантину відповідно до Закону України «Про захист населення від інфекційних хвороб» або введення надзвичайного стану відповідно до Закону України «Про правовий режим надзвичайного стану» на період його встановлення. Право на здійснення такої діяльності було надане лише ліцензіатам, що мають ліцензію на провадження господарської діяльності з роздрібної торгівлі лікарськими засобами, яким також було надано дозвіл на організацію та здійснення доставки лікарських засобів безпосередньо споживачам з дотриманням умов зберігання лікарських засобів, визначених виробником під час їх транспортування, зокрема із залученням на договірних засадах операторів поштового зв'язку.

17 вересня 2020 р. електронна роздрібна торгівля лікарськими засобами отримала законодавче закріплення на підставі Закону «Про внесення змін до ст. 19 Закону України «Про лікарські засоби» щодо здійснення електронної роздрібної торгівлі лікарськими засобами». Цей закон набрав чинності 14.10.2020 р. та був введений в дію через 3 місяці з дня набрання чинності, тобто з 14 січня 2021 р. За час між набранням чинності і введенням в дію Кабінет Міністрів України відповідно до п. 3 Перехідних положень до зазначеного Закону був зобов'язаний розробити нормативно-правові акти, необхідні для його реалізації, привести свої нормативно-правові акти у відповідність із цим Законом, а також забезпечити приведення у таку відповідність нормативно-правових актів міністерствами та іншими центральними органами виконавчої влади. Законодавчі вимоги щодо електронної роздрібної торгівлі лікарськими засобами, передбачені цим Законом, мали забезпечити умови, за яких законну діяльність ліцензіатів можна було б легко відрізнити від незаконної діяльності, а умови доставки лікарських засобів споживачу відповідали б вимогам щодо зберігання і транспортування певного лікарського засобу. Зазначений Закон в цілому відповідає європейським стандартам електронної роздрібної торгівлі лікарськими засобами з використанням інформаційно-комунікаційних систем у частині створення механізму протидії потрапляння в обіг фальсифікованих лікарських засобів (положення Директиви 2011/62/ЕС Європейського парламенту і Ради від 8 червня 2011 р. про внесення поправок в Директиву 2001/83/ЄС). Однак фактично лише 22.09.2021 р. була прийнята Постанова Кабінету Міністрів України «Про внесення змін до Ліцензійних умов провадження господарської діяльності з виробництва лікарських засобів, оптової та роздрібної торгівлі лікарськими засобами, імпорту лікарських засобів (крім активних фармацевтичних інгредієнтів) та затвердження

Типової форми договору про здійснення доставки лікарських засобів кінцевому споживачу» №1002 [7]. Разом із тим, перевірка низки сайтів так званих Інтернет-аптек засвідчила, що до теперішнього часу законодавчі вимоги не виконуються повною мірою.

Як уявляється, ключовим гравцям фармацевтичного ринку набагато вигідніше здійснювати і надалі безконтрольний онлайн продаж ліків і жодним чином не відповідати за додержання умов їх зберігання і транспортування при доставці споживачу. Постійно гальмується впорядкування в Україні електронної роздрібної торгівлі лікарськими засобами, а законодавчі обмеження фактично не діють, контроль з боку Держлікслужби за такою діяльністю майже не здійснюється. Тим часом і надалі залишаються відкритими можливості для розростання незаконного продажу лікарських засобів з використанням так званих Інтернет-аптек і служб доставки ліків.

**Список використаних джерел**


1. National Association of Boards of Pharmacy. Digital Pharmacy. URL: https://nabp.pharmacy/programs/accreditations-inspections/digital-pharmacy/
2. Internet Drug Outlet Identification Program Progress Report for State and Federal Regulators. 2015. *National Association of Boards of Pharmacy*. URL: https://nabp.pharmacy/wp-content/uploads/2016/08/NABPIDOIReport_April2015.pdf
3. Pharmaceutical Crime Operations. Interpol. URL: https://www.interpol.int/en/Crimes/Illicit-goods/Pharmaceutical-crime-operations
4. Viral marketing Counterfeits, substandard goods and intellectual property crime in the COVID-19 pandemic .2020. URL: https://www.europol.europa.eu/publications-documents/viral-marketing-counterfeits-substandard-goods-and-intellectual-property-crime-in-covid-19-pandemic
5. Гуторова Н. О. Чорний онлайн ринок лікарських засобів під час пандемії COVID-19: правові засоби протидії. Форум права. 2021. №3. С. 15–24.
6. Вирок Шевченківського районного суду м. Києва від 15 жовтня 2020 року, справа №761/15193/20 (провадження №1-кп/761/2350/2020). URL: https://reyestr.court.gov.ua/Review/92843132#
7. Про внесення змін до Ліцензійних умов провадження господарської діяльності з виробництва лікарських засобів, оптової та роздрібної торгівлі лікарськими засобами, імпорту лікарських засобів (крім активних фармацевтичних інгредієнтів) та затвердження Типової форми договору про здійснення доставки лікарських засобів кінцевому споживачу : Постанова Кабінету Міністрів України; Форма типового документа від 22.09.2021 №1002. URL: https://zakon.rada.gov.ua/go/1002–2021-%D0%BF

# ВИКОРИСТАННЯ МЕТОДУ РЕКОНСТРУКЦІЇ ПІД ЧАС ЗАСТОСУВАННЯ ІННОВАЦІЙНИХ ДЖЕРЕЛ ЦИФРОВОЇ ІНФОРМАЦІЇ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

**Григоренко Андрій Олександрович**,
аспірант кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого,
молодший науковий співробітник лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України,
м. Харків, Україна

З метою забезпечення найбільш ефективного проведення досудового розслідування кримінальних правопорушень є необхідним впровадження інновацій у професійну діяльність осіб, уповноважених на розслідування суспільно небезпечних діянь. Зазначена потреба обумовлена розвитком суспільства, модернізацією засобів боротьби за злочинністю та новими способами вчинення злочинів.

Одним із напрямків розроблення інновацій є автоматизовані робочі місця (далі АРМ) та бази даних (далі БД). Використання зазначених інновацій є можливим за лише за посередництвом застосування криміналістичного методу реконструкції. Тому, є актуальним дослідження особливостей використання методу реконструкції під час застосування АРМ та БД.

Одним із прикладів АРМ є Автоматизоване робоче місце слідчого «Інсайт» [1]. Співробітники кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого розробили автоматизоване робоче місце слідчого (АРМ) «Інсайт» (Валерій Шепітько, Галина Авдєєва) [2, с. 61]. «Автоматизоване робоче місце слідчого «Інсайт» використовується в практичній, науковій та навчальній діяльності. Автоматизоване робоче місце слідчого «Інсайт» містить розділи: «Законодавство», «Процесуальні документи», «Слідчі дії», «Криміналістичні методики», «Судові експертизи», «Науково-технічні засоби», «Слідча практика», «Бібліографія», «Словник термінів», «Навчання», «Правоохоронні органи та експертні установи», «Довідкова корисна

інформація»" [3, с. 20]. Використання АРМ «Інсайт» надає можливість отримати інформацію щодо складання процесуальних документів, особливостей здійснення досудового розслідування відповідного різновиду кримінальних правопорушень, механізму ефективної реалізації слідчих (розшукових) дій, криміналістичних методик розслідування суспільно небезпечних діянь, науково-технічні засоби, що можуть бути використані та особливості їх застосування. Використання АРМ «Інсайт» можливо лише за посередництвом методу реконструкції, це зумовлено тим, що інформація, яка міститься в АРМ були зібрана і розроблена раніше у часі, а отже її використання є можливим шляхом відтворення у свідомості особи, уповноваженої на розслідування кримінального правопорушення, та співставлення із розслідуваним кримінальним правопорушенням. Особа, в результаті реконструкції, отримує не лише досвід щодо розкриття відповідного різновиду суспільно небезпечних діянь, але й методологічні рекомендації щодо здійснення досудового розслідування, інформації щодо особливостей правової регламентації, особливості застосування науково-технічних засобів, тощо.

Для ефективного здійснення досудового розслідування кримінальних правопорушень є доцільним використання баз даних та інформаційно-пошукових систем. Їх прикладами є БД «Практика слідчого» [4] та БД «Слідчий прецедент» [5]. «БД «Практика слідчого» являє собою сукупність декількох тисяч окремих довідок про процеси і результати розслідування в Україні та інших державах злочинів різних категорій (за останні 70 років), про особливості використання криміналістичних засобів і спеціальних знань у кримінальному провадженні … БД «Слідчий прецедент» являє собою електронну інформаційно-пошукову систему, яка містить більше двох тисяч матеріалів кримінальних проваджень за тяжкими та особливо тяжкими злочинами» [3, с. 20–21]. Пошук інформації та її обробка здійснюється за допомогою комп'ютерів [2, с. 62]. «Обидві БД призначені для використання співробітниками органів правопорядку для побудови слідчих (судових) версій, планування та найбільш ефективного провадження слідчих (судових) дій тощо. Також вони використовуються науковцями і викладачами кафедри криміналістики безпосередньо на практичних заняттях з курсів криміналістики, методики розслідування злочинів та судової експертизи як інтерактивний довідник» [3, с. 21]. Використання БД відбувається за допомогою криміналістичного методу реконструкції. Особа, уповноважена на розслідуван-

ня кримінального правопорушення, має змогу відтворити у своїй свідомості відомості про особливості розслідування відповідних суспільно небезпечних діянь для співставлення їх із розслідуваним суспільно небезпечним діянням. Отримані в результаті здійснення реконструкції дані та інформація є основою для висунення слідчих версій та планування досудового розслідування кримінального правопорушення.

Вагомим є те, що АРМ та БД можуть використовуватися не лише слідчими (детективами), але й прокурорами, адвокатами, суддями тощо. Використання зазначених інформаційних баз є можливим лише за посередництвом методу реконструкції. Це зумовлено тим, що бази даних містять у собі інформацію та дані, які були зібрані раніше, на основі раніше розслідуваних суспільно небезпечних діянь.

**Список використаних джерел**

1. В. Ю. Шепітько, Г. К. Авдєєва Автоматизоване робоче місце слідчого «Інсайт». Свідоцтво № 22566 про реєстрацію авторського права на твір від 6 листопада 2007 р.

2. Shepitko V. Introduction to Criminalistics. Kharkiv: Apostille Publishing House LLC. 2021. 168 p.

3. Шепітько В. Ю., Авдєєва Г. К. Проблеми застосування науково-технічних засобів та інноваційних продуктів у діяльності органів правопорядку. *Теорія та практика судової експертизи та криміналістики*. 2019. Т. 20 № 2. С. 11–26.

4. В. Ю. Шепітько, Г. К. Авдєєва База даних «Практика слідчого». Свідоцтво № 49389 про реєстрацію авторського права на твір від 30 травня 2013 р.

5. В. Ю. Шепітько, Г. К. Авдєєва База даних «Слідчий прецедент». Свідоцтво № 60084 про реєстрацію авторського права на твір від 9 червня 2015 р.

# ВПЛИВ ЦИФРОВИХ ТЕХНОЛОГІЙ НА СВОЄЧАСНІСТЬ ПРИЙНЯТТЯ КРИМІНАЛЬНИХ ПРОЦЕСУАЛЬНИХ РІШЕНЬ ДОСУДОВОГО РОЗСЛІДУВАННЯ

**Донченко Артур Анатолійович**,
аспірант Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

У загальних рисах своєчасність кримінальних процесуальних рішень досудового розслідування (далі – КПР) – це вимога, що висувається до КПР відповідно до якої рішення має бути прийняте в момент, який є об'єктивно необхідним, оптимальним для його прийняття без невиправданої затримки та невиправданого поспіху у межах строку, передбаченого чинним КПК з огляду на специфіку конкретного рішення та обставини кримінального провадження та є оптимальним для досягнення корисного ефекту з максимально можливим рівнем забезпечення прав та законних інтересів учасників процесу [1]. На забезпечення своєчасності КПР досудового розслідування впливає низка чинників, одним з яких є й розвиток цифрових технологій.

Одним з напрямів цифровізації кримінального провадження, що має безпосередній вплив на забезпечення своєчасності КПР досудового розслідування видається запровадження електронного кримінального провадження. Підкреслимо, що у країнах ЄС, США вже давно і успішно запроваджують ІТ-технології у правовій системі у вигляді обміну процесуальними документами, даними, керуванням матеріалами проваджень між прокуратурою, слідством і судами [2].

У цьому контексті не можна оминути увагою той факт, що з 30 квітня 2020 р. розпочала свою роботу пілотна версія електронного кримінального провадження eCase, яка інтегрується з наявними в Україні автоматизованими системами («Трембіта», СЕВ ОВВ) та документообігами, які потрібні в кримінальному процесі, при цьому відсутня необхідність їх змінювати або створювати нові. Перевагами запровадження eCase є те, що: прокур контролює хід розслідування та здійснює процесуальне керівництво в режимі on-line; слідчі оперативно отримують та мають можливість аналізувати всі необхідні дані, адже система оновлює всю інформацію на кожному етапі, планує time-management та ка-

лендар завдань; свідки, підозрювані та їх представники також отримують необхідні документи в електронному форматі; судді та слідчі судді мають можливість доступу до системи навіть в умовах судового засідання для додаткового дослідження доказів та ключових позицій у провадженні [2].

Такий позитивний досвід пілотної системи eCase став підставою для прийняття Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування». Крім того, спільним Наказом Національного антикорупційного бюро України, Офісом Генерального прокурора, Радою суддів України та Вищим антикорупційним судом від 15 грудня 2021 р. № 175/390/57/72 затверджено Положення про інформаційну-телекомунікаційну систему досудового розслідування (далі – Положення). Звернімо увагу на деякі ключові положення зазначеного нормативного документа, які безпосередньо впливатимуть на забезпечення своєчасності КПР досудового розслідування.

По-перше, одним з основних завдань інформаційної-телекомунікаційної системи досудового розслідування (далі – Система) є створення умов для електронної взаємодії та автоматизації роботи суб'єктів Системи з метою підвищення ефективності виконання завдань, покладених на них законодавством, зменшення часових та фінансових витрат на здійснення досудового розслідування, управлінські, інформаційно-пошукові, аналітичні роботи, формування звітності.

По-друге, Положенням передбачається, що матеріали кримінального провадження, зокрема клопотання, постанови, протоколи, доручення тощо, створюються у Системі з використанням форм та шаблонів. Погодження чи відмова у погодженні, затвердження чи відмова у затвердженні процесуального документа здійснюється за допомогою відповідного функціоналу Системи із накладенням кваліфікованого електронного підпису. Безперечно, такий процес прийняття КПР (особливо КПР, що приймаються у порядку складної процедури) є набагато ефективнішим з точки зору забезпечення його відповідності якісним характеристикам та своєчасності, зокрема (п. 32).

Водночас певний подив викликає той факт, що така Система запроваджується виключно у кримінальних провадженнях, досудове розслідування в яких здійснюється детективами Національного антикорупційного бюро України (п. 1 Положення). Адже за логікою вище згадуваного

Закону України функціонування Системи має бути запроваджено в усіх органах досудового розслідування. Підкреслимо, що запровадження електронного кримінального провадження значно прискорює, спрощує та здешевлює процеси розслідування кримінальних правопорушень, підвищує його ефективність, знижує корупційні ризики. У зв'язку з цим видається необхідним розробка Положення про інформаційну телекомунікаційну систему досудового розслідування, яким би унормовувалося функціонування такої системи для всі органів досудового розслідування, прокурорів та судів.

Крім того у аспекті розглядуваного питання перспективним напрямом цифровізації кримінального провадження видається електроне правосуддя. Під електронним правосуддям розуміється використання інформаційно-комунікаційних технологій у реалізації правосуддя усіма зацікавленими сторонами в юридичній сфері з метою підвищення ефективності та якості державних служб, зокрема, для приватних осіб і підприємств, яке охоплює електронне спілкування та обмін даними, а також доступ до інформації судового характеру [3].

Позначені напрями цифровізації кримінального провадження є безпосередніми чинниками, що забезпечують своєчасності КПР досудового розслідування, адже всі вони спрямовані на ефективізацію кримінальної процесуальної діяльності, економію розумових, часових, фінансових ресурсів, а отже оптимізацію роботи органів досудового розслідування, прокуратури та суду.

**Перелік використаних джерел:**

1. Донченко А. А. Поняття та значення своєчасності кримінальних процесуальних рішень досудового розслідування. *Питання боротьби зі злочинністю.* 2021. № 41. С. 138–145

2. Систему електронного кримінального провадження eCase запустять вже 30 квітня // LegalHub.online. 2020, 8 квіт: URL: https://legalhub.online/kryminalne-pravo/systemu-elektronnogo-kryminalnogo-provadzhennya-ecase-zapustyat-vzhe-30-kvitnya/

3. Рекомендации Комитета министров Совета Европы CM/Rec(2009)1 государствам-участникам Совета Европы по электронной демократии : (приняты 18.02.2009 г. на 1049-м собрании зам. министров) // Центральная избирательная комиссия РФ. URL: http://cikrf.ru/international/recommend.doc

# ЦИФРОВІ ДАНІ ЯК ДОКАЗ СКОЄННЯ КІБЕРЗЛОЧИНУ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

**Дунаєва Тетяна Євгенівна,**
кандидат юридичних наук, науковий співробітник
відділу дослідження проблем кримінального процесу та судоустрою
Науково-дослідного інституту вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

Слід зазначити, що законодавець на сьогодні ще не визначив поняття «електронні докази» (electronic evidence) та поняття «цифрові докази» (digital evidence), а тому їх використовують паралельно. Цифрові пристрої є скрізь у сучасному світі, допомагаючи людям легко спілкуватися локально та глобально. Комп'ютери, мобільні телефони та Інтернет не єдині джерела цифрових доказів. Будь-яка технологія, яка обробляє інформацію, може бути використана у злочинний спосіб. Наприклад, портативні ігри можуть передавати закодовані повідомлення між злочинцями, а навіть новіші побутові прилади, такі як холодильник із вбудованим телевізором, можуть використовуватися для зберігання, перегляду та обміну незаконними зображеннями. Важливо слідчим вміти розпізнавати й належним чином вилучати потенційні цифрові докази.

Цифрові докази визначаються як інформація та дані, важливі для розслідування, які зберігаються, отримуються або передаються електронним пристроєм. Ці докази можна отримати, коли електронні пристрої вилучаються та захищаються для експертизи. Цифрові докази: є латентними (прихованими), як відбитки пальців або докази ДНК; швидко та легко перетинають юрисдикційні кордони; можна змінити, пошкодити або знищити без зусиль; можуть бути чутливим до часу. Існує багато джерел цифрових доказів, але є найбільш розповсюдженими такі категорії пристроїв, на яких можна знайти докази: інтернет-мережі, автономні комп'ютери або пристрої та мобільні пристрої. Ці сфери мають різні процеси збору доказів, інструменти та проблеми, а різні типи злочинів, як правило, піддаються тому чи іншому пристрою.

