Міністерство внутрішніх справ України
Львівський державний університет внутрішніх справ

БЛАГУТА Р. І.,
МОВЧАН А. В.

# НОВІТНІ ТЕХНОЛОГІЇ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ: СУЧАСНИЙ СТАН І ПРОБЛЕМИ ВИКОРИСТАННЯ

*Монографія*

Львів
2020

УДК 351.745.7
Б68

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
*(протокол від 26 лютого 2020 р. № 7)*

**Рецензенти:**
***Ортинський В. Л.,*** *доктор юридичних наук, професор, заслужений юрист України;*
***Погорецький М. А.,*** *доктор юридичних наук, професор, заслужений діяч науки і техніки України;*
***Середа В. В.,*** *доктор юридичних наук, професор;*
***Чорноус Ю. М.,*** *доктор юридичних наук, професор*

**Благута Р. І., Мовчан А. В.**
Б68 Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання: монографія. Львів: ЛьвДУВС, 2020. 256 с.

ISBN 978-617-511-309-7

Досліджено актуальні проблеми використання новітніх технологій у розслідуванні злочинів. Викладені теоретичні висновки, практичні рекомендації та інші результати дослідження ґрунтуються на працях учених у галузі криміналістики, кримінального процесу та оперативно-розшукової діяльності, а також законодавчих і відомчих нормативно-правових актах і матеріалах практичної діяльності оперативних підрозділів Національної поліції України.

Для працівників правоохоронних органів, зокрема слідчих та оперативних підрозділів, викладачів і наукових працівників, курсантів, слухачів, а також тих, хто досліджує проблеми криміналістики, кримінального процесу та оперативно-розшукової діяльності.

The monograph examines the current problems of using the latest technologies in the investigation of crimes. The theoretical conclusions, practical recommendations and other results of the research presented in the monograph are based on the works of the scientists in the field of criminology, criminal procedure and operative-search activity, as well as legislative and departmental normative-legal acts and the materials of practical activity of the operative divisions of the National Police of Ukraine.

The work is meant for law enforcement officers, in particular, investigative and operational units, teachers and researchers, cadets, students, as well as those who investigate the problems of criminology, criminal procedure and operational and investigative activities.

**УДК 351.745.7**



**ISBN 978-617-511-309-7**

# З М І С Т

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

| | |
|---|---|
| **АІПС** | – автоматизована інформаційно-пошукова система |
| **АІС** | – автоматизована інформаційна система |
| **БпЛА** | – безпілотний літальний аппарат (дрон) |
| **ГУНП** | – Головне управління Національної поліції |
| **ДБР** | – Державне бюро розслідувань |
| **Закон про ОРД** | – Закон України «Про оперативно-розшукову діяльність» |
| **ЗМІ** | – засоби масової інформації |
| **ІІПС** | – інтегрована інформаційно-пошукова система |
| **ІП** | – інформаційна підсистема |
| **ІС** | – інформаційна система |
| **КК** | – Кримінальний кодекс |
| **КПК** | – Кримінальний процесуальний кодекс |
| **МВС** | – Міністерство внутрішніх справ |
| **НАБУ** | – Національне антикорупційне бюро України |
| **НАІС** | – Національна автоматизована інформаційна система |
| **НПУ** | – Національна поліція України |
| **НСРД** | – негласні слідчі (розшукові) дії |
| **ОГ і ЗО** | – організовані групи і злочинні організації |
| **ОРД** | – оперативно-розшукова діяльність |
| **ОРЗ** | – оперативно-розшуковий захід |
| **ОРС** | – оперативно-розшукова справа |
| **ОТЗ** | – оперативно-технічний захід |
| **ОГП** | – офіс Генерального прокурора |
| **СБУ** | – Служба безпеки України |
| **СРД** | – слідчі (розшукові) дії |
| **СТЗ** | – спеціальні технічні засоби |
| **ЄДР** | – Єдиний державний реєстр |
| **ЄРДР** | – Єдиний реєстр досудових розслідувань |
| **п.** | – пункт |
| **ч.** | – частина |
| **ст.** | – стаття |

# ВСТУП

Під час переходу третьої «цифрової» революції в четверту – промислову – відбувається вибух технологічних відкриттів. Індустрія 4.0 стирає межі між фізичними, цифровими і біологічними сферами. Йдеться про хвилю відкриттів, обумовлених розвитком можливостей встановлення зв'язку: роботи, дрони, «розумні» міста, штучний інтелект і дослідження головного мозку.

