

2.2. Використання цифрової інформації, отриманої під час проведення оперативно-розшукових заходів, у розкритті кримінальних правопорушень

Глобальна цифровізація створює нові виклики та можливості для поліції. Соціальні мережі, інтернет-магазини та інші платформи електронної торгівлі, приховані мережі типу darknet активно використовують злочинці для торгівлі всім, починаючи від диких тварин, заборонених речовин, людських органів, культурних цінностей і контрафактної продукції. Окремі суб'єкти використовують віртуальні валюти та альтернативні банківські платформи для відмивання своїх незаконних доходів, тоді як організована злочинність і терористичні групи вдаються до нових (зашифрованих) комунікаційних технологій і платформ для зв'язку та прихованої взаємодії¹. Разом із цим з'явилися нові інструменти для запобігання, розслідування та боротьби зі злочинністю, а також – для взаємодії правоохоронних органів між собою та громадськістю.

У найближчі десятиліття правоохоронні органи зіткнуться зі все більш оцифрованим і складним світом. За даними міжнародної корпорації Deloitte, у недалекому майбутньому від 20 до 30% діяльності поліцейських може бути автоматизована².

Відповідно до ст. 2 Закону України «Про оперативно-розшукову діяльність» під час проведення негласних слідчих (розшукових) дій, розвідувальних та контррозвідувальних заходів передбачається застосування оперативних та оперативно-технічних засобів³. Застосу-

¹ Transformative Technologies: How digital is changing the landscape of organized crime. Global Initiative Against Transnational Organized Crime. Posted on 29 Jun 2020. p.p. 2–3. <https://globalinitiative.net/wp-content/uploads/2020/06/Transformative-Technologies-WEB.pdf>

² Deloitte. Policing 4.0. Deciding the future of policing in the UK. (2018). URL: <https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/public-sector/deloitte-uk-future-of-policing.pdf>

³ Про оперативно-розшукову діяльність: Закон України №2135-ХІІ від 18.02.1992. Редакція від 15.06.2022. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text>

вання сучасних електронних засобів протидії кримінальним правопорушенням є одним із факторів підвищення якості проведення оперативно-розшукових заходів (ОРЗ) і негласних слідчих (розшукових) дій (НСРД). Такими засобами (серед інших) слугують спеціальні і не спеціальні (побутові) електронні прилади, за допомогою яких здійснюється аудіо- та відеозапис, фотозйомка осіб, документів, предметів, слідів протиправної діяльності.

Спеціальними технічними засобами є пристрої, обладнання, апаратура, прилади та програмне забезпечення, спеціально розроблені, виготовлені, запрограмовані або пристосовані для негласного отримання інформації¹. Перелік спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, а також критерії належності спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації наведені у додатку № 16 Постанови Кабінету міністрів України № 669 від 22 вересня 2016 р.²

В окремих випадках під час проведення ОРЗ та НСРД використовуються такі побутові електронні технічні засоби, як мобільні телефони, диктофони, фото- та відеокамери, GPS-трекери. Завдяки своїм невеликим розмірам, багатофункціональності, можливості негласного фіксування інформації вони правомірно використовуються уповноваженими співробітниками оперативних підрозділів³.

Порядок використання науково-технічних засобів при проведенні НСРД за своєю суттю мало чим відрізняється від їх використання при проведенні оперативно-розшукових дій (ОРД). Навіть окремі норми закону «Про оперативно-розшукову діяльність»

¹ Про затвердження Зводу відомостей, що становлять державну таємницю: Наказ Центрального управління Служби безпеки України 23 грудня 2020 року № 383. Редакція від 13.10.2023. URL: <https://zakon.rada.gov.ua/laws/show/z0052-21#Text>

² Деякі питання щодо спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації: Постанова Кабінету міністрів України № 669 від 22 вересня 2016 р. Редакція від 22.11.2023. URL: <https://zakon.rada.gov.ua/laws/show/669-2016-%D0%BF#n158>

³ Тіхонов С. В., Кобець М. В. Методичні рекомендації щодо застосування GPS-трекерів у розкритті кримінальних правопорушень. Київ : Нац. акад. внутр. справ, 2021. С. 17.