Виділяють два види даних цифрових відбитків: активні і пасивні. Дані, які є частиною активних і пасивних цифрових відбитків, можуть використовуватися як доказ скоєння злочину, в тому числі кіберзлочину

(тобто в якості цифрових доказів). Такі дані можуть також використовуватися для доведення або спростування твердження про факт; підтвердження або спростування показань потерпілого, свідка і підозрюваного; визначення причетності або непричетності підозрюваного до скоєння злочину. Дані, що добуваються, можуть бути ідентифіковані як контент, і дані, що не відносяться до контенту, або мета-дані. Дані, що одержуються в режимі онлайн і добуваються із цифрових пристроїв, можуть містити велику кількість інформації про користувачів і події [1]. Цифрові докази створюють унікальні складності при аутентифікації через обсяг доступних даних, їх швидкості, нестійкості і уразливості. Є міжнародні стандарти, що стосуються поводження з цифровими доказами (ISO/IEC 27037 Керівництво по ідентифікації, збирання, одержання і збереження свідчень, представлених в цифровій формі). Слід зазначити, що є чотири етапи поводження з цифровими доказами (ідентифікація, збір, отримання і збереження) [2].

Отже, інформація та комп'ютерна техніка можуть виступати предметом злочинних посягань, оскільки сфера кіберзлочинності посягає в певній мірі на права та свободи людини у інформаційному просторі. Докази кіберзлочинів досить важко отримати, оскільки інформаційний простір є масштабним полем для діяльності осіб, які посягають на кіберсвободу громадян та їх цифрові права.

**Список використаних джерел**

1. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права.* 2022. № 1. URL: DOI https://doi.org/10.32782/klj/2022.1.27.

2. 2. Спрощений посібник із криміналістики. Цифрові докази. URL: https://www.forensicsciencesimplified.org/digital/.

# ВПРОВАДЖЕННЯ ІННОВАЦІЙ У МЕТОДИЦІ РОЗСІДУВАННЯ КРИМІНАЛЬНИХ ПОЖЕЖ

**Зарубін Кирило Євгенійович**
аспірант кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

У сьогоднішніх реаліях ми можемо спостерігати швидкий розвиток науково-технічного прогресу. Завдяки таким явищам як цифровізація та діджиталізація новітні технології та засоби їх застосування впроваджуються у всі аспекти соціального середовища. Впровадження таких технологій дозволяє більш ефективно вирішувати завдання, що постають перед спеціалістами той чи іншої сфери.

Певні інтеграції відбуваються і в криміналістиці. Сучасний етап розвитку криміналістики, її перспективи характеризуються активними дослідженнями та застосуванням інноваційних засобів і технологій у всіх її складових – загальній теорії криміналістики, криміналістичній техніці, криміналістичній тактиці та криміналістичній методиці [1, с. 21]. Одною із цілей криміналістики є пропонування інноваційних досягнень науки та прогресу та їх впровадження у практику протидії злочинності.

Подібні інновації інтегруються як розробки в галузі криміналістичної техніки, тактики та методики розслідування злочинів, а саме: нові розроблені або прилаштовані до потреб слідчої (судової) практики технікокриміналістичні засоби, сучасні інформаційні технології, електронні бази знань, методи фіксації, аналізу та оцінки доказової інформації, нові тактичні прийоми, їх комплекси, тактичні комбінації та операції, алгоритми першочергових слідчих (розшукових) дій та перевірки типових слідчих версій, методики розслідування нових видів злочинів та ін. [2, с. 147–148].

Впровадження нових ідей та напрямків допомагає з вирішенням різноманітних проблем, які з'являються з появою нових тенденцій у кримінальному середовищі, шляхом пропонування нових варіантів вирішення або пристосуванням вже існуючих.

Досить важливим є питання модернізації криміналістичної методики. На сьогодні з'являється досить багато видів криміналістичних методик, а вже існуючі розширяються та доповнюються новою інформацією. Ця тенденція є результатом впровадження інновацій, але в свою чергу є досить дискусійним явищем.

У прагматичному сенсі криміналістична методика складається із упорядкованого комплексу порад типізованого характеру. Така методика має містити типові комплекси слідчих (розшукових) та інших дій або заходів, передбачає певну послідовність їх реалізації. В свою чергу, головною функцією методики є саме те як здійснювати розслідування. Тому суттєву роль має відігравати саме пізнавальна функція – сприяння оптимальному розслідуванню певного виду злочинів. [2, с. 149].

При побудові окремих криміналістичних методик слід більше зосереджуватися саме на практичному аспекті. На сьогодні такі методики дедалі більше наповнюються теоретичним матеріалом який виражається в пропонуванні різноманітних підходів до визначення понять, думок стосовно спрямованості тих чи інших елементів та дискусій стосовно напрямку подальшого розвитку. Це в свою чергу може ускладнювати сприйняття таких рекомендацій кінцевим реципієнтом – детективом, слідчим або прокурором – та робити застосування таких методик неефективним.

Також важливим елементом будь-якої криміналістичної методики є правильна побудова криміналістичної характеристики окремих злочинів що виявляється у її логічно узгодженій структурі та уніфікації її окремих елементів. Це допомагає використовувати таку характеристику за цільовим, уникаючи питань, що часто виникають у практиці.

Побудова та використання криміналістичної характеристики кримінальних пожеж на сьогодні також потребує інтеграцію інноваційних елементів. Кримінальні пожежі охоплюють як умисні дії певних осіб, спрямовані на знищення або пошкодження майна та іншу шкоду за допомогою вогню (підпал), так і прояв злочинної необережності (порушення встановлених законодавством вимог пожежної безпеки та інші дії чи бездіяльність) [3, с. 401–402].

Слід почати із нагальної потреби побудови та уніфікації структури такої характеристики, адже на сьогодні досі не існує єдиного підходу до її визначення.

Окрім цього, потребує переосмислення окремі елементи криміналістичної характеристики кримінальних пожеж. У поточних реаліях слід приділяти особливу увагу таким складовим як обстановка вчинення кримінальних пожеж та наслідки які можуть бути викликані такими пожежами. Також важливим є розмежування ознак що притаманні підпалам, як складової кримінальних пожеж, та тих, що характеризують порушення встановлених законодавством вимог пожежної безпеки.

Застосування цифрових технологій, наприклад, може знайти своє втілення в узагальненні великого масиву кримінальних проваджень з метою отримання типових даних про особу злочин або способів вчинення. Завдяки цьому, по-перше, витрачається значно менше часу для такого узагальнення, і, по-друге, отримуються більш достовірні дані, підґрунтям яких виступає статистика.

З огляду на викладене, можна дійти висновку, що натепер існує багато шляхів впровадження інновацій у методику розслідування кримінальних пожеж. Але, слід наголосити на тому, що така імплементація має здійснюватися дійсно там, де вона необхідна і полегшувати процеси виконання завдань, покладених на правоохоронні органи та їх посадових осіб, а не ускладнювати їх.

**Список використаних джерел**

1. Шевчук В. М. Криміналістична інноватика: поняття, функції, завдання та перспективи досліджень. *Теорія та практика судової експертизи і криміналістики*. 2020. № 22. С. 20–40. URL: https://khrife-journal.org/index.php/journal/article/view/363/378

2. Шепітько В. Ю. Інновації в криміналістці як віддзеркалення розвитку науки. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матеріали міжнародного «круглого столу», 12 грудня 2019 р. Харків: Право, 2019. С. 147–150.

3. Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. За ред. проф. В. Ю. Шепітька. 4-е вид., перероб. і доп. Харків: Право, 2008. С. 401–402.

# DIGITAL TRAIL…IN SEARCH OF THE PERPETRATOR OF A CRIME AND MORE (…)

**Elżbieta Żywucka – Kozłowska**,
Associate Professor of the Department of Criminal Procedure and Executive Criminal Law
Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, Poland

**Rossana Broniecka**,
Dr of the Department of Criminal Procedure and Executive Criminal Law
Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn, Poland

Contemporary reality is primarily represented by the two dimensions: real and cybernetic.To some extent, we have become accustomed to a digital existence (in the broad sense). A person can work remotely, learn remotely, and commit crimes remotely. It is rightly emphasized in the literature on the subject that «Digital space is created by all our activities that result in the creation of digital data, a digital footprint, and which do not have to be the result of using the Internet.»[ 1. p. 9] . It is difficult to disagree with this thesis in its general sense. The situation changes slightly when the main goal of human activity on the net is a criminal goal. It is impossible not to notice that every cybernetic crime [2. p.34] in the broadest perspective leaves a digital trace. Most often, these are acts involving data destruction, information theft, data manipulation, sabotage [3.p.168]. The digital footprint in question is defined in various ways (lexical perspective), but the essential element of these definitions is «as a digital object that contains credible information to support or reject the hypotheses»[4.p.12]. Digital traces are left by digital devices, as well as by the person who uses them both as an authorized and unauthorized entity [5.p.158]. A different category of crimes (from those mentioned above) in which digital traces are secured are sexual crimes, in particular pedophilia. Disturbed sexual preferences have found outlet not only in the real world, but above all on the net. In fact, pedophiles are looking for optimal (in their opinion, safe) places to look for sexual objects of desire (children). They are anonymous (apparently) online, which intensifies their activity. In most modern countries, sexual intercourse with minors is punishable, but this

prohibition does not stop them from committing a crime [6.pp.37–77]. Such activities enable establishing contact with a potential victim. Law enforcement authorities organize andpra carry out operations aimed at establishing the identity of persons who, on the Internet, encourage minors to meet intimately and take photographs in the same context. It is worth emphasizing here that the possession or dissemination of pornography is also punishable [7.p.49–50]

Digital traces allow you to locate the location of a specific object (but also the movement of such an object). It is not only logins to the network, text information (usually the content of e-mails, messages saved in the history of correspondence (communicators) with a specific recipient, photos, videos. The case files of many criminal proceedings contain lists of telephone calls of the aggrieved person and the suspected, allowing for the assumption of existing relationships or connections of these people. Today, no one is surprised by securing and viewing footage from city (or other) surveillance cameras, the record of which may be of significant (and sometimes crucial) importance for the ongoing criminal proceedings. Digital traces left on the Internet by people the Police are looking for. This applies not only to the perpetrators of crimes, but also to missing persons. Every year, several thousand disappearances of both adults and children are recorded in Poland. It is worth noting that some of these cases are classified as abductions (including kidnapping ). This state of affairs generated horses the necessity of developing new search procedures, including child alert [8.p.44].

Digital technology (in its widest dimension) of the 21st century supports the process of not only identifying a person, but is also extremely useful in searching for missing people and investigating connections between entities committing crimes in the network. This is particularly important in prosecuting perpetrators of trafficking in human beings, pedophilia and combating child pornography. Tools typical of the digital sphere are configured with criminal analysis (more broadly, criminal intelligence) [9.p.6].

It is rightly emphasized in the literature that «criminal analysis is a complex process requiring the collection of information from many different sources, such as telephone billings, bank transaction histories, and eyewitness testimonies. Most of this data is spatial in nature, which means that it can be represented and analyzed using maps. Due to the huge amount of processed data, their analysis is practically impossible without the use of advanced IT systems» [10.p.327]. It is difficult to disagree with this thesis, considering that digital technology has become a permanent part of the everyday life of modern

man. The possibilities in this regard are constantly expanding. It is possible what 30 years ago was something completely unreal or fantastic.

The framework of the study does not allow for a broader presentation of the essence of the digital trace and its usefulness in the practice of law enforcement and the judiciary, therefore we limit ourselves to the presentation of one case in which the key to the detection process was the title digital trace. Police officers from the Cybercrime Department of the Provincial Police Headquarters in Białystok detained a suspect of proposing sexual encounters to minors in exchange for financial remuneration. In the course of the investigation, it was established that the suspect used publicly available social networking sites for this purpose. Several storage media with pedophile content were secured [11, p. 1]

Similar cases could be multiplied, but it does not seem necessary. On the Internet (in particular on the official websites of the Police), announcements about the arrest of perpetrators of crimes, including those operating in cyberspace, are published.

Digital technology, of course, is used in all ways and by various entities, including the criminal world. This legally prohibited activity is countered by forensic computer science with a whole range of different tools necessary to counteract crime. It should also be emphasized that cyber tools are extremely effective, invisible in a way, which significantly shortens the time of identifying the threat and the perpetrator.

**Bibliography**

1. D. Ilnicki , K. Janc, Buszując w sieci ( w:) ACADEMIA-magazyn Polskiej Akademii Nauk 2022.
2. K. J. Jakubski, Przestępczość komputerowa ( w: ) Prokuratura i Prawo 1996, nr 12.
3. M. Szczepaniec, Komputer jako narzędzie przestępstwa ( w: ) Zeszyty Prawnicze 2012, nr 12.2.
4. B. Carrier, File System Forensic Analysis, Addison Wesley Professional, Indiana, 2005.
5. A. Hyła, Analiza śladów cyfrowych ( w: ) Prokuratura I Prawo 2018, nr 5.
6. P. Góralski, O zagadnieniu racjonalnej kryminalizacji i penalizacji pedofilii w polskim prawie karnym. Nowa Kodyfikacja Prawa Karnego 2011, nr 27.
7. E. Zielińska, O zgodności polskiego ustawodawstwa karnego z Protokółem Dodatkowym do Konwencji i Prawach Dziecka w sprawie handlu dziećmi,

dziecięcej prostytucji, pornografii. Dziecko krzywdzone. Teoria, badania, praktyka 2005, nr 4(3).

8. A. Wentkowska, Poszukiwania osób zaginionych. System i metody działania w procedurach służb, Biuro Rzecznika Praw Obywatelskich, Warszawa.2016.

9. W. Ignaczak, Wybrane zagadnienia analizy kryminalnej, Wydawnictwo Wyższej Szkoły Policji, Szczytno 2005

10. R. Marcjan, M. Łakomy, M. Wysokiński, , K. Piętak, M. Kisiel-Dorohinicki, Analiza kryminalna wspomagana narzędziami GIS w aplikacji LINK. *Zeszyty Naukowe AON*, 2013, nr (4 (93)).

11. Źródło: https://www.policja.pl/pol/aktualnosci/160053,Cyberpolicjanci-zatrzymali-pedofila.html [ dostępne 23.12.2022]

# ДЕЯКІ ПРОБЛЕМНІ ПИТАННЯ ЗДІЙСНЕННЯ ДИСТАНЦІЙНОГО СУДОВОГО ПРОВАДЖЕННЯ

**Клепка Дар'я Ігорівна**
кандидат юридичних наук, науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України, м. Харків, Україна

Здійснення дистанційного судового провадження поза межами приміщення суду з використанням власних технічних засобів у кримінальному процесі стало можливим після прийняття рішення «Щодо вжиття невідкладних заходів для забезпечення сталого функціонування судової влади в Україні в умовах припинення повноважень ВРП та воєнного стану у зв'язку зі збройною агресією з боку РФ» Радою суддів України. У цьому рішенні, зокрема, зазначається, що якщо за об'єктивних обставин учасник провадження не може прибути в судове засідання, суд може допустити участь такого учасника в режимі відеоконференції за допомогою будь-яких інших технічних засобів, у тому числі і власних [1]. І хоча позначене рішення й не має нормативного характеру, водночас стало єдиною підставою для здійснення дистанційного судового провадження з використанням власних технічних засобів у кримінальному процесі. Однак враховуючи фактично відсутність нормативного регулювання питання здійснення дистанційного судового провадження поза межами приміщення суду з використанням власних технічних засобів на практиці виникає багато проблемних питань.

Так, наприклад, аналіз судової практики свідчить, що у низці рішень у резолютивних частинах зазначається, що ризики технічної неможливості участі у відеоконференції поза межами приміщення суду, переривання зв'язку тощо несе учасник справи, який подав відповідну заяву [2, 3]. Необхідно зауважити, що у проєкті Закону України «Про внесення змін до Кримінального процесуального кодексу України щодо забезпечення поетапного впровадження Єдиної судової інформаційно-телекомунікаційної системи» від 23 листопада 2022 реєстр № 8219 (далі – проєкт Закону), у якому здійснюється спроба унормувати здійснення дистанційного судового провадження з використанням власних

технічних засобів, пропонується передбачити аналогічне положення в ст. 336 КПК.

Водночас, нами критично оцінюється як судова практика, в якій технічні ризики, пов'язані з участю у дистанційному судовому провадженні з використанням власних технічних засобів, покладаються на особу, яка ініціювала такий судовий розгляд, так і законодавчі ініціативи з цього приводу.

Наведемо відповідні аргументи. *По-перше*, не зовсім зрозумілим є змістовне навантаження такого положення, враховуючи, що наслідки переривання зв'язку та технічної неможливості участі особи у відеоконференції не передбачаються чинним законодавством. *По-друге*, виникає питання щодо можливості покладення на особу ризиків переривання зв'язку та технічної неможливості участі у відеоконференції внаслідок неможливості суду забезпечити стійкий зв'язок або взагалі розпочати відеоконференцію (особливо враховуючи перебої з електропостачанням, які спостерігаються останнім часом у нашій державі). *По-третє*, в аспекті досліджуваного питання необхідно звернути увагу на Висновок Консультативної ради європейських суддів № 14 (2011), у п. 5 якого зазначається, що *ІТ повинні бути інструментом або засобом удосконалення адміністрування судочинства, полегшувати доступ користувачів до судів та укріплювати гарантії, встановлені статтею 6 Конвенції про захист прав людини і основоположних свобод: доступ до правосуддя, неупередженість, незалежність судді, справедливість та розумні строки розгляду справи (курсив наш – Д. К.)*. У будь-якому разі правосуддя не може існувати окремо від осіб, що до нього звертаються, а розвиток ІТ не звільняє суди від здійснення своїх повноважень (п. 20) [4].

З наведеного вбачається, що запровадження у чинному КПК цифрових технологій (наприклад, здійснення судового розгляду в режимі відеоконференції з використанням власних технічних засобів) у будь-якому випадку не можуть зазіхати на фундаментальне право людини на справедливий суд. У той самий час покладення на особу ризиків технічної неможливості участі в відеоконференції поза межами приміщення суду з використанням власних технічних засобів або переривання зв'язку може стати потенційно небезпечним з точки зору забезпечення права особи на доступ до правосуддя.

У продовження аналізу питання щодо наслідків технічної неможливості участі особи, яка подала відповідне клопотання у судовому роз-

гляді, варто звернути увагу, що сьогодні на практиці трапляються випадки, коли, наприклад, слідчі судді розглядають скарги, по суті, за відсутності скаржника та приймають відповідні рішення [5], хоча згідно з ч. 3 ст. 306 КПК участь скаржника є обов'язковою. Видається, що така практика має бути усунена як така, що фактично порушує право особи на доступ до правосуддя.