Першими кроками світу до нової промислової революції стали хмарні технології, розвиток способів збору й аналізу Big Data, краудсорсинг, біотехнології, безпілотні автомобілі і медицина, заснована на 3D-друку.

У світі фінансів це криптовалюта Bitcoin і технології Blockchain. Internet of Things – це концепція простору, у якому все з аналогового і цифрового світів може бути поєднане.

Кінцевою метою цього процесу є формування «розумного», «цифрового» суспільства і «розумної», «цифрової» держави, що припускає досягнення хоча би мінімальної соціальної справедливості, отримання всіма громадянами доступу до досягнень науково-технічної революції і, головне, – розвиток доступу до правосуддя та захисту від злочинності як традиційної, так і нового типу.

У сучасних умовах протидії організованій, транснаціональній злочинності та тероризму застосування новітніх

технологій у розкритті та розслідуванні злочинів набуває першочергового значення.

Багато десятиліть поспіль для встановлення особи громадянина поліцейським, співробітникам державних установ і банківським службовцям було потрібно перевірити посвідчення особи – паспорт. Для негласного спостереження за кимось використовували службу зовнішнього спостереження.

Науково-технічна революція надала для цього абсолютно нові можливості: тепер людину можна впізнати за відеозображенням, провести ідентифікацію за голосом, ДНК, відбитками пальців, сітківкою ока, унікальному малюнку вен на долонях та іншими параметрами. Технології GPS, мобільний зв'язок і Wi-Fi доступ в інтернет уможливили фіксацію її пересування впродовж усього маршруту слідування.

Сьогодні людина, яка проходить під об'єктивом камери або розмовляє мобільним телефоном, може і не здогадуватися, що в цей момент автоматично встановлюється її особа і координати. Сучасні технології здатні на це, не повідомляючи об'єкт.

Удосконалення біометричних систем розпізнавання особи перебуває сьогодні в одному ряду з такими актуальними напрямами, як розвиток реакторів на швидких нейтронах, суперкомп'ютерів і грід-технологій. У межах створення «розумної» поліції розпочали активно використовувати безпілотні літальні апарати та роботів-поліцейських. Криміналісти дедалі частіше застосовують 3D-технології.

На основі нейронних мереж розробляються нові поліграфи. Глобальні навігаційні системи стали невідділь-

ним елементом у розслідуванні злочинів. Водночас наявний рівень терористичних загроз, нелегальної міграції та організованої злочинності, стрімкий розвиток високих технологій вимагають нових підходів до проблем організації розкриття і розслідування злочинів.

Ці проблеми набувають особливої актуальності через низку чинників.

По-перше, це чинники соціально-правового характеру. Йдеться про демократизацію соціальних процесів, запровадження законодавчого регулювання ОРД, необхідності дотримання прав людини, захисту персональних даних.

По-друге, це чинники технічного характеру, а саме: швидкий розвиток комп'ютерної техніки, інформаційно-телекомунікаційних технологій та інноваційних систем, які використовуються для отримання, обробки та використання криміналістичної, оперативної та процесуальної інформації.

По-третє, це чинники криміногенного характеру, які обумовлені розвитком організованих форм злочинності, розбудовою її інфраструктури, наявністю корумпованих зв'язків в органах державної влади. Значного поширення набула злочинність із міжрегіональними та міжнародними зв'язками, що вимагає систематизації великих масивів інформації, отриманої з різних джерел.