(п.п. 2,4,9,10,11.12,14,17 ч.1 ст. 8) є бланкетними із посиланнями на статті глави 21 КПК України.

Оперативним працівникам під час проведення ОРЗ часто доводиться звертатися за інформацією до криміналістичних обліків, які формуються з об'єктів (їх копій, зображень) і (або) відомостей про них та складаються з оперативно-пошукових та інформаційно-довідкових колекцій. Криміналістичні обліки можуть вестися з використанням комп'ютерної техніки та програмного забезпечення і містити фотокопії об'єктів у вигляді їх цифрових зображень¹. Це дозволило створити криміналістичні реєстри у вигляді автоматизованих інформаційно-пошукових систем (АІПС). Прикладом такої АІПС слугує ідентифікаційна балістична система «BALSCAN» виробництва компанії Laboratory Imaging s.r.o. (Чехія), яка спеціалізується на цифровій обробці й порівняльному аналізі зображень. Ця система використовується в Україні з 2019 року. База даних системи містить зображення стріляних із зареєстрованої вогнепальної зброї куль та гільз, а також дозволяє сканувати і порівнювати сліди вогнепальної зброї навіть на деформованих кулях і їх фрагментах з метою ідентифікації конкретного екземпляра вогнепальної зброї.

Збройна агресія РФ проти України прискорила створення за допомогою системи «BALSCAN» електронної бази цифрових копій слідів вогнепальної зброї на гільзах, яка на сьогодні включає більше 600 тисяч зображень гільз зі слідами більше 200 тисяч одиниць зброї. Ці гільзи вилучені з місць вчинення правопорушень та гільз, стріляних з втраченої зброї або такої, яка зареєстрована на певних осіб².

Під час проведення ОРЗ правоохоронні органи України мають можливість отримати інформацію в цифровій формі про організаторів

¹ Інструкція з організації функціонування криміналістичних обліків Головного експертно-криміналістичного центру Державної прикордонної служби України. Затверджена Наказом Міністерства внутрішніх справ України 10.07.2017 № 580. URL: <https://zakon.rada.gov.ua/laws/show/z0957-17#Text>

² Лебідь С. О., Шевчук О. Ю. Проблеми використання балістичних обліків у розкритті злочинів в умовах воєнного стану. *Актуальні питання психологічного забезпечення службової діяльності структурних підрозділів мвс України в умовах воєнного стану* : матеріали V міжвідомчого науково-практичного круглого столу (Київ, 20 квітня 2023 року). С. 92. URL: <https://elar.naiu.kiev.ua/collections/1233252c-327f-41ef-a52a-a3cc38eeb9fe>

і учасників міжнародних організованих злочинних груп з АПС «Millennium», яка створена Міжнародною міжурядовою організацією кримінальної поліції «Інтерпол». Бази даних цієї системи містять персональні та біометричні дані, фотознімки, індивідуальні ознаки, зв'язки з організованими злочинними організаціями та ін.¹ Інтерпол надає можливість правоохоронним органам 196 країн-членів здійснювати обмін службовою інформацією захищеною мережею під назвою I-24/7 та користуватися 19 поліцейськими базами даних з цифровою інформацією про злочини та злочинців (від імен і відбитків пальців до викрадених паспортів), до яких країни мають доступ у режимі реального часу².

В базах даних Інтерполу накопичується безліч інформації у цифровій формі, яка аналізується і структурується за допомогою системи з елементами штучного інтелекту Criminal Analysis Files. На основі такого аналізу для країн-членів (в т.ч. – для України) формуються розвідувальні звіти, акумулюється соціально-демографічна інформація про злочинців (вік, стать, вид діяльності, злочинні зв'язки), а також час і місце злочинної діяльності³.