У сенсі вищевикладеного вважаємо необхідним звернутися до практики ЄСПЛ, у якій зазначається, що статтею 6 Конвенції чітко не передбачено право підсудного у кримінальному провадженні особисто брати участь у судових засіданнях; це право скоріше випливає з більш загального поняття справедливого суду (див., наприклад, рішення від 12 лютого 1985 р. у справі «Колоцца проти Італії» (Colozza v. Italy), п. 27, Series A № 89) Крім того, релевантною до питання, що розглядається, є позиція ЄСПЛ, відповідно до якої стаття 6 у цілому гарантує право обвинуваченого на ефективну участь у кримінальному процесі («Муртазалієва проти Росії» (Murtazaliyeva v. Russia) [ВП], § 91). Загалом, вона включає, зокрема, не лише його або її право бути присутнім, а й право заслуховувати та спостерігати за провадженням. Такі права маються на увазі в самому понятті змагальної процедури і також можуть випливати з гарантій, які містяться в підпунктах (c), (d) і (e) пункту 3 статті 6 («Стенфорд проти Сполученого Королівства» (Stanford v. the United Kingdom), § 26) [6].

У продовження досліджуваного питання варто зазначити, що вже згадуваний проєкт Закону передбачає норму, відповідно до якої у випадку технічної неможливості участі у відеоконференції поза межами приміщення суду з використанням власних технічних засобів, *переривання зв'язку в учасника (курсив наш – Д. К.)*, участь якого є обов'язковою, суд відкладає судовий розгляд. Знову ж таки зазначена норма передбачає виключно наслідки переривання зв'язку в учасника, участь якого є обов'язкова, та не охоплює можливість переривання зв'язку в суді, що в умовах сьогодення є більш ніж ймовірним.

З урахуванням вищевикладеного вважаємо необхідним зазначити, що питання технічної неможливості участі особи у судовому розгляді з використанням власних технічних засобів неодмінно має бути унормоване. Волночас законодавцю необхідно дуже виважено підходити до унормування питання неможливості участі особи у дистанційному судовому розгляді поза межами приміщення суду з використанням власних

технічних засобів. У врегулюванні цього питання має бути неодмінно збалансовані інтереси кримінального провадження та особи. Можна висловити пропозицію щодо оголошення перерви у судовому розгляді до з'ясування можливості відновлення зв'язку, і лише за умови неможливості поновити з'єднання перенести судовий розгляд з урахуванням строків, установлених законом, на розгляд того чи іншого питання.

**Список використаних джерел**

1. Рішення Ради суддів України «Щодо вжиття невідкладних заходів для забезпечення сталого функціонування судової влади в Україні в умовах припинення повноважень ВРП та воєнного стану у зв'язку зі збройною агресією з боку рф» від 24 лютого 2022 р. URL: https://jurliga.ligazakon.net/ru/news/209874_robota-sudv-ukrani-v-umovakh-vonnogo-stanu

2. Ухвала слідчого судді Машівського районного суду Полтавської області від 22 вересня 2022 року справа № 948/665/22 URL: https://reyestr.court.gov.ua/Review/106381802; Ухвала слідчого судді Галицького районного суду м. Львова від 23 вересня 2022 року справа № 461/4871/22 URL: https://reyestr.court.gov.ua/Review/106394437

3. Висновок № 14 (2011) Консультативної ради європейських суддів до уваги Комітету міністрів Ради Європи про правосуддя та інформаційні технології (IT) URL: https://rm.coe.int/opinion-n-14–2011-on-justice-and-information-technologies-it-/16806a1fc0

4. Ухвала слідчого судді Печерського районного суду м. Києва від 14 липня 2022 року справа № 757/12521/22-к URL: https://reyestr.court.gov.ua/Review/106917208; Ухвала слідчого судді Печерського районного суду м. Києва від 20 жовтня 2022 року справа № 757/21353/22-к URL: https://reyestr.court.gov.ua/Review/107648019; Ухвала слідчого судді Шевченківського районного суду м. Києва від 4 серпня 2022 року справа № 761/11074/22 URL: https://reyestr.court.gov.ua/Review/106808449

5. Посібник зі статті 6 Конвенції – Право на справедливий суд (кримінально-процесуальний аспект) URL: https://www.echr.coe.int/Documents/Guide_Art_6_criminal_UKR.pdf

6. COLOZZA v. Italy: Judgment of the ECtHR (N 9024/80) URL: https://ips.ligazakon.net/document/VSS00999

# ПРОБЛЕМИ ВИКОРИСТАННЯ КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ, ВИЛУЧЕНОЇ З АККАУНТІВ В СОЦІАЛЬНИХ МЕРЕЖАХ

**Колеснікова Інна Анатоліївна,**
кандидат юридичних наук, асистентка кафедри криміналістики
Національного юридичного університету імені Ярослава Мудрого,
м. Харків, Україна

Глобальна діджиталізація вплинула на всі без виключення галузі права, оскільки дані, що містяться у відкритому доступі в соціальних мережах активно використовуються як докази у цивільному, господарському та кримінальному провадженнях. Криміналістика та судова експертиза не стали виключенням, оскільки перед ними постав виклик перевірки достовірності таких даних. Така перевірка має обов'язково передувати проведенню судових експертиз, об'єктом дослідження яких є цифрові фотографічні зображення.

Зі стрімким розвитком інформаційних комп'ютерних технологій більшість процесів сучасної криміналістики, з одного боку, стали простішими, але з іншого – робота експертів криміналістів суттєво ускладнилася. Так, за статистичними даними в соціальній мережі Instagram зареєстровано більше 2 мільярдів активних користувачів [1], в Facebook 1,93 мільярди користувачів [2].

Цифрові фотографічні зображення, що містяться у соціальних мережах не завжди об'єктивно та достовірно відтворюють реальність. Через застосування різноманітних ефектів фотокорекції зображень, особа, що на них відтворена, може отримати інші ознаки зовнішності, тому використання таких даних може привести до перекручення криміналістично значущої інформації.

Під час розкриття та розслідування кримінальних правопорушень фото особи вилучене з аккаунтів в соціальних мережах може бути використано наприклад для з'ясування чи зображена на обох фото одна й та сама особа (фото підозрюваного з камер відеоспостереження та фото з соціальних мереж), для встановлення особи невпізнаного трупа та інше. Суттєвою перешкодою в розкритті та розслідуванні злочинів стає редагування зовнішнього вигляду особи на фотографіях, що вилучені з аккаунтів в соціальних мережах. Так, застосування інструментів Photoshop надає можли-

вість змінити колір очей, колір волосся, замаскувати шрами, татуювання, родимки, змінити фігуру, додати або зменшити об'єм тих чи інших частин тіла, змінити риси обличчя, колір шкіри. Підтвердженням масштабного поширення цієї проблеми є рішення керівництва соціальної мережі Instagram заборонити «фільтри» (спеціальний ефект, який можна додати до фото при його публікації у вищезазначеній соціальній мережі, або при його створенні), що імітують пластичну хірургію. Ця проблема є дискусійною в криміналістичній науці вже досить давно і основні напрацювання спрямовані на виявлення змінених, відредагованих фото та недопущення їх до використання при проведенні, зокрема, портретної експертизи.

Одним із методів виявлення маніпуляцій із зображенням шляхом повторного збереження зображення на певному рівні якості, а потім обчислення різниці між рівнями стиснення є аналіз рівня помилок (error level analysis, далі ELA). Якщо зображення не змінені, квадрати 8x8 повинні мати подібні потенціали помилки [3, с. 18]. Однак, якщо зображення змінено, частина зображення, з якою маніпулювали, повинна мати більший потенціал помилки, ніж інша частина зображення. ELA працює, навмисно повторно зберігаючи зображення з відомою частотою помилок, наприклад 95%, а потім обчислюючи різницю між зображеннями.

Коли фотографія вперше зберігається у графічному форматі JPEG, він вперше стискає фотографію. Рівень стиснення може бути вибраний як розумний компроміс між розміром зображення та якістю зображення. Масштаб стиснення JPEG зазвичай становить 10:1 [4]. Більшість програм для редагування зображень, таких як Adobe Photoshop або GIMP, підтримують функцію стиснення JPEG. Тому, якщо потім зображення відкрити в Photoshop, відредагувати та знову зберегти як JPEG, воно буде знову стиснуте. З цього процесу видно, що «оригінальні» частини фотографічного зображення були стиснуті двічі, один раз – камерою, яка зробила фотографію, і ще раз – Photoshop. Тоді як «відредагована» частина фотографічного зображення була стиснута лише один раз за допомогою Photoshop. Для людського ока ми не можемо помітити різницю, дивлячись на зображення. Однак ми можемо порівняти ці два зображення разом і подивитися на відмінності.

Іншим методом перевірки оригінальності цифрового фотографічного зображення є веселковий метод. Так, Photoshop, продукти Adobe та інші виробники програмного забезпечення, такі як FilterGrade, створюють велику кількість райдужних зображень при коригуванні зображень. Модифікація зображень за допомогою комерційних інструментів, таких

як Photoshop або Gimp може призвести до створення чітких поверхонь з райдужним візерунком, які мають майже однорідне забарвлення.

Таким чином, з метою попередження виникнення перекручень криміналістично значущої інформації під час дослідження цифрових фотографічних зображень, необхідно перш за все встановити оригінальність таких зображень, зокрема, якщо вони вилучені з аккаунтів в соціальних мережах. Для цього можна ліцензовано використовувати вже розроблене програмне забезпечення. Але в такому випадку можна зіткнутись з деякими перешкодами. Незважаючи на те, що така програма може дозволити слідчим та експертам легко виявляти модифікації зображення (включаючи операції масштабування, обрізки та повторного збереження), аналіз ELA залежить від якості зображення. Робота із зображенням, отриманим у результаті численних операцій повторного збереження, є неефективною. Якщо зображення повторно зберігається багато разів, воно може мати мінімальний рівень помилки, при якому більша кількість повторних збережень не змінює зображення.

Цей метод є ефективним при виявленні змін, внесених за допомогою таких інструментів як Photoshop або Gimp. Зберігаючи зображення за допомогою цих додатків, користувачі вносять зображення більш високий потенційний рівень помилок. Недоліком є те, що ці інструменти можуть бути причиною ненавмисної модифікації. При аналізі будь-якого зображення вважається, що ELA – це лише алгоритм для аналізу зображень. Незважаючи на те, що він є ефективним у певних умовах, пропонується інтегрувати його з іншими інструментами криміналістики для отримання достовірних результатів.

**Список використаних джерел**

1. Статистика Instagram за 2022 год: интересная статистика, демография пользователей и факты. Website Rating. URL: https://www.websiterating.com/ru/research/instagram-statistics/

2. Статистика Facebook 2022: интересная статистика, демография пользователей и факты. Website Rating. URL: https://www.websiterating.com/ru/research/facebook-statistics/

3. Krawetz N. A pictures worth digital image analysis and forensics. Black Hat Briefings. 2007. P. 1–31.

4. Photo forensics: Detect photoshop manipulation with error level analysis – Infosec Resources. Infosec Resources. URL: https://resources.infosecinstitute.com/topic/error-level-analysis-detect-image-manipulation/

# КРИМІНАЛІСТИЧНІ ДОСЛІДЖЕННЯ ЦИФРОВИХ ДЖЕРЕЛ ЗВУКУ ТА ЇХ НОСІЇВ

Корнієнко Василь Володимирович,
кандидат юридичних наук, доцент кафедри криміналістики, судової експертології та домедичної підготовки факультету № 1 Харківського національного університету внутрішніх справ, м. Харків, Україна

Кримінальна подія породжує різні сліди звуку, які у своїй сукупності утворюють так звану звукову «картину». Судова акустика допомагає встановити закономірності виникнення цих джерел слідів звуку, методи й засоби їх дослідження для розслідування кримінальних правопорушень. Джерелами слідів звуку є матеріальні системи органічного і неорганічного походження (живі організми, неживі об'єкти та явища природи). Сучасна судова акустика охоплює спеціальні експертні дослідження за двома напрямками: а) технічне дослідження матеріалів та засобів звукозапису; б) дослідження голосу за фізичними параметрами усного мовлення, акустичних сигналів та середовищ. Матеріальними об'єктами-носіями слідів звуку традиційно називали фонограми (магнітні, оптичні, тощо), тоді як зараз, в епоху повного витіснення аналогового способу запису звуку цифровим, відповідно дістало змін експертна назва носія звукозапису – сигналограма, а також ускладнено перелік завдань які вирішують відповідні експертизи.

Стрімкий розвиток технологій за останні 10 років переоснастив сучасну аудіо та відео індустрію з аналогового на цифровий спосіб фіксації, зберігання та передачі інформації. Побутові пристрої стали компактніші, при цьому не втрачаючи якісні показники порівняно з професійними зразками. Разом з цим активно розвиваються чисельні програми по обробці цифрової інформації, які вносять зміни у оригінальний запис на досить високопрофесійному рівні. Це ускладнює процес встановлення ознаку внесення змін у фонограму. Наразі використовують технічні засоби для одночасної фіксації звуку й зображення, тому представлені зразки для експертних досліджень потребують комплексного аналізу.

Сучасний криміналістичний аналіз технічних засобів фіксації та матеріальних носіїв слідів звуку та зображення (відеозапису) традиційно вирішує коло ідентифікаційних та діагностичних питань:

1) на якому пристрої записана відеофонограма, за допомогою якого комплекту апаратури (одного чи кількох технічних пристроїв);

2) встановлення наявності ознак монтування, чи проводився запис відео- фонограми безперервно;

3) чи одночасно проводився запис відеозображення і звуку у відеофонограмі файлу та чи відповідає зміст відеозображення запису звуку;

4) оригіналом чи копією є відео-, фонограма.

Хотілося б звернути увагу на останній пункт. В цифрових технологіях запису звуку, на відміну від аналогового, не втрачається якість запису. Експерт, як правило, робить копіювання файлу на комп'ютер для проведення дослідження матеріальних носіїв слідів звуку та зображення. З технічної точки зору оригіналом є відео- фонограма, виконана в результаті запису сигналу безпосередньо від першоджерела (пристрою) на носій інформації (DV-касета, SD-карта пам'яті) або безпосередньо на пам'ять аудіо, відео записуючого пристрою. Під копією розуміють файл, скопійований на будь-який інший носій інформації. Якщо сигналограма (файл) є копією та зазнає відповідних змін за допомогою монтажних програм та плагінів, він також втрачає наявність мета даних та інших ознак, що ідентифікують зроблену запис з відповідним пристроєм. Тому вважаємо, що слід виключити із слідчо-судової практики постановку питання про оригінал чи копію запису, тому що в епоху цифрового запису він втратив свою актуальність. У даному випадку слідство та суд цікавить інформація про достовірність запису, чи були внесені зміни засобом монтажу. У галузі наук щодо технічного захисту інформації така процедура називається верифікацією даних.

Цифровий спосіб запису та збереження відео-, фонограм вимагає від експертів постійного вдосконалення засіб їх аналізу та дослідження. Сьогодні найбільшу складність представляє встановлення ознак монтування (вставки, видалення, накладення) звукозапису. Сучасні програми обробки аудіо та відеозапису дозволяють на високоякісному рівні робити імітації звуків та голосу, створювати необхідне середовище (імітація різних видів приміщень, фонових звуків, реверберацій), а також робити видалення та вставки/накладення окремих фрагментів запису, роблячи абсолютно непомітними «стики» фонограм. До таких програм, наприклад, відносяться Audacity чи FL Studio. Порівняно з іншими аналогами, ці програми по обробці звуку мають багато плагінів, завдяки яким можна якісно імітувати звуки широкого частотного діапазону, тональності;

створювати шуми, накладати ефекти, штучно погіршувати якість звуку, тощо. У цьому випадку ототожнення голосу, а також обстановки запису ускладнює й спосіб збереження фонограми, коли використовується алгоритм сильної компресії (Mb/sec) при збереженні фонограми після монтажу у файл.

Для ефективного проведення експертних досліджень бажано щоб записана фонограма у файл мала як найменшу компресію та кодування у форматах *.wav, *.avi, *.dv, *.mkv. Це дозволяє фахівцю якісніше проаналізувати сигналограму. Для цього використовуються традиційні методи сприйняття на слух (органолептичні), порівняння, а також із застосуванням спеціальних комп'ютерних програм автоматичної ідентифікації сигналу. Ефективним засобом аналізу звукозапису у експертній практиці також залишається спектрографічний метод. Предметом його дослідження є сонограми, на яких може бути помітно «випадіння» звуку, розбіжність або ж графічна нестиковка кривих частотної модуляції звуку. Спектрограми аудіо-сигналів надають акустичним експертам об'єктивні дані, графічно відображаючи повний звуковий спектр голосу. Горизонтальна вісь показує, в який час, а вертикальна вісь – на якій частоті протікають звукові хвилі. Кожен звук в сонограмі має свій власний зразок, тобто формат. Сукупність цих форматів і утворює акустичний відбиток голосу чи звуку і тим самим дає підґрунтя для подальшої роботи, в якій на перший план виходить тонкий слух і досвід експерта.

**Список використаних джерел**

1. Біленчук П. Д., Салтевський М. В. Судова акустика. Велика українська енциклопедія. URL: https://vue.gov.ua/Акустика судова

2. Рыбальский О. В., Близников С. А., Мыслинский А. В., Брягин О. В. Особенности проведения экспертизы аутентичности цифровых сигналограмм, полученных оперативным путем. *Захист інформації*. – К. : КМУЦА, 2005. – № 1. – С. 57–62.

# ПРОБЛЕМА ПОБУДОВИ КРИМІНАЛІСТИЧНИХ МЕТОДИК РОЗСЛІДУВАННЯ КОРУПЦІЙНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ: ІННОВАЦІЙНИЙ ПІДХІД

**Мишков Ярослав Євгенович,**
кандидат юридичних наук, молодший науковий співробітник Науково-дослідного інституту вивчення проблем злочинності ім. академіка В. В. Сташиса НАПрН України, м. Харків, Україна

У структурі корупції як соціального явища особливу небезпеку становлять корупційні кримінальні правопорушення. У кримінальному законодавстві до корупційних кримінальних правопорушень віднесено певну групу правопорушень. У примітці до ст. 45 КК України вказано, що корупційними кримінальними правопорушеннями вважаються кримінальні правопорушення, передбачені статтями 191, 262, 308, 312, 313, 320, 357, 410, у випадку їх вчинення шляхом зловживання службовим становищем, а також кримінальні правопорушення, передбачені статтями 210, 354, 364, 364–1, 365–2, 368-369-2. У КК України фактично визначено перелік корупційних правопорушень, за вчинення яких встановлено кримінальну відповідальність. При цьому, це досить різні кримінальні правопорушення, які потребують використання відмінних моделей (алгоритму дій) щодо їхнього розслідування.

Питання побудови типових криміналістичних методик розслідування корупційних кримінальних правопорушень не достатньо досліджені у вітчизняних літературних джерелах. Лише окремі автори зверталися до деяких проблем розслідування злочинів корупційної спрямованості (В. Ю. Шепітько, В. А. Журавель, 2013).

Розслідування корупційних кримінальних правопорушень має значні складнощі у співробітників органів правопорядку. Розслідування – це завжди створення певних моделей події, що відбулися, здійснення ретроспективного аналізу діяння, залучення відповідних засобів для встановлення винуватих осіб. Підхід до формування типових криміналістичних методик розслідування корупційних кримінальних правопорушень може бути розглянутий як *інноваційний*. Такий підхід дозволяє вирішувати проблемні завдання завдяки пропонуванню чітких алгоритмів дій у різних слідчих ситуаціях.