Крім того, проблеми використання новітніх технологій у розслідуванні злочинів потребують правового врегулювання на законодавчому та відомчому рівнях. У зв'язку з цим автори монографії обрали мету – розглянути сучасний стан і проблеми використання новітніх технологій у розкритті й розслідуванні злочинів та окреслити напрями їх вирішення з урахуванням чинної законодавчої бази, можливостей

інноваційних систем, а також ймовірної протидії з боку правопорушників.

Сподіваємося, що монографія знадобиться вченим у галузі криміналістики, кримінального процесу та оперативно-розшукової діяльності, викладачам, здобувачам ступенів вищої освіти, працівникам правоохоронних органів, а також усім, хто цікавиться проблемами використання новітніх технологій.

## *Розділ 1*

# ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ

## 1.1. Історичні аспекти розроблення та використання новітніх технологій у розслідуванні злочинів

Як засвідчують стародавні джерела, розшук злочинців, викрадених тварин і предметів злочинного посягання здійснювався ще за часів общинно-родового ладу. Вважається, що однією з перших спроб ідентифікації та обліку злочинців було їх таврування та каліцтво. Одночасно здійснювалися функції покарання та ідентифікації злочинців (II ст. до н. е. – древньоіндійські Закони Ману, Закони Хаммурапі Древнього Вавілону)[1].

Фізичні каліцтва вказували не лише на спосіб учинення злочину, але й на кількість учинених злочинів цією особою. Перші відомості про таврування злочинців у Росії сягають XIII століття, коли злодіям на щоку накладали особливе тавро. З метою реєстрації відрубували пальці рук, відрізали вуха, носи, рвали ніздрі. Як свідчить «Соборное уложение»

[1] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Росинская Е. Р. Криминалистика: учеб. для вузов; под ред. Р. С. Белкина. 2-е изд., перераб. и доп. Москва: Норма, 2004. С. 384.

1649 року[2], за часів Петра І стали прикладати до тіла злочинців пластинку з голками, а потім у ранки втирали порох. З метою ідентифікації злочинців в Австрії та Росії намагалися випалювати на їхніх тілах цілі анкети[3].

Ці приклади, на нашу думку, були одними з перших передумов створення примітивного обліку злочинців, який, проте, мав несистематизований та децентралізований характер.

Розшук особливо небезпечних злочинців здійснювався на основі словесного портрета. В описі злочинців вирізняли особливі прикмети: «голова посечена в одном месте, а на грудях признаки, чаеть были мети», «правоя нога пробита из пищали в одном месте» тощо[4].

На початку XIX ст. в Англії і Франції інспектори поліції проводили у в'язницях так звані «ідентифікаційні паради», під час яких водили навколо себе ув'язнених, аби тренувати «фотографічну пам'ять», запам'ятовуючи обличчя раніше засуджених злочинців[5].

Тоді ж почали реєструвати злочинців за способом учинення злочинних посягань. Зокрема, в Англії видавався календар-довідник про ув'язнених лондонської Ньюгетської в'язниці, що містив біографічні дані злочинців і опис способів учинених ними злочинів.

Керівник французької кримінальної поліції Сюрте Франсуа Єжен Відок уперше створив картотеку викритих злочинців, до якої заносилися прізвище злочинця, опис зовнішності, вид учиненого злочину. Перевірку за картотекою застосовували щодо всіх, хто мешкав у готелях, заїжджих у дворах, а також

---

[2] Соборное уложение 1649 г. Памятники русского права. Вып. 6. С. 383–406.

[3] Аверьянова Т. В., Белкин Р. С., Корухов Ю. Г., Росинская Е. Р. Криминалистика: учеб. для вузов; под ред. Р. С. Белкина. 2-е изд., перераб. и доп. Москва: Норма, 2004. С. 384.

[4] Антологія сиску: в 14 т. / відп. ред. Ю. І. Римаренко, В. І. Кушерець; упоряд. Ю. І. Римаренко та ін. Київ: Знання України, 2005. Т. 1: Документи та матеріали з кримінального сиску (1397–1918 рр.), 2005. С. 109.