Інтерпол для правоохоронних органів країн-учасниць також надає доступ до Автоматизованої системи ідентифікації осіб за відбитками пальців AFIS та до системи розпізнавання облич за допомогою портативних пристроїв для збирання біометричних даних⁴.

Сучасні науково-технічні електронні пристрої повністю витіснили аналогові і інформація, яка ними створюється, не є безперервною, а має вигляд бінарного (двійкового) коду (є дискретною, цифровою). Цифрова інформація відрізняється від аналогової тим, що всі її копії

¹ Project Millennium. Interpol : website. URL: <https://www.interpol.int/Crimes/Organized-crime/Project-Millennium#:~:text=Facilitating%20the%20exchange%20of%20investigative,criminal%20networks%20and%20their%20activities>.

² What is INTERPOL? Interpol : website. URL: <https://www.interpol.int/Who-we-are/What-is-INTERPOL>

³ Criminal Intelligence analysis. Interpol. URL: <https://www.interpol.int/en/How-we-work/Criminal-intelligence-analysis2>

⁴ Мовчан А. В. Міжнародний досвід застосування сучасних технологій у протидії організованій злочинності. *Актуальні питання психологічного забезпечення службової діяльності структурних підрозділів МВС України в умовах воєнного стану* : матеріали V міжвідомчого науково-практичного круглого столу (Київ, 20 квітня 2023 року). С 115. URL: <https://elar.naiau.kiev.ua/collections/1233252c-327f-41ef-a52a-a3cc38eeb9fe>

(незалежно від носія) є ідентичними оригіналу. Однак цей факт не обумовлює обов'язкове визнання такої інформації належним і допустимим джерелом доказів.

Співробітникам оперативно-розшукових органів під час виконання своїх службових обов'язків доводиться використовувати цифрові фотознімки та відеозаписи, виконані свідками або потерпілими за допомогою власних мобільних телефонів. Така цифрова інформація процесуально не оформлена і може в подальшому використовуватись як докази лише за умови встановлення її автентичності (справжності). На жаль, лише деякі мобільні телефони (Samsung, Apple) залишають у своїх записах певні «мітки» (метадані), за яким судовий експерт може встановити автентичність файлу. В усіх інших випадках для отримання записів з такими «мітками» необхідно заздалегідь на телефон встановити мобільний додаток eyeWitness to Atrocities, який дозволяє робити фотографії та знімати відео, в які в момент зйомки вшиваються метадані, необхідні для підтвердження їх справжності в суді¹.

В межах МВС створено спільні групи Національної поліції України, Державної служби з надзвичайних ситуацій, Експертної служби Міністерства Внутрішніх Справ України, які виконують 3D зображення зруйнованих внаслідок російської агресії споруд. Після систематизації і аналізу таких зображень вони розміщуються в центральній підсистемі єдиної інформаційної системи Міністерства внутрішніх справ України та відтворюються через додаток «Інтерактивна мапа пошкоджень»². Співробітництво з компанією Google Maps дозволило розміщувати такі зображення на Google-картах та спостерігати панорамні зображення вулиць населених пунктів з пошкодженими спорудами за допомогою вбудованої функції Google Street View³.

¹ Welcome to eyeWitness. Україна – центр ресурсів. URL: <https://www.eyewitness.global/index>

² Бондаренко І. П., Андреев Д. В. Застосування сучасних цифрових комунікацій та інформаційних технологій у фіксації та розслідування воєнних злочинів. *Теорія та практика протидії злочинності у сучасних умовах* : матеріали Міжнародної науково-практичної конференції (21 жовтня 2022 року. Львів: Львівський державний університет внутрішніх справ, 2022. С. 54–55.

³ Створюємо карту крок за кроком. URL: https://www.google.com/intl/ru_ua/streetview/.