Перелік корупційних кримінальних правопорушень є доволі широким. Окремі правопорушення можуть бути пов'язані між собою і потребувати використання комплексних криміналістичних методик. Деякі правопорушення мають складний кримінальний ланцюг, що передбачає за необхідне обрання і застосування лише певних засобів. Зокрема, у криміналістичних джерелах акцентувалася увага на тому, що прийняття пропозиції, обіцянки або одержання неправомірної вигоди службовою особою та пропозиція, обіцянка або надання неправомірної вигоди службовій особі – найбільш складно доказувані види кримінальних правопорушень, які передбачають проведення комплексу організаційних, оперативних та слідчих (розшукових) дій або тактичних операцій.

Оптимізація в розслідуванні корупційних кримінальних правопорушень має за мету використання типових криміналістичних методик. Їх розроблення повинно здійснюватися із врахуванням виду кримінального правопорушення – формування видової методики. Окрім того, оскільки кримінальне правопорушення може виявлятися у вигляді злочину або кримінального проступку, то на це має бути розрахована і методика. На сьогодні відсутні типові криміналістичні методики, які б стосувалися кримінальних проступків. Важливим є й те, що типові методики розслідування корупційних кримінальних проступків повинні мати належну структуру і зміст. Суб'єктом їхнього використання є процесуальна фігура – дізнавач із наділеними повноваженнями.

У сучасних криміналістичних джерелах до структурних елементів окремих криміналістичних методик віднесено криміналістичну характеристику кримінального правопорушення, предмет розслідування, типові слідчі ситуації та версії, а також найбільш ефективні слідчі (розшукові) дії. Окремим елементом в структурі окремої криміналістичної методики є предмет розслідування – коло обставин, що підлягають з'ясуванню. Предмет розслідування визначає напрямок діяльності та порядок дій.

Таким чином, розроблення та пропонування типових криміналістичних методик розслідування корупційних кримінальних правопорушень дозволить підвищити ефективність слідчої діяльності та не допустити слідчих помилок.

# ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ДЛЯ ОПТИМІЗАЦІЇ РОЗСЛІДУВАННЯ НЕЗАКОННОЇ ПОРУБКИ ЛІСУ

**Мойсюк Катерина Олександрівна,**
аспірантка кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

В сучасних реаліях функціонування особи та світу без використання цифрових технологій стало неможливим. Роль технологій яскраво простежується і у сфері правоохоронної діяльності, у тому числі, при їх використанні для розслідування кримінальних правопорушень, зокрема незаконної порубки лісу.

Варто зазначити, що в насьогодні в Україні приділяється велика увага розвитку та вдосконаленню інноваційної діяльності, цифровим технологіям та комп'ютеризації криміналістичної техніки, криміналістичної тактики і методики. Це зумовлено тим, що для вдалого та швидкого розслідування злочинів, співробітникам органів правопорядку необхідно бути на крок попереду злочинців за забезпеченням, володінням та активним використанням сучасних науково-технічних засобів і технологій. До інноваційних криміналістичних продуктів у цьому разі можна віднести розробки в галузі криміналістичної техніки, тактики та методики розслідування злочинів, а саме: нові розроблені або прилаштовані до потреб слідчої (судової) практики технікокриміналістичні засоби, сучасні інформаційні технології, електронні бази знань, методи фіксації, аналізу та оцінки доказової інформації, нові тактичні прийоми, їх комплекси, тактичні комбінації та операції, алгоритми першочергових слідчих (розшукових) дій та перевірки типових слідчих версій, методики розслідування нових видів злочинів та ін. [2, С. 338]. Вивченням цих питань займалося багато вчених, але на конкретні інновації, що можуть бути використані під час розслідування злочину незаконної порубки лісу достатньої уваги звернуто не було в жодній з робіт.

Одним із перших прикладів використання інноваційних технологій для полегшення процесу розслідування такого злочину, як незаконна порубку лісу в Україні може бути відносно нова функціонуюча система «Ліс у смартфоні», що розміщена на сайті ДП «Лісогосподарський Інноваційно-Аналітичний Центр» (надалі ДП «ЛІАЦ»), яка надає можливість

здійснити онлайн-перевірку законності порубки лісу, за допомогою онлайн-карти, якою може скористатися будь-яка особа на своєму смартфоні, планшеті чи іншому гаджеті, для цього необхідно зайти на сайт ДП «ЛІАЦ» [6], натиснути кнопку «мапа», після цього особу буде знайдено за геолокацією. Ця геолокація підв'язується під карту лісів і під дозвільні документи на вирубку. Тобто, якщо особа бачить, що в лісі здійснюється порубка, то вона має можливість перевірити легальність її здійснення, якщо з'ясовується, що порубка здійснюється нелегально, то особа має повідомити інформацію до поліції. Тобто завдяки цьому електронному сервісу, правоохоронні органі, дізнаються про скоєння злочину з максимальною економією часу та енергетичних ресурсів. Однак, варто зазначити, що сьогодні, недивлячись на користь яку приносить цей електронній сервіс, тимчасово було вимушено прибрано мапу лісів України з сайту ДП «ЛІАС» через військове вторгнення країни агресора рф на територію України, задля уникнення її потрапляння до рук ворога. Але можливість перевірити легальність рубки залишилася завдяки вкладці «Лісові квитки».

Ще одним прикладом використання цифрових технологій під час розслідування такого злочину, як незаконна порубку лісу в Україні на практиці може бути пеленгування мобільних телефонів осіб, що знаходились поруч із місцем незаконної порубки лісу у приблизний час скоєння злочину, тобто отримання інформації у операторів та провайдерів телекомунікацій про зв'язок абонента, зміст і маршрути передавання (так звані трафіки), що несуть за собою подальші перевірки особи.

Наявність мобільного стільникового телефону, який можна назвати «радіомаяком», дозволяє визначити не тільки поточне місце розташування абонента, але і простежити його попередні переміщення в просторі.

Складовим елементом будь-якого стільникового телефону стандарту GSM є SIM-карта (Subscriber Identification H14- Module) – модуль ідентифікації абонента. Даний модуль становить собою мікрокомп'ютер у вигляді пластикової картки з незалежною пам'яттю і власним мікропроцесором, та слугує для забезпечення доступу до інформації, що зберігається в пам'яті і функції безпеки. SIM-карта встановлюється в SIM-тримач стільникового телефону, який в сучасних стільникових телефонах зазвичай розташовується під акумуляторною батаресю. Основна функція у SIM-карти – зберігання ідентифікаційної інформації про акаунт, що дозволяє абоненту міняти стільникові апарати, не змінюючи

при цьому свого облікового запису. SIM-карта призначена для ідентифікації абонента в мережі стільникового зв'язку. На SIM-карті міститься важлива інформація: ідентифікаційний GSM-номер абонента, пароль блокування клавіатури (PIN-код) та код розблокування (PUK-код), записна книжка. SIM-карта може також зберігати додаткову тиформацію; телефонну книжку абонента, списки вхідних/вихідних телефонних номерів, текст SMS-повідомлень. Крім того, SIM- карта містить мікросхему пам'яті, яка підтримує шифрування. При увімкнені в мобільну мережу номер SIM-карти так само як і номер IMEI, в автоматичному режимі передається на технічні засоби оператора зв'язку. Номер SIM-карти призначений для ідентифікації в мережі абонента, номер IMEI – телефонного апарату [1, с. 203].

Дозвіл на застосування таких заходів відповідно до п. 7 ч. 1 ст. 162 КПК надає слідчий суддя суду першої інстанції [4].

Також дієвим технологічним засобом може бути використання безпілотних літальних аппаратів (дронів), порядок застосування яких визначено в Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису [5]. Цей засіб може бути використаний безпосередньо з метою огляду великих територій (до яких відносяться ліси) або застосування методики створення 3D-моделей.

Для створення 3D-моделей придатні дані, отримані за допомогою БПЛА (зйомка значних територій та об'єктів з висоти) – може проводитися трьохмірне моделювання при огляді місця події: повна реконструкція та відтворення місця події будь-якого розміру. Збереження 3D-моделей в різних форматах дозволяє поміщати їх в графічні редактори (Autodesk 3ds Max та ін.) та проводити подальше моделювання різних ситуацій з урахуванням даних слідства та використовувати створені сцени при проведенні ситуаційних експертиз. Застосування таких моделей-копій розширює можливості, підвищує наочність і доказове значення експертиз, а методика трьохмірного моделювання не викликає особливих складнощів, оскільки використовуються цифрові фото- чи відеозйомка, зроблені з дотриманням відповідних вимог щодо режиму і умов зйомки [2, с. 12].

Отже, були розглянуті деякі аспекти цифровізації криміналістичної діяльності при розслідуванні злочинів пов'язаних з незаконною порубкою

лісу, такі як підвищення ефективності пошуково-пізнавальної діяльності слідчого з використанням цифрових технологій, ефективної організації такої діяльності та економії часу, за допомогою використання електронних сервісів, БПЛА, а також отримання інформації у операторів та провайдерів телекомунікацій про зв'язок абонента, зміст і маршрути передавання. В результаті аналізу новітніх інноваційних засобів були зроблені висновки, що поширення технологій у криміналістичній сфері сприяє подальшим змінам в області алгоритмізації та здійснення процесу розслідування злочину.

**Список використаних джерел**

1. Луцик В. Установлення місцезнаходження радіоелектронного засобу. Юридичний електронний науковий журнал. 2014. №4. С. 202–205.

2. Александренко О., Женунтій В. Інновації та цифрові технології в криміналістиці та судовій експертизі: сучасні можливості та проблеми застосування. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матеріали міжнар. «круглого столу». Харків, 2019. С. 10–14.

3. Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 338.

4. Кримінальний процесуальний кодекс України від 13.04.2012 №4651-VI URL: http://zakon5.rada.gov.ua/laws/show/4651-l7

5. Про затвердження Інструкції із застосування органами та підрозділами поліції технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, засобів фото- і кінозйомки, відеозапису: наказ МВС України від 18 грудня 2018 р. №1026. Зареєстровано в Міністерстві юстиції України 11 січня 2019 р. за №28/32999

6. ДП «Лісогосподарський Інноваційно-Аналітичний Центр». URL: https://lk.ukrforest.com

# ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ПРИ ПОКРАЩЕННІ ЯКОСТІ ФОТОЗОБРАЖЕНЬ У СУДОВІЙ ЕКСПЕРТИЗІ

**Лозовий Андрій Миколайович,**
завідувач сектору досліджень у сфері інформаційних технологій
Кіровоградського науково-дослідного експертно-криміналістичного
центру МВС України, м. Кропивницький, Україна

**Сивоконь Євген Ігорович,**
завідувач сектору досліджень у сфері інформаційних технологій
Луганського науково-дослідного експертно-криміналістичного центру
МВС України, м. Рубіжне, Україна

Поряд із стрімким розвитком наукового прогресу змінюється і концепція щодо можливостей використання його надбань як у нашому повсякденному житті, так і в професійній діяльності. Наприклад, сьогодні основа розвитку сучасних міст ґрунтується на забезпеченні комфортних та безпечних умов життя населення за допомогою інноваційних технологій. Інноваційною складовою системи розвитку та безпеки міста, безперечно, є сучасна система фото- та відеофіксації, відеокамери, які встановлюються відкритим способом у загальнодоступних громадських місцях та ведуть безперервну фіксацію і трансляцію всього, що відбувається.

Підґрунтям стрімкого розвитку сучасних систем фото- та відеофіксації у містах України в даний час є наявність в них розвинутої підсистеми «розумної» відеоаналітики, яка повною мірою адаптована під потреби безпеки та розвитку самого міста і функціонально може вирішувати безліч завдань, зокрема: аналіз ситуації на дорозі; контроль за неправильним паркуванням, що блокує транспортний потік; розпізнавання осіб, що знаходяться в розшуку; розпізнавання номерних знаків транспортних засобів; фото- та відеофіксація порушень ПДР та багато інших.

Так, згідно зі ст. 84 Кримінального процесуального кодексу України, доказами у кримінальному провадженні є фактичні дані, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для

кримінального провадження й підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів [1].

Відповідно до ст. 98 Кримінально-процесуального кодексу України речовими доказами є матеріальні об'єкти, котрі були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження, у тому числі – предмети, які були об'єктом кримінально протиправних дій, гроші, цінності та інші речі, набуті кримінально протиправним шляхом або отримані юридичною особою внаслідок вчинення кримінального правопорушення [1].

Станом на сьогодні у кримінальному провадженні події, зафіксовані за допомогою засобів фото-, відеофіксації починають набувати великого значення серед інших джерел доказів. Так, здійснення фото- та відеофіксації у громадських місцях за допомогою камер відеоспостережень, встановлених на будівлях, громадянами за допомогою мобільних телефонів, відеореєстраторів тощо, дозволяє зафіксувати певні події. Відповідно до ст. 1 Закону України «Про інформацію», інформація – це будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Таким чином, у процесі здійснення фотографування та відеозапису створюється інформація [2].

Використання фотознімку та відеозапису під час розслідування вчиненого правопорушення сприяє не лише розширенню, а й стабілізації доказової бази. Під час дослідження фотознімку або відеозапису здійснюється виконання різних завдань щодо поліпшення якості зображення або певних кадрів відеозапису, наприклад, для видалення шуму, відновлення зображень із високою роздільною здатністю із даних зображень із низьким розширенням (супер-розширення).

Покращення зображення – процес поліпшення якості картинки без втрати інформації до отримання бажаного візуального результату (дозвіл, колір і стиль) або підготовка фото для подальшого аналізу у різних програмах комп'ютерного зору: розпізнавання об'єктів, класифікації, інтерпретації зображень. Підвищення якості зображення зазвичай включає ряд перетворень: шумозаглушення, поліпшення розмитого фото, підвищення розширення, контрастності, освітлення темної фотографії, усунення оптичних спотворень тощо [3, с. 695].

Популярними фоторедакторами (наприклад, Adobe Photoshop, Adobe Lightroom або RawTherapee) пропонуються різні набори інструментів для покращення зображень. Проте, якість результату обробки сильно залежить від навичок і естетичного сприйняття ретушерів та містить суб'єктивний фактор. До того ж редагування цифрових фотознімків вручну зазвичай займає багато часу. Тому для прискорення виконання покращення фотозображень та окремих кадрів відеозаписів використовуються методи автоматичної обробки на основі штучного інтелекту.

Сучасні сервіси для автокорекції фотозображень значно полегшують і спрощують процес покращення для всіх користувачів. Фоторедактори на основі штучного інтелекту роблять все те саме, що ретушер б робив вручну у фотошопі, і в той же час дозволяють оператору повністю керувати процесом. Автоматична ретуш допомагає: надати знімкам, зробленим на просту камеру, професійний вигляд і поліпшити якість зображення; економити час, дозволяючи програмі автоматично виконувати всю роботу замість ручного редагування; друкованим і видавничим компаніям – поліпшити процес корекції зображень для журналів, маркетингових кампаній і не тільки [4, с. 149].

Різні типи нейронних мереж можна використовувати для вирішення різних завдань щодо поліпшення якості зображення, наприклад, для видалення шуму, відновлення зображень із високою роздільною здатністю з даних зображень із низьким розширенням (супер-розширення). Розглянемо основні засоби, які можливо використовувати для покращення фотознімків та окремих кадрів відеозаписів [5, с. 86]:

1. Deep Photo Enhancer використовує GAN (Generative Adversarial Networks – генеративно-змагальні нейронні мережі) і непарні алгоритми навчання. Deep Photo Enhancer пропонує метод поліпшення зображень на основі вивчення фотографій. Нейрони навчаються знаходити загальні характеристики в наборі зразків зображень (наприклад, рівень контрастності, баланс білого, колірна гамма) і потім застосовувати ці характеристики до поліпшеного зображення так, щоб зберігався сенс оригінальної картинки. Цей метод вимагає використання вихідних зображень високої якості, і його можна у подальшому персоналізувати.

2. Супер-розширення фото з використання Neural Enhance. Алгоритми глибокого навчання дозволяють навчити нейронну мережу збільшувати зображення в 2 або навіть 4 рази, що дозволяє підвищити якість знімків із низьким розширенням. Глибокі нейронні мережі (GAN, гли-

бокі рекурсивні згорткові нейронні мережі (DRCN)) здатні відновлювати фотореалістичні текстури із зображень із дуже низьким розширенням: нейронна мережа «домальовує» деталі за результатами навчання на прикладах зображень.

3. IBM/MAX Image Resolution Enhancer – нейронна мережа для відновлення стислих фотозображень. Ця модель, що розгортується, дозволяє збільшувати розмір пікселізованого зображення в 4 рази, одночасно генеруючи фотореалістичні деталі, використовуючи GAN (SRGAN-tensorflow). Ідеальним вхідним зображенням повинен бути PNG-файл розміром від 100x100 до 500x500 пікселів, бажано без постобробки. Модель може генерувати деталі з 57 пікселізованого зображення, але вона не підходить для корекції розмитих зображень.

4. Deep Image – програмне забезпечення для збільшення розширення зображення на основі штучного інтелекту, що використовує нейронні мережі (CNN і GAN) для видалення JPG артефактів і зворотного перетворення зображення, відновлення його майже до вихідного якості. Програма також дозволяє збільшити розширення і розмір картинки в 2 і 4 рази: нейронна мережа розраховує, як має виглядати збільшене зображення, щоб зберегти його якість.

Отже засоби автоматичної обробки зображень на основі штучного інтелекту, що використовують нейронні мережі, можуть допомогти у розробці інтелектуальних додатків, впровадженні елементів комп'ютерного зору, виявленні та розпізнаванні об'єктів і дій на зображеннях і відеозаписах.

Питання застосування можливостей штучного інтелекту при проведенні судової експертизи є актуальним та потребує не тільки подальшого ґрунтовного наукового дослідження, а й законодавчого закріплення та методичного забезпечення.

**Список використаної літератури**

1. Кримінальний процесуальний кодекс України// Відомості Верховної Ради України: кодекс від 13.04.2012, редакція від 17.03.2021. URL: http://zakon3.rada.gov.ua/laws/show/4651–17

2. Про інформацію: Закон України від 16.07.2020. URL: http://zakon4.rada.gov.ua/laws/show/2657–12

3. Садыхов Р. Х., Дудкин А. А. Обработка изображений и идентификация объектов в системах технического зрения. Искусственный интеллект. 2006. №3. С. 694–703.

4. Хуанг Т. С., Эклуид Дж.-О., Нуссбауыер Г. Дж. и др. Быстрые алгоритмы в цифровой обработке изображений. Пер. с англ.; под ред. Т. С. Хуанга.: М.: Радио и связь, 1984. 224 с.

5. Кожем'яко В. П., Павлов С. В., Станчук К. І. Оптико-електронні методи і засоби для обробки та аналізу біомедичних зображень: (монографія). Вінниця: УНІВЕРСУМ-Вінниця, 2016. 203 с.