[5] Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. 3-е изд. Москва: Прогресс, 1991. С. 24.

обліковувалися всі прибулі іноземці. Однак ефективність використання даних картотеки була низькою[6].

Загальна історія використання новітніх технологій у розслідуванні злочинів у правоохоронних органах охоплює понад триста років: від створення регулярної поліції – до наших днів. Історію розроблення та використання новітніх технологій у розслідуванні злочинів у правоохоронних органах умовно можна розділити на п'ять основних етапів: початок XVIII ст. – жовтень 1917 р.; жовтень 1917 р. – середина 50 рр. XX ст.; середина 50 рр. XX ст. – початок 90 рр. XX ст.; початок 90 рр. XX ст. – 19 листопада 2012 р.; 20 листопада 2012 р. – наші дні.

*Перший етап використання новітніх технологій у розслідуванні злочинів охоплює початок XVIII ст. – жовтень 1917 р.* Із XVII ст. у роботах із кримінального судочинства трапляються рекомендації осіб, обізнаних у звірянні почерків, розпізнанні отрут і тих, котрі володіють медичними знаннями, що об'єднувалися у своєрідні корпорації «майстрів-письмоводів»[7].

У Франції та Італії виходять у світ перші роботи Ф. Демеля, К. Бальді, Є. Равено, присвячені дослідженням почерку. М. Мальпігі (1687 р.), Б. З. Альбінус (1764 р.), Й. К. А. Майер (1788 р.) і Я. Пуркіньє (1823 р.) здійснюють наукові дослідження в галузі вивчення папілярних узорів. Доволі докладно описує період зародження криміналістичних знань Юрген Торвальд у книзі «Вік криміналістики»[8].

Серед перших російських учених-криміналістів можна назвати Н. Орлова[9], Я. І. Баршева[10], В. Д. Спасовіча[11], А. А. Ква-

[6] Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. 3-е изд. Москва: Прогресс, 1991. С. 24.

[7] Белкин Р. С. История отечественной криминалистики. Москва: Норма, 1999. С. 1.

[8] Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. 3-е изд. Москва: Прогресс, 1991. 323 с.

[9] Орлов Н. Опыт краткого руководства для проведения следствия. Москва, 1833. 144 с.

[10] Баршев Я. И. Основания уголовного судопроизводства с применением к российскому уголовному судопроизводству. Санкт-Петербург, 1841. 298 с.

чевського[12], П. В. Макалінського[13], Е. Ф. Бурінського[14], Л. Є Владімірова[15] та ін. У їхніх працях, окрім методичних рекомендацій з тактики ведення слідства, розглядалися питання, пов'язані з ідентифікацією особи на основі вивчення різних слідів, предметів, документів та інших доказів.

У середині XVIII ст. правоохоронними органами в Україні започатковано практику використання спеціальних хімічних речовин для виявлення записів на папері, виконаних у неявний спосіб (за допомогою невидимих, так званих «хімічних» чорнил)[16].

У практиці боротьби зі злочинністю набув поширення розроблений А. Бертільоном у 1882 році антропологічний метод реєстрації й ототожнення злочинців (бертільйонаж), який полягав у обмірюванні їхнього росту, розмірів голови, довжини рук, пальців, ступнів тощо. Систематизовані картки з даними обмірювання злочинців давали змогу за кілька хвилин установити, чи містяться в картотеці дані про будь-якого затриманого[17].

Крім того, Бертільон запровадив обов'язкову фотозйомку кожного затриманого злочинця в анфас і профіль, а також

---

[11]Спасович В. Д. О теории судебно-уголовных доказательств в связи с судоустройством и судопроизводством. Санкт-Петербург, 1861. 92 с.

[12] Квачевский А. А. Об уголовном преследовании, дознании и предварительном исследовании преступлений по судебным уставам 1864 г. Санкт-Петербург, 1867.

[13] Макалинский П. В. Практическое руководство для судебных следователей, состоящих при окружных судах. Санкт-Петербург: Типография Н. А. Лебедева, 1890. Т. 1. 400 с. Т. 2. 775 с.