Для пошуку розшукуваних осіб з 2022 р. правоохоронні органи України використовують систему розпізнавання осіб за ознаками зовнішності американської компанії Clearview AI¹, а для збирання інформації про осіб за допомогою інформації з відкритих джерел – систему BigDataPeople української компанії Artelligence². З моменту повномасштабного вторгнення РФ в Україну підрозділи кримінального аналізу здійснюють ідентифікацію військових злочинців, колаборантів, зрадників, диверсантів та ін. Загалом протягом минулого року підрозділами кримінального аналізу ідентифіковано майже 5.5 тис. осіб, причетних до збройної агресії³.

Інформація у цифровій формі, отримана під час проведення ОРЗ, може слугувати основою розслідування злочинів. Певні труднощі викликає те, що в КПК норми щодо регулювання цих процесів є нечіткими. Відповідно до ч.2 ст. 84 КПК України цифрова інформація віднесена до документів/електронних документів разом з матеріалами фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі комп'ютерних даних) (п. 1 ч. 2 ст. 99 КПК) та носіями інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії (п. 3 ч.2 ст. 99 КПК)⁴.

Не зважаючи на те, що цифрова інформація характеризується високим рівнем достовірності, сутність і ознаки цифрової інформації в окремих випадках призводять до появи певних труднощів щодо її визнання допустимим і достовірним доказом. Зокрема, в Ухвалі Верховного Суду України від 29.05.2018 р. за справою №397/2588/13-к зазначено, що цифровий відеозапис, виконаний під час проведення оперативно-розшукових заходів за допомогою спеціальної техніки, був скопійований на оптичний диск і наданий до суду. Оскільки до суду наданий не оригінал, а копія цифрової інформації, суд визнав

¹ War in Ukraine. Clearview AI : website. URL: <https://www.clearview.ai/>

² Open Data matters now. Artelligence : website. URL: <https://artelligence.com/>

³ Овсянюк Д. І., Худенко Д. М. Використання підрозділами кримінального аналізу технологій розпізнавання облич та фенотипування днк в умовах воєнного стану. *Актуальні питання психологічного забезпечення службової діяльності структурних підрозділів МВС України в умовах воєнного стану*: матеріали V міжвідомчого науково-практичного круглого столу (Київ, 20 квітня 2023 року). С. 232.

⁴ Кримінальний процесуальний кодекс України від 13 квітня 2012 року №4651-VI. Редакція від 05.02.2023. URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>

її недопустимим доказом через те, що задля надання можливості дослідити відеофайл за допомогою комп'ютерної техніки, формат файлу міг бути змінений. Аналогічне рішення викладено і в Постанові Верховного Суду України від 17.03.2020 р. за справою №426/12149/17 щодо наркотичних засобів.

Для підвищення ефективності використання цифрової інформації у розкритті злочинів до КПК України бажано внести зміни і доповнення щодо більш чіткого визначення цифрових доказів, їх копій та носіїв, закріпити порядок оцінки цифрових доказів на предмет їх допустимості та достовірності.

===== 2.3. Сутність цифрових доказів і проблеми їх використання у кримінальному провадженні

На початку 1990-х років завдяки розвитку цифрових і мережевих технологій співробітники правозастосовних органів почали працювати з доказовою інформацією в електронній (цифровій) формі з різноманітних електронних пристроїв і телекомунікаційних мереж, а саме: комп'ютерів, мобільних телефонів, фото- й відеокамер, *GPS*-навігаторів, соціальних мереж, різних інтернет-сайтів та ін. Зокрема, використання даних *GPS* дає змогу встановити факт перебування підозрюваних осіб на місці скоєння злочину, а аналіз електронних листів і текстових повідомлень, цифрових фотознімків, аудіо- й відеозаписів – причетність осіб до протиправної діяльності.

Розвиток інформаційних технологій, виникнення нових галузей їх застосування та поява нових електронних пристроїв збільшили кількість видів цифрової інформації та способів її кодування й перетворення. Для перегляду й дослідження окремих видів інформації недостатньо звичайної комп'ютерної техніки зі стандартним програмним забезпеченням: для цього необхідні спеціальні електронні пристрої та спеціальне програмне забезпечення. Це спричиняє певні труднощі для слідчих, суддів, прокурорів, адвокатів, експертів та ін.