# ПРОЦЕСУАЛЬНА РЕГЛАМЕНТАЦІЯ НАДАННЯ ПОЯСНЕНЬ СПЕЦІАЛІСТОМ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ (КІБЕРЗЛОЧИНІВ)

**Неділько Ярослав Валентинович,**
аспірант кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка, м. Київ, Україна

Успіх досудового розслідування кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій (кіберзлочинів), обумовлений ефективним збиранням та дослідженням так званих «електронних слідів», що передбачає використання спеціальних знань. Однією з форм використання спеціальних знань є участь спеціаліста під час проведення окремих процесуальних дій.

Аналіз ст. 71 КПК України дозволяє виділити дві допоміжні функції спеціаліста у кримінальному провадженні: 1) надання безпосередньої технічної допомоги (фотографування, складання планів, схем тощо; 2) надання консультацій, довідок, висновків та пояснень, що потребують спеціальних знань і навичок [2, с. 43].

Дискусійним питанням визнається надання спеціалістом пояснення, оскільки на практиці використовується переважно саме такий вид спілкування слідчого, дізнавача, прокурора зі спеціалістом. Законодавчо не визначено, у якій формі усно чи письмово повинні надаватися пояснення спеціалісти під час досудового розслідування. З урахуванням специфіки кримінальних правопорушень, що вчиняються з використанням інформаційних комп'ютерних технологій (кіберзлочинів) доцільно використовувати пояснення спеціаліста у письмовій формі.

З огляду на вітчизняні криміналістичні дослідження [3], [4], [5], можна виокремити наступні тактичні рекомендації, якими необхідно користуватися при залученні спеціаліста під час розслідування зазначеної категорій кримінальних правопорушень: 1) пропонувати спеціалісту писати письмове пояснення власноруч з метою уникнення неправильного

розуміння термінології слів та забезпечення логічного й послідовного викладення фактів, що мають значення для розслідування; 2) не обмежувати спеціаліста у формі та обсязі письмового пояснення. Це забезпечить повне та всебічне відображення результатів застосування ним спеціальних знань та навичок та дозволить отримати професійне пояснення щодо певних процесів, виявлення електронних слідів, їх аналіз у зв'язку з подією, що розслідується; 3) до протоколу відповідної процесуальної дії необхідно долучати письмове пояснення спеціаліста щодо: методів та технічних засобів, що він застосував, його думки щодо виявлення, вилучення, копіювання та збереження електронних слідів, інших матеріальних об'єктів, пов'язаних з подією кримінального правопорушення.

Письмове пояснення спеціаліста долучається як додаток до протоколу, це передбачено п. 2 ч. 2 ст. 105 КПК України, і повинно відповідати загальним вимогам оформлення додатків (ч. 3 ст. 105 КПК України).

Не варто нехтувати і усними поясненнями спеціаліста. Значення усних пояснень під час проведення процесуальних дій полягає в тому, що слідчий оперативно отримує кваліфіковану допомогу із спеціальних питань, що допомагають оцінити електронні докази, своєчасно вирішити питання про призначення відповідної експертизи, визначити коло питань, адресованих експертові [2, 45–46]. Не можна оминути висловлені в науковій літературі думки вчених з приводу того, чи є письмове пояснення спеціаліста джерелом доказу. У ч. 2 ст. 84 КПК України пояснення спеціаліста як джерело доказу відсутнє; письмові пояснення спеціаліста як додатки до протоколів відсутні і в ч. 2 ст. 99 КПК України.

Разом з тим, привертає на себе увагу ст. 298–1 КПК України «Процесуальні джерела доказів у кримінальних провадженнях про кримінальні проступки», у якій визначено, що процесуальними джерелами доказів у кримінальному провадженні про кримінальні проступки, крім визначених ст. 84 КПК України, також є, зокрема, пояснення осіб, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису. Водночас наведені процесуальні джерела доказів не можуть бути використані у кримінальному провадженні *щодо злочину*. Але на підставі ухвали слідчого судді, винесеної за клопотанням прокурора, пояснення осіб, висновок спеціаліста, показання технічних приладів і технічних засобів, що мають функції фото- і кінозйомки, відеозапису, чи засобів фото- і кінозйомки, відеозапису можуть бути використані як

процесуальні джерела доказів у кримінальному провадження щодо злочину (абз. 2 ч. 1 ст. 298–1 КПК України). Варто звернути увагу, що у вищенаведеній статті акцентується увага на поясненні осіб, а *не на поясненні спеціаліста* як процесуальному джерелу доказів. У зв'язку з цим постає питання: чи можна до пояснення осіб відносити і пояснення спеціаліста? Відповідаючи на дане питання, звернемося до ч. 8 ст. 95 КПК України, у якій зазначено, що сторони кримінального провадження, потерпілий, представник юридичної особи, щодо якої здійснюється провадження, мають право отримувати від учасників кримінального провадження та інших осіб за їх згодою пояснення. Спеціаліст згідно до п. 25 ч. 1 ст. 3 КПК України відноситься до учасників кримінального провадження. Тобто термін «пояснення осіб» у положеннях ст. 298–1 КПК України охоплює і пояснення спеціаліста. Таким чином, законодавець пояснення спеціаліста відносить до джерел доказів.

Підтвердженням цього є положення Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події, в якій зазначено, що при виготовленні оригіналу документа в електронній формі (його відображення) після завершення огляду місця події *спеціалістом* за дорученням слідчого у довільній формі *складається письмове пояснення*, у якому зазначаються дата проведення процесуальної дії, дата виготовлення документа (відображення), номер та/або параметри технічних носіїв інформації, а також прізвище особи, яка виготовила копію запису. Письмове пояснення та відображення запису процесуальної дії приєднуються як додатки до протоколу [6].

Враховуючи специфіку розслідування зазначених кримінальних правопорушень, пояснення спеціаліста варто використовувати до внесення відомостей до ЄРДР. Це сприятиме встановленню обставин, що можуть свідчити про вчинення кримінального правопорушення, а також слугувати підґрунтям для прийняття рішення про початок досудового розслідування. Вбачається за доцільне використовувати пояснення спеціаліста і на наступних етапах розслідування.

**Список використаних джерел**

1. Щербаковський, М. Г. Консультаційна функція спеціаліста у кримінальному провадженні. *Криміналістика і судова експертиза*. Київ, 2017. Вип. 62. С. 43–51.

2. Антонюк П. Є. Щодо сутності письмового пояснення спеціаліста у кримінальному провадженні. Актуальні питання судової експертології, криміналістики та кримінального процесу: матеріали II міжнар. наук.-практ. конф. (м. Київ, 19 листопада 2020 р.). Київ, 2020. С. 47–50.

3. Щербаковський М. Г. Консультаційна функція спеціаліста у кримінальному провадженні. *Криміналістика і судова експертиза*. Київ, 2017. Вип. 62. С. 43–51.

4. Чигрина Г. Л. Електронні документи: залучення спеціаліста до збирання та використання під час кримінального провадження. *Jurnalul Juridic naţional: Teorie şi Practică*, (3), С. 134–137.

5. 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, затверджена Наказом Міністерства внутрішніх справ України 03.11.2015 № 1339. URL: https://zakon.rada.gov.ua/laws/show/z1392-15#Text

# СПЕЦІАЛЬНІ ІНФОРМАЦІЙНІ ОПЕРАЦІЇ ЯК ЕЛЕМЕНТ ГІБРИДНОЇ ВІЙНИ ТА СУЧАСНІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

**Нетеса Наталія Володимирівна,**
кандидат юридичних наук,
вчений секретар Науково-дослідного
інституту вивчення проблем злочинності імені академіка
В. В. Сташиса НАПрН України, м. Харків, Україна

**Мокляк Володимир Вікторович,**
кандидат юридичних наук, полковник СБУ,
Служба безпеки України, м. Київ, Україна

Технології гібридної війни, окрім власне збройної агресії, включають різноманітні моделі й механізми втручання в інформаційний простір, одним із найнебезпечніших проявів якого є цілеспрямоване маніпулювання громадською думкою із застосуванням технологій інформаційно-психологічного впливу [3, с. 116]. Основним компонентом такого інформаційного впливу є спеціальні інформаційні операції, які можуть бути визначені як комплекс взаємозалежних гласних та негласних заходів, об'єднаних єдиним оперативним задумом, змістом яких є приховане керування процесами інформаційної сфери супротивника (шляхом впливу на інформацію, інформаційні системи та інформаційну інфраструктуру) з одночасним посиленням забезпечення безпеки власної інформаційної сфери, кінцевою метою яких є маніпулювання масами на рівні суспільної та індивідуальної свідомості. Як зазначається в Стратегії інформаційної безпеки, такі спеціальні інформаційні операції становлять загрозу національній безпеці України і спрямовані, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини [4].

Спеціальні інформаційні операції, що проводяться спецслужбами рф проти України, мають одразу декілька векторів спрямування: інформа-

ційний простір України, а також інших країн світу та міжнародних організацій (так звані зовнішні спецоперації), інформаційний простір рф (внутрішні спецоперації) та інформаційний простір анексованих та окупованих територій.

Щодо різновиду *зовнішніх* спецоперацій інформаційного впливу, що здійснюються супротивником в *інфопросторі України*, то вони здебільшого спрямовані на: підрив національної безпеки України, її національних інтересів, ліквідацію української державності та знищення української ідентичності, провокування проявів сепаратизму, екстремізму, тероризму, поширення панічних настроїв у суспільстві, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації в Україні тощо.

Дещо інші завдання ставляться перед *зовнішніми* інформаційними операціями проти України, що здійснюються в *інформаційному просторі зарубіжних країн* (та міжнародних організацій), які спрямовані на: легітимізацію спроби анексії Автономної Республіки Крим та міста Севастополя, заперечення участі рф у війні на території Донецької та Луганської областей та обвинувачення української влади та збройних сил у провокаціях збройної агресії, посилення адвокаційної кампанії за зняття санкцій, запроваджених у зв'язку з порушенням рф суверенітету й територіальної цілісності України. Причому такі спеціальні інформаційні операції стосуються як дружніх супротивнику країн, так і тих, які налаштовані нейтрально чи навіть вороже [2, с. 82] стосовно рф. Наприклад, щодо країн, які надають військову допомогу Україні, застосовуються інформаційні спецоперації, змістом яких є дискредитація українського військово-політичного керівництва та ЗСУ, які начебто не здатні опанувати надану військову зброю і швидко її втрачають на полі бою, з одночасним демонструванням власної «могутності» та можливості завдання удару у відповідь у разі, наприклад, втручання в конфлікт та застосування ядерної зброї (тактичної чи стратегічної).

*Внутрішні* спеціальні інформаційні операції передбачають інформаційний вплив на власне населення рф і спрямовані на: інспірування ідей про можливий наступ США та НАТО з боку українських територій з метою посіяти паніку серед населення рф; мобілізацію бойового духа власних громадян та отримання підтримки широких верств населення шляхом демонстрації нібито досягнутих здобутків «визвільної» спецоперації в Україні та виправдовування в їх очах збройного вторгнення на

територію суверенної України, зокрема, нібито боротьбою з фашизмом; укріплення духу патріотизму; придушення будь-яких опозиційних та протестних настроїв; навіювання остраху суворого покарання за ухилення від мобілізації.

Як окремий різновид можна виокремити й *спеціальні інформаційні операції на незаконно анексованих та тимчасово окупованих українських територіях,* де поєднуються засоби й методи зовнішнього та внутрішнього інформаційного впливу. Вони мають своїм спрямуванням поширення серед їх населення сепаратистських, автономістських, екстремістських та терористичних настроїв, навіювання думки про звільнення цих територій від українських фашистів та необхідність долучення до збройного протистояння ЗСУ заради утвердження нібито соціальної та історичної справедливості.

Звісно, що в умовах гібридної війни рф проти України всі ці спецоперації застосовуються паралельно. При цьому за характером здійснення їх прийнято поділяти на *інформаційно-технічні*, що передбачають вплив на функціонування інформаційно-технічного середовища суспільства (інформаційно-комунікаційні системи та мережі) та *інформаційно-психологічні,* що передбачають вплив на функціонування й розвиток інформаційно-психологічного середовища суспільства, психіку й поведінку окремих осіб та їх груп [1, с. 129]. Окрім названих, на виокремлення у самостійну групу, на наше переконання, заслуговують так звані *комбіновані* спеціальні інформаційні операції, за яких через вплив на інформаційно-комунікаційні системи та мережі здійснюється вплив на інформаційно-психологічне середовище. Саме такі інформаційні спецоперації, що базуються на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій [5], є найбільш поширеними у вік бурхливого розвитку інформаційно-комунікаційних технологій, що зумовлено їх порівняно невеликою вартістю, можливістю робити це дистанційно та масштабно, а також з огляду на наявність практичного досвіду спецслужб рф з їх реалізації, що дозволяє забезпечити довготривалий ефект без активного втручання.

Способи здійснення таких операцій є різноманітними: від проведення кібератак, використання можливостей соціальних мереж («ВКонтакте», «Одноклассники», «Facebook», «Instagram», «Twitter») та мессенджерів («Viber», «Telegram», «WhatsApp» та ін.), створення спеціальних блог-платформ та інформаційних майданчиків, розсилання фішингових

листів та SMS-повідомлень на персональні електронні пристрої до розміщення реклами та користування послугами SMM/SEO-маркетингу для просування інформації з деструктивним контентом у пошукових системах та соціальних мережах з метою нарощування їх рейтинговості та значимості в інформаційному просторі.

Найпоширенішими формами та методами проведення спеціальних інформаційних операцій впливу у кіберпросторі є: злам спеціалізованих баз даних для подальшого здійснення контрольованого витоку «чутливої» інформації, яка, будучи вирваною з контексту, може спровокувати/поглибити розбіжності у поглядах населення та призвести до його розділення (т.зв. «Hack-and-Leak-atack»); злам медійних вебсайтів для подальшого розміщення на них інформації впливу та її поширення через численні інтернет-платформи (у тому числі російськомовні медійні вебсайти, інтернет-форуми, блоги тощо); DDoS-атаки (виведення сайту з ладу шляхом його перевантаження), які спрямовуються проти урядового сектора та ЗМІ і таким чином перешкоджають доступу населення до офіційних даних (активно використовувались противником у період 24–28 лютого 2022 року під час широкомасштабного вторгнення до України); злам вебсайтів або інформаційних систем провайдерів інтернет-послуг для подальшого розміщення текстів, зображень, відео- та аудіо інформації загрозливого змісту тощо.

Щодо напрямів здійснення спеціальних інформаційних операцій у соцмережах та мессенджерах, то найбільшого розповсюдження набули ті, що спрямовані на: збір та передавання даних про військові об'єкти, об'єкти критичної інфраструктури (зокрема в частині проведення та подальшого підтвердження результатів ракетних атак на них), розташування логістичних вузлів, обсягів та видів наданої Україні партнерами військової допомоги та ін.; розміщення та поширення матеріалів деструктивного та антидержавного характеру; поширення закликів до повалення конституційного ладу або посягань на територіальну цілісність України; фінансування терористичної та іншої кримінально протиправної діяльності; публічне обговорення питань, які провокують панічні настрої, загострюють соціальні протиріччя, викривляють погляди на перебіг бойових дій на окремих територіях України.

**Список використаних джерел**

1. Верголяс О. О. Інформаційно-правове забезпечення спеціальних інформаційних операцій. *Інформація і право*. 2018. №4(27). С. 126–133.

2. Когут Ю. І. Кібервійни, кібертероризм, кіберзлочинність (концепції, стратегії, технології): практ. посіб. Київ: Консалт. компанія «СІДКОН»; ВД «Дакор», 2022. 284 с.

3. Новицький В. Я. Стратегічні засади забезпечення інформаційної безпеки в сучасних умовах. *Інформація і право*. 2022. № 1(40). С. 111–118.

4. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року «Про Стратегію інформаційної безпеки»: Указ Президента України від 28.12.2021 р. № 685/2021. URL: https://www.president.gov.ua/documents/6852021–41069

5. Про рішення Ради безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

# ВИКОРИСТАННЯ ДАНИХ АВТОМАТИЗОВАНОЇ СИСТЕМИ ВІДСТЕЖЕННЯ В ОБІГУ ЛІКАРСЬКИХ ЗАСОБІВ З ВИКОРИСТАННЯМ МАРКУВАННЯ (КОДИФІКАЦІЇ) ТА ІДЕНТИФІКАЦІЇ ПРИ РОЗСЛІДУВАННІ ФАКТІВ ФАЛЬСИФІКАЦІЇ ЛІКАРСЬКИХ ЗАСОБІВ АБО ОБІГУ ФАЛЬСИФІКОВАНИХ ЛІКАРСЬКИХ ЗАСОБІВ

**Нога Петро Петрович,**
асистент кафедри цивільного, господарського і фінансового права Полтавського юридичного інституту Національного юридичного університету імені Ярослава Мудрого, молодший науковий співробітник Лабораторії дослідження проблем національної безпеки у сфері громадського здоров'я Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

Директива 2011/62/EU (Директива Європейського Парламенту №2011/62/ЄС з метою внесення поправок у Директиву №2001/83/ЄС у питаннях забезпечення безпеки лікарських засобів та запобігання їх фальсифікації) була прийнята в 2011 році з метою зменшення фальсифікованої продукції на фармацевтичному ринку. Всі країни-члени ЄС мали до 2019 року уніфікувати власне законодавство та дистриб'юторську практику у відповідності до вимог цього нормативного акту [1]. Україна запровадила пілотний проект щодо створення автоматизованої системи відстеження в обігу лікарських засобів від виробника до кінцевого споживача з використанням маркування (кодифікації) та ідентифікації з 24.10.2017 року в кількох областях України [2]. Нові вимоги передбачають, що захист від фальсифікації здійснюється шляхом нанесення на упаковку лікарських засобів спеціального унікального номера, що дозволить відрізнити фальсифікат від оригінального препарату, так як унікальний номер кожної упаковки можна в будь-який момент перевірити за спеціальною базою даних. При цьому використовуються 2-D штрих-коди, які розроблені для кодування великого обсягу інформації. Розшифровка такого коду проводиться в двох вимірах (по горизонталі і по вертикалі). Використовується вид такого коду під назвою Data Matrix. Передбачається, що унікальним ідентифікатором повинні бути промар-

ковані виробники всіх рецептурних препаратів, зареєстрованих у країні, і деяких безрецептурних лікарських засобів (індивідуалізація кожної упаковки), а отже передбачається створення бази даних обігу лікарських засобів від виробника до кінцевого споживача [1].