[14] Буринский Е. Ф. Судебная экспертиза документов, производство ее и пользование ею. Санкт-Петербург: Тип. СПб. т-ва печ. и изд. дела «Труд», 1903. 386 с.

[15] Владимиров Л. Е. Учение об уголовных доказательствах: учебное пособие. Санкт-Петербург: Издание книжного магазина Законоведение, 1910. 331 с.

[16] Пиджаренко А. М. История и тайны уголовного и политического сыска. Киев: Юринформ, 1994. С. 52.

[17] Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. 3-е изд. Москва: Прогресс, 1991. С. 29–30.

складання «словесного портрета», який заносився до облікової картки.

Видимі характерні ознаки кожної особи описувалися за допомогою спеціальних формул, які в подальшому використовувалися за проведення «парадів арештантів» для розпізнавання затриманих[18].

«Словесний портрет» Бертільона був удосконалений у 1905 році швейцарським професором Р. А. Рейссом, який застосував цифровий код для передачі даних телеграфом, що значно пришвидшувало розшук злочинців.

1887 року В. Гершель і Г. Фолдс запропонували відбирати відбитки пальців рук у всіх злочинців із метою ідентифікації особи[19]. У 1891 році Ф. Гальтон довів, що, згідно з теорією ймовірності, збіг відбитків пальців рук двох людей практично неможливий[20].

Важливу роль у практиці боротьби зі злочинністю виконали картотеки злочинців, які виникли у 80-х роках XIX століття і актуальні дотепер. Зокрема, наприкінці 1896 року Е. Р. Генрі знайшов спосіб упорядкувати в картотеках мільйони карток із відбитками пальців. Із 1901 року у Скотланд-Ярді функціонувала перша в Європі дактилоскопічна картотека, яка стала основою побудови відповідних обліків криміналістичного та оперативного призначення[21]. Пізніше з'явилися картотеки, побудовані за іншими принципами ідентифікації осіб (за почерком, ознаками зовнішності, татуюванням, фотопортретом тощо).

Однією з перших була створена механічна система картотечної обробки інформації у Федеральному бюро розслідувань

---

[18] Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. 3-е изд. Москва: Прогресс, 1991. С. 29–30.

[19] Кобзар С. І., Сегай М. Я. Криміналістичне дослідження слідів рук людини (праксіологічний аспект): монографія. Луганськ: РВВ ЛДУВС, 2006. 208 с.

[20] Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. 3-е изд. Москва: Прогресс, 1991. С. 55.

[21] Дубовий О. П., Лукашенко В. Я., Рибалко Я. В. Криміналістичне дослідження слідів рук: науково-практичний посібник; за заг. ред. Я. Ю. Кондратьєва. Київ: Атіка, 2000. С. 10–11.

США. Дані про злочинців заносилися до спеціальних карток, на яких, крім анкетних відомостей, зазначалася злочинна «спеціалізація» кожного фігуранта картотеки, яка фіксувалася шляхом перфорації відповідного поля картки. За необхідності відбору підозрюваних за сукупністю певних ознак крізь відповідні отвори карток протягувалися металеві спиці й таким відбиралися розшукувані особи[22].

Місцеві обліки злочинців, солдатів-дезертирів, осіб, які ведуть підозрілий спосіб життя, облік карткових та інших «злачних» закладів, осіб, які прибували і вибували з міст, що використовувалися для аналізу криміногенної обстановки та розкриття неочевидних злочинів, з'явилися в поліцейських установах Росії ще в XVIII ст. Для виявлення осіб, які підлягали постановці на облік, проводилися спеціальні облави[23].

Можливості фотографії в поліцейській реєстрації почали використовувати ще в 60-х роках XIX ст. У 1862 році при санктпетербурзькій поліції було організовано фотографічне бюро для зйомки обвинувачених з метою встановлення їх особи. В Україні перше поліцейське фотоательє з'явилося в 1864 році у м. Бобринці Одеської губернії (нині Кіровоградської обл.). 1890 року при петербурзькій сискній поліції вперше з'явилися спеціальні підрозділи, які здійснювали дактилоскопіювання, фотографування злочинців і систематизацію інших даних про них. Дещо пізніше, у 1896 році, там же був заснований стіл знахідок. У цей же період була організована реєстрація осіб, які володіють холодною зброєю[24].

У 1902 році при сискній поліції почав створюватися облік швейцарів, двірників, службовців питних закладів і візників. Тоді ж у Петербурзі була створена картотека фотографій

---

[22] Костин В. П. Тайная полиция США. ФБР: прошлое и настоящее. Москва: Мысль, 1986. 284 с.

[23] Наша служба уголовный розыск: историко-художественно-публицистический сборник к 80-летию уголовного розыска России. Москва: Олимп, 1998. С. 36.

[24] Криміналістика (криміналістична техніка): курс лекцій / П. Д. Біленчук, А. П. Гель, М. В. Салтевський, Г. С. Семаков. Київ: МАУП, 2001. 216 с.

злочинців, які систематично здійснювали крадіжки. Упродовж року на облік ставилося до 5 тисяч злочинців[25].

Доволі помітне місце у практиці поліції в той період посідав метод кримінальної реєстрації за способом учинення злочинів (Modus operandi). Він був ефективний у реєстрації злочинців-професіоналів, особливо «гастролерів»[26].

Відомий криміналіст М. Н. Гернет зазначав, що професійна злочинність передбачає чітко виражений поділ злочинної діяльності та чисельні категорії «спеціалістів». Вона знає своїх «робітників» і своїх «підприємців», має свою «професійну» честь і «солідарність». Найбільш наочно цей поділ простежувався у професійних злодіїв. До жовтня 1917 року злочинний світ налічував більше 50 злодійських «професій»[27].

У цей період з'явилися перші теоретичні роботи, присвячені криміналістичному обліку й реєстрації. Так, відомий австрійський юрист і кримінолог Ганс Гросс у посібнику «Руководство для судебных следователей как система криминалистики» розглянув основи обліку злочинців із використанням антропометричної та дактилоскопічної інформації[28].

Уже в 1902 році спецслужби царської Росії володіли алфавітною картотекою, що налічувала 65 тисяч облікових карток, а архіви містили до 200 тисяч фотографій «державних злочинців» та алфавітні списки осіб, які перебували під негласним наглядом поліції, з фотографіями[29].

---

[25] Елинський В. И. Основы методологии теории оперативно-розыскной деятельности: монография. Москва: Изд. Шумилова И. И., 2001. С. 40–41.

[26] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И. И., 2005. С. 24.

[27] Преступный мир Москвы / под ред. М. Н. Гернета. [Репринтное издание. Ржев, Типография Укоммунотдела 1924 г.]. Москва: ЛЮКОН, 1991. С. 24.

[28] Гросс Г. Руководство для судебных следователей как система криминалистики. [Новое изд., переп. с изд. 1908 г.]. Москва: ЛексЭст, 2002. С. 323–334.

[29] Линдер И. Б., Чуркин С. А. Спецслужбы России за 1000 лет. Материалы секретных фондов. Москва: РИПОЛ классик, 2006. С. 416–417.

Відповідно до «Інструкції чинам Київської сискної поліції» (затвердженої в січні 1905 р.), до складу поліції входило розшукове відділення, спеціальними завданнями якого були: реєстрація всіх злочинців і підозрюваних осіб, ототожнення особи злочинця за допомогою антропологічного дослідження, а також реєстрація візників, швейцарів, двірників і сторожів[30].

Відомий криміналіст В. І. Лєбєдєв видав книгу «Искусство раскрытия преступлений»[31], яка містила докладні наукові відомості про дактилоскопію, антропометрію, судово-поліцейську фотографію.

У 1914 році Департаментом поліції був виданий «Розыскной альбом», який містив систематизовані відомості про злочинців-професіоналів. Першоосновою цього альбому слугував «Справочный указатель для чинов полиции» В. І. Лєбєдєва (виданий у 1903 році)[32], що містив світлини та описи особливих прикмет одинадцяти категорій професійних злочинців.