У системі органів державної виконавчої влади функціонує Державна служба України з лікарських засобів та контролю за наркотиками (далі – Держлікслужба), основним завданням якої є реалізація державної політики у сферах контролю якості та безпеки лікарських засобів, а отже Держлікслужба може стати держателем бази даних обігу лікарських засобів в контексті створення автоматизованої системи відстеження в обігу лікарських засобів від виробника до кінцевого споживача з використанням маркування (кодифікації) та ідентифікації GS1. Після створення такої бази даних, інформація із неї може бути використана як доказ фальсифікації лікарського засобу чи факту обігу таких ліків у кримінальному провадженні. Для сприйняття такої інформації необхідно використати програмно-технічні засоби, вона може копіюватися, переміщатися, зберігатися тощо без втрати головних характеристик, може створюватися не лише людиною (користувачем), а й інформаційною системою (трафік зв'язку, файли реєстрації тощо), зміст інформації не завжди має класичну форму сприйняття, а й у вигляді коду, модулів, баз даних тощо, мають властивості як ідеальних слідів злочину так і речових, поняття «копія» та «оригінал» до них не може застосовуватися, динамічність, складеність із низки послідовних окремих частин (бази даних) дають змогу вести мову про їх особливу природу, а отже необхідність виокремлення в окрему групу джерел доказів.

На сьогодні у кримінальному процесі (на противагу цивільному, господарському і адміністративному) простежується дефіцит нормативного регулювання субінституту цифрових (віртуальних) доказів. Така тенденція не відповідає загальним реаліям, за якими у значній частині судових засідань відбувається дослідження цифрових (віртуальних) доказів. З огляду на зазначене існує необхідність у ліквідації законодавчої прогалини стосовно використання цифрових доказів як джерела доказів у кримінальному процесі шляхом визначення порядку їх отримання, зберігання, оцінки, дослідження у судовому засіданні. Законодавча регламентація субінституту цифрових доказів має відбуватися на рівні КПК України, а не спеціального закону, як пропонується деякими дослідниками (з огляду на те, що ст. 1 КПК України визначає, що провадження

здійснюється виключно на підставі КПК України). Відповідно до даних Офісу Генерального прокурора в період з 2013 по 2020 рр. в Україні зареєстровано 256 кримінальних проваджень за статтею 321–1 КК України за фактом фальсифікації лікарських засобів та їх обігу. У той же час, направлено до суду із обвинувальними актами лише 36 кримінальних проваджень [3]. У свою чергу, із 2013 по серпень 2021 рр. судами І інстанції постановлено 30 вироків, з яких 2 вироки є виправдувальними (вирок Приморського районного суду м. Одеси від 28 грудня 2015 р. у справі № 522/14195/15-к [4] та вирок Лубенського міськрайонного суду Полтавської області від 21 лютого 2018 р. у справі № 539/1590/15-к [5]), а решта 28 – обвинувальними [3]. Незважаючи на кількість повідомлень про те, що правоохоронними органами були виявлені особи, які займаються випуском в обіг фальсифікованих лікарських засобів, лише одиниці із підозрюваних у вчиненні злочину, передбаченого ст. 321–1 КК України, постають перед судом. Аналіз обвинувальних вироків, постановлених судами по ст. 321–1 КК України в період з 2013 по серпень 2021 р. в частині встановлення предмету цього злочину свідчить про те, що починаючи з 2016 р. до кримінальної відповідальності притягуються переважно особи, які вчиняли фальсифікацію медичного спирта або дезінфікуючих засобів [3]. Проте повідомлення у ЗМІ свідчать про те, що виявляються й особи, які фальсифікують й інші лікарські засоби (проти онкологічних, ендокринних, серцево-судинних певних інфекційних та інших небезпечних для життя пацієнта захворювань). Разом із тим, в Єдиному державному реєстрі судових рішень відповідні вироки відсутні, що може бути свідченням того, що кримінальні провадження по таким справам не доходять до суду з обвинувальними актами і закриваються на стадії досудового розслідування. Така ситуація свідчить про фактичну безкарність тих фальсифікаторів, які є «торговцями смертю», збуваючи пацієнтам, захворювання яких є небезпечним для життя, підроблені ліки. В жодному із вироків, які розміщені в Єдиному державному реєстрі судових рішень, не було притягнуто до відповідальності осіб, які поставляли фальсифіковані лікарські засоби або активний фармацевтичний інгредієнт для їх виготовлення. В усіх вироках зазначалось, що засуджений придбав відповідні предмети у невстановленої слідством особи. Це свідчить про те, що організатори злочинів та реальні канали поставки в Україну фальсифікованих лікарських засобів правоохоронними органами не виявляються, а до кримінальної відповідаль-

ності притягуються лише окремі виконавці [3]. Така ситуація свідчить про те, що надсуворі санкції, передбачені ст. 321–1 КК України, лишаються декларативними, оскільки судами не застосовуються. Таким чином, ми можемо зробити наступні висновки: а) Україна по завершенню війни має створити автоматизовану систему відстеження в обігу лікарських засобів від виробника до кінцевого споживача з використанням маркування (кодифікації) та ідентифікації з метою протидії обігу фальсифікату на фармацевтичному ринку; б) інформація з цієї системи (бази даних) може бути доказом факту обігу фальсифікованих лікарських засобів, яка за своєю суттю є електронною (цифровою, віртуальною); в) процедура дослідження електронних доказів у кримінальному провадженні потребує суттєвого вдосконалення, а також подальшого розвитку і нарощування ефективності (зокрема в аспекті роз'яснення що таке оригінал та копія цифрових доказів, порядку дослідження таких доказів тощо); г) аналіз практики притягнення до кримінальної відповідальності за ст. 321–1 КК України свідчить про недоліки саме правозастосовної діяльності, а не про недоліки законодавства, і навіть запровадження нових технологій виявлення та відстеження фальсифікату не стане запорукою успішної протидії цьому явищу.

**Список використаних джерел**

1. Directive 2011/62/EU of the European Parliament and of the Council. *Official Journal of the European Union*. 2011. C. 74–87.

2. Питання оптимізації діяльності територіальних органів Державної служби України з лікарських засобів та контролю за наркотиками: Проект постанови Кабінету Міністрів України. URL: http://www.apteka.ua/article/436973.

3. Статистика – Офіс Генерального прокурора. Офіційний сайт. URL: https://www.gp.gov.ua/ua/1stat

4. Вирок Приморського районного суду м. Одеси від 28 грудня 2015 р., справа № 522/14195/15-к (провадження № 1-кп/522/847/15) URL: http://reyestr.court.gov.ua/Review/54720617

5. Вирок Лубенського міськрайонного суду Полтавської області від 21 лютого 2018 р., справа № 539/1590/15-к (провадження № 11-кп/814/43/21) URL: http://reyestr.court.gov.ua/Review/72368054#

# ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ ПРИ ВПРОВАДЖЕННІ АЛГОРИТМІВ СЛІДЧИХ ДІЙ

**Соколенко Микита Олександрович,**
молодший науковий співробітник лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса
НАПрН України, м. Харків, Україна

На сьогоднішній день однією з найважливіших передумов підвищення ефективності розслідування кримінальних правопорушень є активне впровадження в практику діяльності органів досудового розслідування сучасних досягнень науки і техніки, зокрема цифрових технологій. Одним із перспективних напрямів оптимізації слідчої діяльності необхідно визнати можливість запровадження кібернетичних підходів і пов'язаних з цим перспектив використання комп'ютерної техніки шляхом побудови і застосування відповідних алгоритмів, зокрема слідчих дій. Саме алгоритми здатні істотно скоротити витрати часу для підготовки і проведення слідчої дії, надати цьому процесу більшої керованості, оскільки слідчий, спираючись на розроблені в науці алгоритми, має можливість в тих випадках, коли є готові оптимальні рішення не займатися їх винаходом, а брати і використовувати вже готові.

Впровадження алгоритмів слідчих дій на базі сучасних комп'ютерних технологій передбачає застосування максимально повної варіативності зазначених даних. Наприклад, алгоритми допиту мають стосуватися наступних категорій свідків: очевидців кримінальної події; підозрюваних або потерпілих; обізнаних осіб, що використовували свої знання в ході кримінального провадження (спеціалісти); осіб, що залучалися до провадження окремих слідчих (розшукових) дій (поняті, співробітники оперативних підрозділів). Допит зазначених осіб відрізняється не лише предметом, тобто колом питань, які необхідно з'ясувати у допитуваного, а й тактикою провадження.

Алгоритми слідчих дій кожного з учасників кримінального провадження будується на основі виокремлення максимально вичерпного переліку типових ситуацій і надання до кожної з них відповідних завдань та засобів їх розв'язання. При цьому треба враховувати, що стовідсотко-

во побудувати алгоритми до всіх ситуацій, що виникають на практиці, неможливо. Завжди будуть залишатися такі ситуації, що виникають непередбачувано і до яких алгоритми слідчих дій відсутні, тобто йдеться про обмеженість алгоритмізації.

Разом з цим, застосування алгоритмів слідчих дій засобами комп'ютерної техніки можливе за рахунок створення відповідного програмного забезпечення. Це можуть бути спеціально розроблені програми або відповідні блоки в системі автоматизованого робочого місця (АРМ) слідчого, який розглядається як комплекс програмно-технічних засобів інформаційної підтримки прийняття рішень слідчим. Наприклад, щодо такої слідчої дії як допит до цих блоків мають входити такі складові: алгоритми допиту всіх передбачених чинним кримінальним процесуальним законодавством учасників кримінального провадження; алгоритми допиту в конфліктних ситуаціях; алгоритми викриття неправдивих показань; алгоритми спростування необґрунтованого посилання на алібі; алгоритми припинення обмови або самообмови; алгоритми актуалізації у пам'яті допитуваного забутих фактів; алгоритми допиту потерпілого з елементами віктимної поведінки; алгоритми встановлення психологічного контакту з допитуваним та інші.

Комп'ютерна програма являє собою формалізований запис алгоритмів та складається з набору символів, синтаксичних правил і семантичних визначень. При цьому, мова програмування, що використовується в обчислювальній техніці, не зовсім придатна для опису алгоритмів слідчих дій, які мають певну специфіку. Тому розроблення чітко визначених (формалізованих) термінів є необхідною умовою створення алгоритмів слідчих дій і ще одним спільним напрямом діяльності математиків-програмістів і криміналістів.

Виходячи з вищевикладеного необхідно зазначити, що однією з причин недостатнього використання сучасних цифрових технологій, поряд із низьким технічним забезпеченням органів досудового розслідування, є недостатня координація розробок відповідних алгоритмів і програм, а також відсутність рекомендацій використання в роботі слідчих автоматизованих інформаційних систем. Тому, більш активне використання засобів комп'ютерних технологій, зокрема, спеціалізованого програмного забезпечення, яке б мало вигляд навчальної програми для слідчих, може допомогти слідчим продуктивно користуватись узагальненими знаннями, прийомами, зменшити кількість помилок і упущень. На тепе-

рішній час існує тенденція збільшення кількості комп'ютерних операцій, що входять до структури вирішення криміналістичних завдань і, безперечно, у зв'язку з цим виникають багато проблем методологічного, криміналістичного та організаційного характеру, що потребують подальшого дослідження.

# ЗНАЧЕННЯ «ІНЕТЕРНЕТУ РЕЧЕЙ» У РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

**Чорноус Юлія Миколаївна,**
доктор юридичних наук, професор, професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ, м. Київ, Україна

**Козицька Олена Геннадіївна,**
кандидат юридичних наук, доцент, заступник начальника відділу поліції № 3 – начальник сектору кримінальної поліції Хмельницького районного управління поліції ГУНП в Хмельницькій області, м. Хмельницький, Україна

Сучасний світ неможливо уявити без функціонування різноманітних інноваційних пристроїв та технологій, більшість з яких з'явилося протягом останніх десятиліть. Наразі практично у всіх сферах суспільного життя використовуються електронно-цифрові пристрої, котрі приєднані до мережі Інтернет та взаємодіють між собою, а також генерують надвеликі масиви цифрової інформації, що дозволяє говорити про виникнення Інтернету речей, складовою частиною якого є такі пристрої, як мобільні телефони, навігатори, цифрові відеокамери, дрони, «розумні» годинники, телевізори тощо, а також технології «розумних» будинків та навіть «розумних» міст.

Загалом, реальне впровадження Інтернету речей слід розглядати як: черговий етап розвитку інформаційного суспільства; перехід від глобальної інформатизації до глобальної механізації, автоматизації та роботизації; механізм, інструментарій переходу «інформаційного суспільства» та «суспільства знань», а також як реальне формування фундаментальних основ кіберцивілізації [3, с. 39].

Вперше термін «Інтернет речей» було запропоновано британським інженером К. Ештоном ще у 1999 році [4], однак до цього часу продовжують тривати наукові дискусії щодо його розуміння.

Так, в цілому, під терміном «Інтернет речей» слід вважати:

– сукупність взаємодіючих технічних систем і комплексів, що складаються з мікропроцесорів, сенсорів, пристроїв, систем передачі даних,

локальних і / або розподілених обчислювальних ресурсів і програмних засобів, зокрема програм штучного інтелекту, призначених для реалізації суспільних відносин, в тому числі, пов'язаних з наданням послуг і проведенням робіт при безпосередній участі або без участі суб'єктів (юридичних або фізичних осіб) на основі використання великих даних і мережі Інтернет [1, с. 128];

– концепцію та парадигму, які враховують постійну присутність в оточуючому середовищі значної кількості речей / об'єктів, котрі за допомогою безпровідних та провідних з'єднань та унікальних схем адресацій здатні взаємодіяти між собою, а також з іншими речами / об'єктами для створення нових додатків і послуг [5, с. 6122];

– випадки використання можливостей обчислювальної техніки та підключення до мережі Інтернет об'єктів, датчиків і побутових предметів (пристроїв), які не належать до звичайних комп'ютерів, що дозволяє цим пристроям забезпечувати генерацію, обмін і використання даних з мінімальним втручанням людини [6, с. 9].

Розглянемо більш детально можливості використання в процесі розслідування кримінальних правопорушень інформації, що утворюється внаслідок функціонування «Інтернету речей». Отже, «розумними» речами може генеруватися криміналістично значуща інформація, що може бути використана:

а) в процесі доказування таких обставин, як:

– подія кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення). До прикладу, збережена в пам'яті фітнес-браслету інформація про фізичний стан (пульс, артеріальний тиск, насиченість крові киснем) та фізичну активність (відстань, пройдена за певний проміжок часу, кількість кроків) його власника, дозволяє висунути та перевірити версії про маршрут пересування, вчинення певних дій у відповідний проміжок часу, у випадку смерті – приблизний час її настання. Дані, зафіксовані датчиками «розумного» автомобіля дозволяють реконструювати обставини дорожньо-транспортної пригоди, а також встановити маршрут руху та поточне місцезнаходження автомобіля, яким незаконно заволоділи;

– винуватість обвинуваченого у вчиненні кримінального правопорушення, форма вини, мотив і мета вчинення кримінального правопорушення. Інформація (аудіо, відеофайли, архіви дій користувача), зібрана датчиками «розумного» будинку, а також деякими побутовими прилада-

ми («розумними» пилососом, холодильником, телевізором тощо), дозволяє підтвердити чи спростувати показання підозрюваного щодо його місцезнаходження у визначений час, а також встановити коло осіб, які відвідували визначене приміщення у певний період часу;

– вид та розмір шкоди, завданої кримінальним правопорушенням (наприклад, у випадку проведення незаконних фінансових транзакцій за допомогою «розумного» годинника);

– обставини, які впливають на ступінь тяжкості вчиненого кримінального правопорушення, характеризують особу обвинуваченого, обтяжують чи пом'якшують покарання, які виключають кримінальну відповідальність або є підставою закриття кримінального провадження. Як приклад, наведемо можливість використання даних «розумних» годинників, фітнес-браслета, «розумного» телевізора для створення психологічного портрету їх власника, а також для підтвердження чи спростування факту вчинення кримінального правопорушення обвинуваченим в стані алкогольного, наркотичного сп'яніння чи в стані сильного душевного хвилювання.

В цілому, усі джерела доказів, отримані внаслідок функціонування «Інтернету речей» можна поділити на три групи: докази, зібрані з розумних пристроїв і датчиків; докази, зібрані з апаратного та програмного забезпечення, які забезпечують зв'язок між розумними пристроями і зовнішнім світом; докази, зібрані з апаратного та програмного забезпечення, які знаходяться поза межами мережі, що досліджується (хмарні середовища, соціальні мережі, постачальники послуг Інтернету та мобільних мереж, віртуальні онлайн-ідентифікації тощо) [2, с. 19];

б) з метою встановлення місцезнаходження осіб, які переховуються від органів досудового розслідування або суду, безвісти зниклих осіб, а також для вирішення завдань ідентифікації осіб, чиї протиправні дії були раніше зафіксовані камерами відеоспостереження. Впровадження сучасних технологій «розумного» міста передбачає розміщення та функціонування в громадських місцях (на станціях метро, в підземних переходах, в залах вокзалів, аеропортів тощо) камер відеоспостереження з модулями біометричної ідентифікації, які надають можливість ідентифікувати людину на підставі рис обличчя, ходи, голосу та проінформувати правоохоронні органи щодо його поточного місцезнаходження;

Узагальнюючи вищевикладене, слід зазначити, що використання можливостей «Інтернету речей» має суттєве значення для підвищення

ефективності розслідування кримінальних правопорушень. Водночас, на теперішній час вказане питання досліджено недостатньо і потребує проведення подальших наукових розвідок в цьому напрямі.

**Список використаних джерел**


1. Баранов О. А. Інтернет речей: теоретико-методологічні основи правового регулювання. Т.1: *Сфери застосування, ризики і бар'єри, проблеми правового регулювання*: монографія. НДІІП НАПрН України. Київ : Видавничий дім «АртЕк». 2018. 342 с.
2. Бурдін М. Ю. Безпека і криміналістична експертиза інтернету речей: проблеми та аналіз напрямів протидії кіберзлочинності. *Протидія кіберзлочинності та торгівлі людьми*. Харків, 2022.С.18–19.
3. Фурашев В. М. Інтернет речей і право. *Інтернет речей: проблеми правового регулювання та впровадження:* матеріали науково-практичної конференції. 24 жовт. 2017 р., Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського». Вид-во «Політехніка». 2017. 238 с.
4. Ashton K. That «Internet of Things» Thing. RFID Journal, 22 June 2009. URL: http://www.rfidjournal.com/articles/view?4986. (Last accessed: 22.11.2022).
5. Keyur K. Patel, Sunil M. Patel. Internet of Things-IOT: Definition, Characteristics, Architecture, Enabling Technologies, Application & Future Challenges. *International Journal of Engineering Science and Computing.* 2016. Vol. 6 Issue 5. P. 6122–6131. DOI 10.4010/2016.1482
6. Rose K., Eldridge S., Chapin L. The Internet of Things: An Overview Understanding the Issues and Challenges of a More Connected World. The Internet Society (ISOC). 2015 75 p.