1915 року С. М. Трєгубов опублікував практичний посібник для судових слідчих «Основы уголовной техники. Научно-технические приемы расследования преступлений»[33], який містив обсяжні відомості, що стосувалися кримінальної реєстрації.

Підсумовуючи перший етап розроблення і використання новітніх технологій у розслідуванні злочинів, слід зазначити, що спочатку їхніми основними формами були ідентифікація (криміналістична) і діагностика (судово-медична, криміналістична, кримінологічна). Водночас з'явилися перші знання

---

[30] Чисніков В. М. Правові витоки карно-розшукової служби України (історичний аспект). Теорія оперативно-службової діяльності правоохоронних органів України / за ред. В. Л. Регульського. Львів: Львів. ін-т внутр. справ, 2000. С. 307.

[31] Лебедев В. И. Искусство раскрытия преступлений. Москва, 1912. 218 с.

[32] Лебедев В. И. Справочный указатель для чинов полиции. Москва: Тип. Н. И. Пастухова, 1903. 165 с.

[33] Трегубов С. Н. Основы уголовной техники. Научно-технические приемы расследования преступлений. Новое изд., переп. с изд. 1915 г. Москва: ЛексЭст, 2002. 336 с.

в галузі криміналістичного прогнозування, почав зароджуватися прообраз і такої комплексної форми, як кримінальний аналіз[34].

На наш погляд, до характерних особливостей першого етапу розроблення і використання новітніх технологій у розслідуванні злочинів слід віднести: запровадження дактилоскопії в практику роботи поліцейських служб, централізацію обліків і створення реєстраційної мережі.

*Другий етап використання новітніх технологій у розслідуванні злочинів – це жовтень 1917 р. – середина 50 рр.* Означений період характеризується подальшим розвитком криміналістичних та інших наукових знань, що використовувалися у розслідуванні злочинів, в основі діяльності якого лежали ті ж основні методи, які застосовував колишній кримінальний сиск Російської імперії.

Серед учених, які зробили суттєвий внесок у розвиток криміналістики на цьому етапі, можна виокремити В. І. Громова[35], Г. Ю. Маннса[36], С. М. Потапова[37], П. С. Семеновського[38], І. М. Якімова[39] та ін.

У 1917 році було знищено більшу частину обліків охоронних і сискних відділень, що суттєво вплинуло на результати боротьби зі злочинністю. Причому вершилось це як представниками старої влади, так і звільненими за амністією кримінальними злочинцями. Різке зростання рівня злочинності

[34] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И. И., 2005. С. 12.

[35] Громов В. И. Методика расследования преступлений: руководство для органов милиции и уголовного розыска. Москва: Издательство НКВД РСФСР, 1930. 136 с.

[36] Маннс Г. Ю. Общее и специальное предупреждение в уголовном праве. Иркутск: Тип. изд-ва «Власть труда», 1926. 72 с.

[37] Потапов С. М. Принципы криминалистической идентификации. Москва: Сов. гос. и право, 1940. № 1.

[38] Семеновский П. С. Дактилоскопия как метод регистрации. Москва: Розыск республики, 1923. 113 с.

[39] Якимов И. Н. Криминалистика. Уголовная тактика. М.: Издательство НКВД РСФСР, 1929. 312 с.

призвело до того, що, приміром, у Москві кількість убивств перевищила довоєнний рівень у 10–15 раз[40].

28 жовтня 1917 року (за старим стилем) постановою НКВС «О рабочей милиции» була створена робітнича міліція. Дактилоскопічна та алфавітна реєстрація злочинців розглядалися як найважливіші засоби боротьби зі злочинністю. 1919 року створюється Центральне реєстраційне бюро і реєстраційні бюро в республіканських і губернських відділах та відділеннях карного розшуку[41].