# РОЛЬ ЦИФРОВОЇ КРИМІНАЛІСТИКИ У ВИЯВЛЕННІ, ФІКСАЦІЇ ТА РОЗСЛІДУВАННІ ВОЄННИХ ЗЛОЧИНІВ

**Шевчук Віктор Михайлович,**
доктор юридичних наук, професор, Заслужений юрист України,
професор кафедри криміналістики Національного юридичного
університету імені Ярослава Мудрого, м. Харків, Україна

У сучасних реаліях XXI століття нерідко називають ерою *цифрових технологій.* Сьогодні цифрова епоха – це сучасна ера, в якій соціальна, економічна та політична діяльність залежить від інформаційно-комунікаційних технологій. Вбачається*, що світ цифрових технологій, в який ми зараз входимо, – це не лише новий логічний етап розвитку технологічної сфери людства, а й усієї існуючої правової та соціально-політичної реальності.* У цю епоху, в якій ключове місце займають новітні «високі технології», суспільство переходить у нову реальність цифровізації, активно використовуючи *цифрові технології в* усіх сфер діяльності суспільства [7, с. 203].

Застосування *цифрових технологій* насьогодні це не просто технологічний тренд, модне слово чи тимчасове захоплення – це фактично третя комп'ютерна ера, заснована на інноваціях та передових технологіях цифровізації *(англ. digitalization)*. За таких умов *цифровізація стає найважливішим фактором економічного зростання економіки будь-якої країни і, взагалі, є сучасним трендом розвитку суспільства*, забезпечуючи практично всю цінність та інновації функціювання цифрового сектору держави. Очевидно, що процеси цифровізації зараз виступають, як нова реальність перспективного розвитку передових держав Європи та світу, у тому числі й України, яка обрала європейський вектор розвитку.

З розвитком суспільства, цифровізацією усіх сфер життя потребує постійного вдосконалення система правоохоронних та судових органів, зокрема, її перехід до нової реальності – цифрової. Цифрова інформація, як невід'ємний атрибут сучасної злочинної й діяльності органів кримінальної юстиції, визначає перспективи подальшого розвитку юридичної науки, у тому числі й криміналістики. Цифрова реальність сьогодення пов'язана із появою нових форм злочинності – кіберзлочинів, інформаційного шахрайства, великою кількістю кібернетичних атак на різні

підприємства та установи, в тому числі, і державні бази даних [9, с. 41]. Безумовно, що такі загрози потребують вироблення нових та сучасних підходів, засобів протидії, трансформації й оновлення системи системи органів кримінальної юстиції до сучасних умов та глобальних загроз XXI століття. Серед нових викликів особливо шокуючим та безпрецедентним нині є військова агресія РФ і повномасштабне вторгнення російських військ на територію України 24 лютого 2022 року.

В таких умовах головним завданням криміналістики є розроблення та застосування засобів, прийомів та методів, що дозволяють збирати, досліджувати, використовувати доказову інформацію в умовах війни та глобальних загроз XXI століття [11, с. 898]. Перед системою органів досудового розслідування, прокуратури, органами кримінальної юстиції постають нові виклики, пов'язані із необхідністю швидкого, всебічного та якісного документування, збирання доказової бази масових кримінальних порушень міжнародного гуманітарного права [14, с. 188–190]. Така ситуація створила додаткове навантаженням на судові і правоохоронні органи, які у посиленому режимі забезпечують охорону громадського порядку в містах і населених пунктах, на слідчих та прокурорів, на яких покладається виявлення та документування фактів і наслідків воєнних злочинів, а також на суддів, які у цих надзвичайно складних і небезпечних умовах забезпечують здійснення судового контролю за кримінальним провадженням і правосуддя.

В реаліях воєнного часу гостро постає питання про підвищення ролі криміналістики у умовах війни, у тому числі й за допомогою цифрових технологій, зокрема, формування та застосування нового наукового напрямку – *цифрової криміналістики* (Digital Forensics). Ідея появи цієї галузі криміналістики пояснюється тим, що у сучасному світі практично вся діяльність людини, у тому числі і злочинців, супроводжується своєрідною «слідовою картиною», серед якої особливе місце набувають *цифрові сліди* [6, с. 92–97], як важливе джерело криміналістично-значущої інформації, а засоби цифрової криміналістики стають дієвим напрямком, які суттєво підвищують ефективність традиційних методів розслідування та роботи із доказами.

Вважаємо, що треба чітко розрізняти цифрову криміналістику як окрему галузь криміналістичних знань, спрямовану на дослідження цифрових слідів, з одного боку, та з іншого – застосування цифрових технологій у розслідуванні та судовому розгляді, тобто процес *цифро-*

*візації криміналістики* як закономірний сучасний етапу її розвитку та формування, який передбачає впровадження цифрових технологій у різні галузі криміналістичної техніки та судової експертизи, до самого процесу досудового розслідування [8, с. 288]. Цифровізації криміналістики може включати декілька аспектів, зокрема такі як: 1) використання цифрових технологій для підвищення ефективності пошуково-пізнавальної діяльності слідчого, ефективної організації цієї діяльності на сучасному рівні, оптимізації взаємодії різних органів, установ при розслідуванні кримінальних правопорушень; 2) використання інформаційно-комунікативних (інформаційних комп'ютерних) технологій для розслідування кримінальних правопорушень, що сприяє алгоритмізації процесу досудового розслідування в цілому і окремих його етапів; 3) рішення дидактичних завдань в сфері підготовки, перепідготовки, підвищення кваліфікації слідчих, слідчих-криміналістів, судових експертів, обміну досвідом [1, с. 104–105].

Як показує практика, в сучасних умовах російсько-української війни традиційні криміналістичні засоби та форми збирання доказів воєнних злочинів можуть працювати обмежено через небезпеку для всіх учасників слідчих (розшукових) дій, а також через неможливість безпосереднього доступу до місця події. Тому виникає потреба у пошуку в мережі Інтернет, соціальних мережах, телеграм-каналах та інших відкритих джерерах інформації, тобто широкого застосування інструментів цифрової криміналістики [12], які суттєво розширюють можливості виявлення, документування та розслідування воєнних злочинів, що вчинюються окупаційними військами РФ на території України.

У цьому плані слушно зазначає В. Ю. Шепітько, що сучасний розвиток цифрової криміналістики відбувається у трьох основних напрямах: 1) формування окремої наукової галузі в криміналітиці; 2) застосування спеціальних знань шд час роботи з цифровими доказами; 3) проведения судових експертиз (зокрема, комп'ютерно-технічної експертизи) [10, с. 21]. Цифрова криміналістика, зокрема, має відношення до процесу збору, отримання, збереження, аналізу та подання електронних (цифрових) слідів з метою отримання оперативно-розшукових відомостей, доказової інформації і здійснення розслідування та кримінального переслідування по відношенню до різних видів кримінальних правопорушень [3, с. 21], включаючи кіберзлочини та воєнні злочини.

У воєнних реаліях центральне місце для збирання доказів воєнних злочинів у цифровій криміналістиці посіли технології штучного інтелекту. Так, у ситуації повномасштабної агресії інструменти цифрової криміналістики значно допомагають у виявленні, розкритті та розслідуванні воєнних злочинів. Саме завдяки іструментам цифрової криміналістики та даних з відкритих джерел було встановлено факти масових вбивств, воєнних злочинів, які було вчинено у містах Київської області у період з 27 лютого 2022 р. по 31 березня 2022 р. Збройні сили України, звільнивши місто Буча, знайшли велику кількість тіл цивільних громадян, що лежали просто на дорогах. Після оприлюднення кадрів з цими тілами російська влада почала просувати ідею, що це постанова і тіла були підкинуті після звільнення міста. Проте *супутникові знімки допомогли довести, що тіла з'явилися саме під час російської окупації*. У цьому контексті не можна також забувати про масові поховання людей. Оскільки вони, здебільшого, знаходяться на тимчасово окупованих територіях і до них немає доступу – цифрова криміналістика, а саме аналіз та порівняння супутникових знімків, може суттєво допомогти у встановленні винних. Так відбулося і з масовим похованням біля церкви святого Андрія в Бучі, що було зафіксоване на супутникових знімках Maxar [6].

Певний науковий та практичний інтерес, на наш погляд, набувають інструменти цифрової криміналістики, які допомагають у виявленні та розслідуванні воєнних злочинів та сприяють невідворотності покарання воєнних злочинців, що виокремлюються у фаховій літературі. Серед них акцентується увага на таких: пошук за ключовими словами та хештегами, списки яких попередньо піготовлені, моніторинг радарівв та системи офіційного моніторингу суден Marine Traffic, аналіз супутникових знімків, використання технології аналізу «великих даних» (Big Data); аналіз геолокаційних міток, дослідження фото- та відеоматеріалів у відкритому доступі та наданих слідству, використання програм для аналізу та обробки цифрових зображень, дослідження телефонних розмов, аналіз електронних пристроїв, аналіз ігрових систем, система розпізнавання облич і пошуку їх у відповідних базах даних (в Україні використовують додаток з розпізнавання облич Clearview Af для ідентифікації потенційних злочинців і загиблих) [5, с. 32].

В інших джерелах виокремлюються такі сучасні напрями цифрової криміналістики: 1) дослідження хмарних сховищ; 2) дослідження мо-

більних пристроїв (телефонів); 3) дослідження програм (месенджерів та інших застосунків для смартфонів, що використовуються для обміну інформацією); 4) дослідження інтернет-речей (IoT); 5) мережеві дослідження; 6) дослідження новітніх приладів і додатків (Alexa від Amazon, Google Assistant, Siri від Apple та ін.); 7) дослідження додатків не для телефону (дослідження баз даних, Spotlight, America online instant messaging, дронів, волатильної пам'яті, Даркнету, засобів антикриміналістики, видалених і фрагментованих файлів, зображень, флеш-пам'яті, криповалют); 8) цифровий аналіз поведінки окремих осіб, груп людей та їх взаємозв'язків і відносин; 9) цифрова криміналістична розвідка та розвідка на основі відкритих джерел тощо [13].

Вбачається, що у сучасних умовах війни збір та робота із цифровими доказами вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні. Заслуговують на увагу розробки українських науковців щодо методик розслідування злочинів, скоєних у кіберпросторі, побудови їх криміналістичної характеристики, визначення алгоритму їх розслідування, а також специфіки використання спеціальних знань і проведення судових експертиз під час розслідування цієї категорії кримінальних правопорушень[15, с. 16].

Крім цього, серед завдань криміналістики важливими є дослідження проблематики формування цифрової криміналістики та її співвідношення з криміналістикою як юридичною наукою і навчальною дисципліною, місця цифрової криміналістики в діяльності органів правопорядку та правосуддя, питань щодо усунення прогалин у нормативно-правовому регулюванні використання цифрових доказів у досудовому розслідуванні та судовому розгляді тощо.

Таким чином, насьогодні існує нагальна потреба у розробленні та формуванні окремого розділу криміналістики, пов'язаного із криміналістичним дослідженням цифрових доказів, зміст якого включатиме наукові положення цифрової криміналістики як галузі судових наук, адаптованих до сучасних реалій і потреб практики та теоретико-методологічних засад криміналістики. За таких умов активізація дослідження проблематики ролі цифрової криміналістики у виявлені та розслідувані воєнних злочинів, що вчинюються РФ на території України, є перспективним стратегічним напрямком розвитку сучасної криміналістики, який потребує подальших наукових розробок.

**Список використаних джерел**


1. Думчиков М. О. Процеси діджиталізації і криміналістика: ретроспективний аналіз. *Криміналістика і судова експертиза*, 2020,65, 100–108.
2. Когутич І. І. Застосування цифрових технологій – новий напрям криміналістики. *Наукові читання пам'яті Ганса Гросса*: збірник тез міжн. наук.-практ. конф. (м. Чернівці, 09 грудня 2021 р.). Чернівецький нац. Ун-т імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79–84.
3. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. *Київський часопис права*, 2022, (1), 176–180.
4. Крицька І. О. «Доріжка цифрових слідів»: доказове значення й окремі аспекти збирання та дослідження у кримінальному провадженні. *Цифрові трансформації України 2020: виклики та реалії*: зб. наук. пр. НДІ ПЗІР НАПрН України, 18 вересня 2020 р. Харків, 2020. С. 92–97.
5. Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika* ir *teismo ekspertologija*: *mokslas*, *studijos*, *praktika*: *XVIII*, 2022. Т. 18. С. 31–37.
6. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі?: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html
7. Наджафлі Е. Цифрова держава в контексті правової реформи в Україні: теоретико-правовий аспект. *Право і безпека*, 2022, 2 (85). С. 202–217.
8. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського держ. ун-ту внутр. справ ім. Е. О. Дідоренка*. 2022. №3 (99). С. 283–294.
9. Тимошенко, Ю., Кисленко, Д. Правоохоронна система в епоху діджиталізації. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*, (1 (59), 2022, 40–45. С. 41.
10. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України*. 2021. №8. С. 12–27.
11. Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science*: Proceedings of the 5th International scientific and practical conference (August 7–9, 2022). Sci-conf.com.ua‖. Lviv, Ukraine. 2022. Pp. 896–903.
12. Latysh, K. V. Criminalistics Analysis of Cyber Tools for Committing Crimes. *Probs. Legality*, *153*, 165.
13. Reedy P. Interpol review of digital evidence 2016–2019. *Forensic Science International: Synergy*. 2020. Vol. 2. P. 489–520.

14. Shevchuk V. M. The role of criminalistics in improving the efficience of the investigation of war crimes committed by military of the RF in Ukraine. *Scientific Collection «InterConf»*, (122): 1st International Scientific Conference «Diversity and Inclusion in Scientific Area» (August 26–28, 2022). Warsaw, 2022. Pp. 187–195.

15. Shepitko V. Theoretical and methodological model of criminalistics and its new directions. *Theory and Practice of Forensic Science and Criminalistics*. Issue 3 (25). 2021. P. 9–20.

# ФОРМУВАННЯ ЦИФРОВОЇ КРИМІНАЛІСТИКИ ТА ЇЇ РОЛЬ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

**Шепітько Валерій Юрійович,**
доктор юридичних наук, професор, заслужений діяч науки і техніки України, завідувач кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, завідувач лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, дійсний член (академік) Національної академії правових наук України,
м. Харків, Україна

Криміналістичні знання відображають певні тенденції глобалізованого світу. В сучасних умовах змінюється також й вектор криміналістичних досліджень в Україні і наближення його до єдиного європейського простору [1, с. 651–669]. На сьогодні розвиток криміналістики та судової експертизи обумовлений науково-технічним прогресом світового співтовариства, запровадженням новітніх технологій.

Прикладами використання новітніх інформаційних технологій є пропонування дистанційних форм досудового розслідування та судового розгляду, проведення процесуальних дій у дистанційному режимі, режимі відеоконференцзв'язку, формування електронного кримінального провадження (справи), розроблення та впровадження різного роду єдиних реєстрів (наприклад, єдиний реєстр судових рішень, єдиний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань, єдиний реєстр боржників, державний реєстр атестованих судових експертів, реєстр методик проведення судових експертиз та ін.). Певним брендом цифрової держави (держава в смартфоні) в Україні визнано мобільний застосунок, веб-портал – «Дію». Значним досягненням є й те, що в Україні запроваджується інформаційно-телекомунікаційна система досудового розслідування [2]. При цьому, у ч. 1 ст. 106–1 КПК передбачено, що «інформаційно-телекомунікаційна система досудового розслідування – це система, яка забезпечує створення, збирання, зберігання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні».

Тенденцією криміналістики є інтеграція знань, пропонування новітніх, інноваційних розробок науки, спрямованих на вирішення завдань протидії злочинності. Важливим інноваційним напрямом у розвитку криміналістики та судової експертизи є використання цифрової інформації. У криміналістиці та судовій експертизі має місце тенденція щодо впровадження прогресивних технологій, методів та засобів, які ґрунтуються на належному співвідношенні заходів безпеки і свободи, застосуванні стандартів доказування у кримінальному провадженні, відбувається забезпечення криміналістичними знаннями різних суб'єктів кримінального провадження.

У вітчизняних літературних джерелах вивчення доктринальних проблем криміналістики та судової експертизи вперше на рівні узагальнення загальнотеоретичних, методологічних та інших актуальних питань розвитку цих наукових знань було здійснено у межах комплексного міжгалузевого дослідження в структурі юридичної доктрини України. У п'ятому томі «Правової доктрини України» (2013), який було присвячено «Кримінально-правовим наукам України: стану, проблемам та шляхам розвитку», запропоновано два розділи щодо досліджуваної проблематики: «Сучасний стан та розвиток криміналістики» і «Теоретико-методологічні засади судової експертизи» [3].

Останнім часом суттєвим зрушенням у дослідженні доктринальних проблем криміналістики та судової експертизи є підготування актуальної теми номера «Криміналістика та судова експертиза в юридичній доктрині України» в журналі «Право України» (2021, № 8). До підготування серії наукових статей у цей номер журналу були залучені провідні українські фахівці в галузі криміналістики та судової експертизи, представники Харківської, Київської та Одеської наукових шкіл. Статті були підготовлені та розміщені за трьома рубриками: 1) криміналістика та судова експертиза в структурі юридичної доктрини; 2) доктринальні підходи в окремих напрямах криміналістики; 3) інноваційні напрями розвитку криміналістики.

Певним синтезом у дослідженні доктринальних підходів до криміналістики та судової експертизи, а також змінення їх парадигми є стаття «Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору» в журналі «Право України» (2022, № 2) [4. с. 76–90].

У криміналістиці існує аксіома, яка свого часу була запропонована доктором Е. Локаром (принцип Локара) «кожний контакт – залишає слід». Можна констатувати, що будь-яке кримінальне правопорушення завжди залишає сліди (матеріально-фіксовані, ідеальні, віртуальні або електронні). Тому розслідування і судовий розгляд має відбуватися шляхом пізнання події, що відбулася, засобами криміналістики у встановленому законом порядку.

В юридичні доктрині існують різні підходи до розуміння доказів. Докази розглядають як «факти реальної дійсності», «будь-які фактичні дані, що мають значення для кримінального провадження», «відповідний носій (джерело) відомостей про них», «процесуальну процедуру та форму (спосіб) її закріплення в матеріалах кримінального провадження».

Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому 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.

Окремої уваги заслуговують так звані цифрові докази (цифрова інформація) – інформація, яка створена за допомогою високих інформаційних технологій. У наукових джерелах зарубіжних країн широкого застосування набув термін «digital evidence» (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютерної чи іншої техніки [5, с. 257].

Цифрові докази – це фактичні дані, що подані у цифровій формі та зафіксовані на будь-якому типі носія [5, с. 256–260]. Поряд із терміном «цифрові докази» використовуються й інші, наприклад: «електронні докази», «електронні сліди», «цифрові джерела інформації», «електронні документи» тощо.

У ч. 2 ст. 99 КПК України вказано, що до документів, зокрема, можуть належати «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні). У ч. 4 ст. 99 КПК України регламентовано, що «дублікат документа, а також копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа».

Цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні. У роботі з цифровими доказами необхідно дотримуватись таких принципів, як: наявність фахової підготовки, експертна підтримка і розумна обережність.

Фактично можна констатувати появу окремого криміналістичного напрямку – *«цифрової криміналістики»* [6, с. 148] (Digital Forensic, Digital Forensic Science or Digital Criminalistics). У спеціальних джерелах для позначення даного напрямку використовуються й інші терміни – «комп'ютерна криміналістика» (Computer Forensic) або «криміналістика в комп'ютерних системах». Цифрова криміналістика – «окрема криміналістична теорія та вид судової експертизи, що ставить своїм завданням дослідження цифрових доказів з використанням криміналістичної техніки та наявних методик в цілях досудового розслідування та судового розгляду» [7, с. 130]. При цьому, деякі науковці навіть розглядають комп'ютерну криміналістику як «прикладну науку про розслідування злочинів (інцидентів), пов'язаних із комп'ютерною інформацією, при дослідженні цифрових доказів, методів пошуку, отримання і фіксації таких доказів» [8, с. 120–126].

Розвиток цифрової криміналістики відбувається у трьох основних напрямах: 1) формування окремої наукової галузі в криміналістиці; 2) застосування спеціальних знань під час роботи з цифровими доказами; 3) проведення судових експертиз (зокрема, комп'ютерно-технічної експертизи) [9, с. 21].

**Список використаних джерел**

1. Журавель В. А., Шепітько В. Ю. Розвиток криміналістики та судової експертизи в Україні: наближення до єдиного європейського простору. *Правова наука України: сучасний стан, виклики та перспективи розвитку*: монографія. Харків, 2021. С. 651–669.

2. Закон України від 1 червня 2021 р. №1498-IX «Про внесення змін до Кримінального процесуального кодексу України щодо запровадження інформаційно-телекомунікаційної системи досудового розслідування» [Електронний ресурс]. URL: https://zakon.rada.gov.ua/laws/show/1498–20#Text

3. Правова доктрина України: у 5 т. Харків: Право, 2013. Т. 5: Кримінально-правові науки в Україні: стан, проблеми та шляхи розвитку / за заг. ред. В. Я. Тація, В. І. Борисова. 1240 с.

4. Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України*. 2022. № 2. С. 76–90.

5. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету.* Сер.: Юриспруденція. 2013. № 5. С. 256–260.

6. Шепітько В. Ю. Інновації в криміналістиці як віддзеркалення розвитку науки. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці*: матер. міжнар. «круглого столу» (Харків, 12 грудня 2019 р.). Харків: Право, 2019. С. 147–150.

7. Шепітько В. Ю., Шепітько М. В. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. 508 с.

8. Гриців О. І. Криміналістика в комп'ютерних системах: процеси, готові рішення. *Вісник Національного університету «львівська політехніка». автоматика, вимірювання та керування.* 2013. № 774. С. 120–126.

9. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України.* 2021. № 8. С. 12–27.

# ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

**Яремчук Вікторія Олегівна,**
кандидат юридичних наук, старший науковий співробітник,
Науково-дослідного інституту вивчення проблем злочинності
імені академіка В. В. Сташиса
НАПрН України, м. Харків, Україна

Поява нових вдів кримінальних правопорушень, змінення способів їх вчинення потребує застосування нових інформаційних технологій при розслідуванні. Так, фахівці у сфері інформаційних технологій визнають, що організована злочинність дедалі частіше використовує Інтернет з метою ведення і приховання своєї діяльності. Зараз нікого не здивуєш існуванням мережі «Darknet», за допомогою якої правопорушники створили незаконний ринок для збуту наркотиків, зброї, крадених товарів тощо. Завдяки технологіям, які забезпечують мережеву анонімність, ця частина Інтернету залишається абсолютно безконтрольною, а тому безпечною для діяльності злочинців. За даними, наданими Національною поліцією України, кількість організованих груп і злочинних організацій, що вчиняють кримінальні правопорушення з використанням цифрових технологій, за останній рік збільшилась на 36%[1] Нині цифрова інформація та цифрові носії інформації можуть бути отримані: під час обшуку (ст. 234 КПК), огляду (ст. 237 КПК), витребування документів і предметів (ст. 93 КПК) та негласних слідчих (розшукових) дій (гл. 21 КПК). Вилучення цифрової інформації під час проведення обшуку й огляду проводиться шляхом її копіювання з інформаційного простору або цифрового носія інформації у такий спосіб: а) вилучення (копіювання) цифрової інформації з місця її виявлення на цифровий носій інформації; б) пред'явлення виявленої цифрової інформації понятим, спеціалісту й іншим учасникам слідчих дій; в) відображення у протоколі слідчих дій часу, місця й обстановки виявленої інформації; г) пакування і опечатування цифрових носіїв інформації, які містять шукану цифрову інформацію [2, с. 179]. Під час вилучення цифрових носіїв інформації важливим є залучення спеціалістів. За їх допомогою слідчий, детектив вилучить

саме потрібний обсяг інформації, а не всю інформацію. Надалі це полегшить та пришвидшить виконання судової експертизи.

Якщо говорити про науковий підхід, то можна констатувати появу окремого криміналістичного напряму – «цифрової криміналістики» (Digital Forensic, Digital Forensic Science or Digital Criminalistics). У спеціальних джерелах для позначення цього напряму використовуються й інші терміни – «комп'ютерна криміналістика» (Computer Forensic) або «криміналістика в комп'ютерних системах»[3, с.12].

Коли звернутися до практики правоохоронних органів, то в умовах війни саме цифрова криміналістика сприяє розкриттю кримінальних правопорушень. Так, під час військових подій у місті Буча Київської області у 2022 р. знайдено велику кількість тіл цивільних громадян, що лежали просто на дорогах. Після оприлюднення кадрів із загиблими, російська влада заявила, що ці тіла підкинуті після звільнення міста. Проте за допомогою супутникових знімків було встановлено, що тіла з'явилися саме під час російської окупації. Крім того, при виявленні масових поховань людей на тимчасово окупованих територіях, «цифрова криміналістика», а саме, аналіз та порівняння супутникових знімків, надають суттєву допомогу у розслідуванні [4].

Тому у нинішньому світі використання цифрових технологій надає суттєву допомогу у розслідуванні, без якої розкриття сучасних кримінальних правопорушень є неможливим. Широко розповсюдені сьогодні саме «цифрові кримінальні правопорушенн». Необхідно запрошувати спеціалістів під час вилучення носіів цифрової інформації під час слідчих (розшукових) і негласних слідчих (розшукових) дій. Для ефктивності розслідування даних видів кримінальних правопорушень створено окремий розділ криміналістичної науки – «цифрова криміналісика». Під час російської війни на території України саме «цифрова криміналістика» допомагає слідчим, прокурорам розслідувати кримінальні правопорушення вчинені російськими військовими.

**Список використаних джерел**

1. Кіберзлочинність в Україні. Ера цифрових технологій – ера нових злочинів. URL: https://uz.ligazakon.ua/ua/magazine_article/EA013606

2. Метелев О. П. Збирання цифорової інформації як окремий спосіб отримання доказів під час кримінального провадження *Науковий вісник Ужгородського національного університету*. Серія ПРАВО. 2020. Вип. 60. С. 177–180.

3. Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні *Право України* 2021. Вип. 8. С. 12–27

4. 4. Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html

# DIGITAL CRIMINALISTICS: FORMATION AND ROLE IN THE FIGHT AGAINST CRIME IN WARTIME CONDITIONS IN UKRAINE

**Shevchuk Viktor**
Doctor of Legal Sciences, Professor,
Professor of Criminalistics Yaroslav Mudryi National Law University,
leading researcher Academician Stashis Scientific Research
Institute for the Study of Crime Problems, UKRAINE
ORCID ID: 0000-0001-8058-3071

**Konovalova Violeta**
Doctor of Legal Sciences, Professor, Academian
National Academy of Legal Sciences of Ukraine,
chief researcher Academician Stashis Scientific Research
Institute for the Study of Crime Problems, UKRAINE
ORCID ID: 0000-0003-2043-8694

**Sokolenko Mykyta**
junior research fellow of the Academician Stashis Scientific
Research Institute for the Study of Crime Problems, UKRAINE
ORCID ID: 0000-0002-0302-162X

In today's realities, digitalization is not only a modern trend in the development of society, but also becomes the most important factor in the economic, social, political and international growth of any country. Granting Ukraine the status of a candidate for EU membership created an additional impetus for harmonizing approaches to digital transformation. In this regard, an important event was the fact that Ukraine joined the Program «Digital Europe» until 2027, the purpose of this program is to activate the recovery of the economy and the digital transformation of Ukraine [1]. The formation of a single digital market with the EU and the approximation of the digital sector of Ukraine to the European one are the priorities of the domestic policy of digital transformations in the conditions of war [2] and the choice of the European development of modern criminalistics [3, p. 325–327].

Digital technologies in modern conditions are an integral component, integrated into all spheres of human activity, which determines the prospects for the development of the economy, politics, national security and defense

capabilities of the state. Under such conditions, with the development of society and the digitalization of all spheres of life, the problem of constant improvement of state bodies, local self-government, judicial and law enforcement bodies, in particular, their modernization and transition to a new digital reality, becomes acute. At the same time, this reality is closely related to the emergence of new forms of crime – cybercrimes, information fraud, a huge number of cyberattacks on various enterprises and institutions [4, p. 77–89]. Digital information, as an integral attribute of criminal justice and criminal activities, determines the development trends of legal science, including criminalistics, which is at the forefront of the fight against crime.

The development of science and society was significantly affected by the full-scale armed aggression of the Russian Federation and the introduction of martial law in Ukraine. According to the official statistics of the Office of the Prosecutor General, the most common crimes are the following: a) crimes of aggression and war crimes – 52,157 crimes were registered (as of December 9, 2022); b) crimes against national security – 18,542 crimes; c) crimes against children – 443 children were killed, 855 children were injured; 4) the main case concerning the aggression of the Russian Federation – 627 suspects are representatives of the military and political leadership of the Russian Federation [5].

It is obvious that such dynamics and trends of crime in Ukraine during the war had a significant impact on changing the priorities of criminalistics tasks and the activities of the criminal justice system. Under such conditions, there was an urgent need to develop new approaches in the fight against modern military challenges, the need to modernize and update law enforcement and judicial bodies to modern conditions of martial law [6, p. 92–98], creation and introduction of an effective system of counteraction to existing threats, including the means of criminalistics, criminal procedural and criminal law.

In today's military realities, the system of pre-trial investigation bodies, the prosecutor's office, and criminal justice bodies face new challenges related to the need for quick, comprehensive and high-quality documentation, gathering the evidence base of mass criminal violations of international humanitarian law. Today, the question of increasing the effectiveness of the investigation of modern crime, including war crimes and cybercrimes with the help of digital technologies, is a pressing issue. Under such circumstances, it is now possible to talk about the activation of trends in the formation and application of a new scientific direction – Digital Forensics, Digital Forensic Science

or Digital Criminalistics. Other terms are used to denote this direction – «Computer Criminalistics» [7], «Electronic Criminalistics» [8, p. 79].

The further development of criminalistics in the conditions of the information society, digitization and military realities of today is impossible without the wide use of innovative and fundamental knowledge in the field of digital criminalistics – a new field of criminalistics that is dynamically developing today and forms theoretical and methodological foundations in this area of knowledge. Today, criminalistics corresponds to the development of digital technologies, creating means and methods for the possibility of extracting forensically significant information from a new type of media [9, pp. 8–25]. Thanks to scientific and technical progress, it is possible to use digital technologies in law enforcement activities, which accelerates the process of pre-trial investigation, allows to more fully form the evidence base in the investigation of criminal offenses, and in the future ensures the quality of judicial review of materials of criminal proceedings.

In the specialized literature, there are different approaches to defining the concept of digital criminalistics and its place in the system of criminalistics and forensic sciences. Some scientists point out that digital criminalistics is a separate branch of criminalistics science, which is a system of scientific methods for researching digital evidence with the aim of facilitating the detection and investigation of criminal offenses. Others point out that digital criminalistics is related to the process of collecting, receiving, saving, analyzing and submitting electronic (digital) data for the purpose of obtaining investigative information, evidentiary information and carrying out investigations and criminal prosecutions in relation to various types of crimes [10, p. 179], including cybercrimes and war crimes committed by the military of the Russian Federation on the territory of Ukraine.

Some sources indicate that digital forensics is «a branch of criminalistics that focuses on criminal procedural law and evidence related to computers and related devices» [11, p. 29], such as mobile devices (for example, telephones and smartphones), game consoles and other devices that function via the Internet. In addition, digital forensics is related to the process of collecting, obtaining, preserving, analyzing and presenting electronic (digital) evidence in pretrial and judicial proceedings. Therefore, digital criminalistics can be a strategic direction in the development of criminalistic science [12, p. 192].

In view of the above, it can be stated that the subject of digital criminalistics is the regularities of detection, recording, preliminary research,

use of computer information, digital traces and means of their processing for the purpose of solving the tasks of detection, disclosure, investigation and prevention of criminal offenses, as well as development based on this knowledge of the patterns of technical means, methods, and methodological recommendations aimed at optimizing activities to combat criminal offenses in the digital space. Therefore, digital criminalistics is a branch of criminalistics that studies the patterns of occurrence and use of digital traces and, based on the knowledge of these patterns, develops technical means, techniques and methods for detecting, recording, extracting and researching digital information (evidence) and means of processing it for the purpose of disclosure, investigation and prevention of criminal offenses.

We believe that it is necessary to clearly distinguish digital criminalistics as a separate field of criminalistic knowledge, aimed at the study of digital traces, on the one hand, and on the other – the use of digital technologies in investigation and judicial proceedings [13], that is, the process of digitization of criminalistics as a natural modern stage of its development and formation, which involves the implementation of digital technologies in various fields of criminalistic technology and forensic examination, to the very process of pre-trial investigation.

In the realities of war, the central place for gathering evidence of war crimes in digital criminalistics was occupied by artificial intelligence technologies. In modern conditions of war, the following areas of application of digital criminalistics are of particular importance: obtaining information from mobile devices of seized phones of participants in criminal proceedings; receiving information from personal computers of individuals and legal entities; obtaining information from servers and other information stores in organizations and institutions; obtaining information about radio frequency identifiers, GPS trackers, sensors, stationary and mobile measuring devices using geolocation, video surveillance and positioning systems; receiving information from network services that establish voice and video communication between computers via the Internet, such as ICQ, Skype, WhatsApp, Viber, Telegram and others; receiving information from banking systems on appropriate digital media (SD disks, flash cards, etc.); receiving information from cellular communication operators regarding the details of subscriber communication and establishing the location of the subscriber from geolocation; obtaining information from video surveillance cameras of various commercial and state structures; obtaining information from cameras

and video cameras seized from participants in criminal proceedings [14, p. 165].

Thus, in today's realities, it is necessary to update the development of the issues of digital criminalistics in modern conditions of war. Particular attention should be paid to increasing the role of criminalistics didactics, in particular, criminalistics training of investigators, prosecutors, courts, detectives, criminalistics investigators, forensic experts in the field of digital technologies. Starting a new profession and training a digital criminalistist is quite relevant today. Therefore, in the realities of martial law, there is an urgent need to form the concept of digital criminalistics and improve educational programs, taking into account innovative approaches of criminalistic didactics and European integration processes aimed at the modern development of criminalistics.

**References:**


1. Digital Europe programme for the period 2021–2027. URL: https://www. europarl. europa. eu/doceo/document/TA-8-2019-0403_EN. html (date of application:10.12.2022).
2. Digital single market for Europe – Consilium. URL: https://www. consilium. europa. eu/en/policies/digital-single-market/ (date of application:10.12.2022).
3. Шевчук В. М. Європейський вектор розвитку сучасної криміналістики. *Адаптація правової системи України до права Європейського союзу: теоретичні та практичні аспекти*: матеріали VI Всеукр. наук.-практ. конф. (м. Полтава, 29.09.2022). Полтава: Полт. юрид. ін-т, 2022. С. 325–327.
4. Dubord P (2008) Investigating cybercrime. In: Barbara JJ (ed) *Handbook of Digital and Multimedia Forensic Evidence*. Totowa, NJ: Humana Press Inc, 77–89.
5. Website of the Prosecutor General's Office. URL: https://www. gp. gov. ua/ (date of application:10.12.2022).
6. Raharjo, E., Monica, D. R., Anwar, M., & Cahyani, K. I. Criminal protection against victims criminal actions in cyber crime. *South East Asia Journal of Contemporary Business, Economics and Law*, Vol. 24, Issue 4 (June), 2021. P. 92–98.
7. aved A. R., Ahmed W., Alazab M., Jalil Z., Kifayat K., Gadekallu T. R. A compre hensive survey on computer forensics: State-of-the-art, tools, techniques, challenges, and future directions. IEEE Access. 2022. Vol. 10. P. 110650–11089. DOI: 10.1109/ACCESS. 2022.3142508.

8. Заєць І. С. Перспективи криміналістики в умовах інформатизації суспільства. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід*: матеріали Міжнар. наук.-практ. круглого столу (Київ, 19 лют. 2020). Київ: НАВС, 2020. С. 77–81.

9. Shevchuk, V. Innovative optimization directions of investigative (detective) activity in modern condition. *Theory and Practice of Forensic Science and Criminalistics*: Collection of Scientific Papers, 2021. Issue 2 (24), 2021. P. 8–25.

10. Kolodina A. S., Fedorova T. S. Tsyfrova kryminalistyka: problemy teorii i praktyky. *Kyivskyi chasopys prava – Kyiv Journal of Law*, issue 1, 2022. P. 176–180.

11. Maras M.-H. Computer Forensic: Cybercriminals, Laws, and Evidence. Second Edition, 2014. 408 p.

12. Шепітько В., Шепітько М. Формування цифрової криміналістики як стратегічний напрямок розвитку науки. *XVII Medzinarodny Kongres Kriminalistika a Forenzne Vedy.* (September 16–17, 2021). Bratislava, Slovak Republic. 2021. С. 187–198.

13. Найдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. Підприємництво, господарство і право. 2019. № 5. С. 304–307.

14. Latysh, K. V. Criminalistics Analysis of Cyber Tools for Committing Crimes. *Probs. Legality*, 2021, *153*, 165.

*Наукове видання*

# ВИКОРИСТАННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ В РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Матеріали міжнародного науково-практичного круглого столу,
присвяченого Всеукраїнському тижню права
м. Харків, 12 грудня 2022 року

*Електронне наукове видання*

Видається в авторській редакції

Комп'ютерна верстка *А. Т. Гринченка*

Підписано до поширення через мережу Інтернет 17.12.2022.
Відповідає формату друкованого видання 60×84/16. Гарнітура Times.
Обл.-вид. арк. 5. Об'єм даних 0,95 Мб.
Вид. № 3083

Видавництво «Право» Національної академії правових наук України
та Національного юридичного університету імені Ярослава Мудрого,
вул. Чернишевська, 80-А, Харків, 61002, Україна
Тел./факс (057) 716-45-53
Сайт: https://pravo-izdat.com.ua
E-mail для авторів: verstka@pravo-izdat.com.ua
E-mail для замовлень: sales@pravo-izdat.com.ua
Свідоцтво про внесення суб'єкта видавничої справи
до Державного реєстру видавців, виготовлювачів і розповсюджувачів
видавничої продукції – серія ДК № 4219 від 01.12.2011