Постановою НКЮ України від 11 травня 1919 року було введено в дію Положення про органи карного розшуку й судово-карної міліції, згідно з яким до Центральної секції судово-кримінального розшуку ввійшло реєстраційне бюро, яке займалося обліком реєстраційних і розшукових карток, дактилоскопічних листків злочинців і відповідало на запити місцевих секцій карного розшуку щодо встановлення судимості затриманих злочинців[42].

В Україні налічувалося 40 реєстраційно-дактилоскопічних бюро, у великих містах – Харкові, Києві, Одесі, Дніпропетровську – реєстраційний апарат було передано до міських управлінь міліції та розшуку. За загальним правилом, реєстраційні бюро обслуговували всю територію округу, проводячи реєстрацію злочинного елементу та письмового розшуку[43].

---

[40] Наша служба – уголовный розыск: историко-художественно-публицистический сборник к 80-летию уголовного розыска России. Москва: Олимп, 1998. С. 37.

[41] Выступление начальника главного информационно-аналитического центра МВД России генерал-майора милиции Сергея Перова на страницах газеты «Щит и меч». URL: http://www.mvdinform.ru.

[42] Чисніков В. М. Правові витоки карно-розшукової служби України (історичний аспект). Теорія оперативно-службової діяльності правоохоронних органів України / за ред. В. Л. Регульського. Львів: Львів. ін-т внутр. справ, 2000. С. 302–309.

[43] Антологія сиску: в 14 т. / відп. ред. Ю. І. Римаренко, В. І. Кушерець; упоряд. Ю. І. Римаренко та ін. Київ: Знання України, 2005. Т. 1: Документи та матеріали з кримінального сиску (1397–1918 рр.). 2005. С. 58.

У 1919 році з'являються перші криміналістичні музеї, які систематизували колекції знарядь злочину, слідів, залишених на місці події, підроблених документів тощо. У музеях накопичувалися відомості, які характеризували прийоми та способи вчинення різних злочинів, прикмети і фотографії злочинців, інші відомості, що сприяли їх установленню, розшуку та затриманню[44].

У той період підрозділами карного розшуку активно практикувалися фотографування і дактилоскопіювання злочинців. 1920 року було створено централізований облік розшукуваних злочинців і осіб, які зникли безвісти, розроблена детальна класифікація злочинців, практична цінність і пізнавальне значення якої актуальні і в даний час[45].

У 1920-х рр. були підготовлені та направлені на місця такі аналітичні розробки, як «Руководство по дактилоскопии», «Руководство по судебной медицине», словник злодійської мови «Блатная музыка»[46].

На початку 30-х років минулого століття із апаратів карного розшуку були виділені науково-технічні підрозділи, які в подальшому, у 1948 році, перетворені в самостійні структурні підрозділи міліції[47].

З'являються перші систематизовані знання, пов'язані з теорією криміналістичного прогнозування. Зокрема, Б. М. Шавер зазначав, що на основі вивчення конкретних даних про розслідування окремих категорій злочинів «можна визначити ще не розкриті, але можливі способи і прийоми вчинення злочинів»[48].

---

[44] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И.И., 2005. С. 14.

[45] Там само.

[46] Там само.

[47] Галахов С. С., Комарова Е. В. Этапы становления информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел. Научный портал МВД России. 2008. № 1. С. 61.

[48] Голунский С. А., Шавер Б. М. Криминалистика. Методика расследования отдельных видов преступлений. Москва: Юрид. изд.-во НКЮ СССР, 1939. С. 9.

1934 року О. Є. Брусіловський та М. С. Строгович висловили пропозицію про доцільність застосування магнітного звукозапису в кримінальному процесі[49].

У 1935 році після об'єднання органів ОДПУ та міліції криміналістичні обліки із карного розшуку перейшли у підпорядкування Особливого бюро НКВС СРСР[50].

У лютому 1941 року відбувся поділ НКВС колишнього СРСР на два самостійних наркомати: НКВС і НКДБ. Перший спецвідділ увійшов у структуру Наркомату внутрішніх справ, до його складу були передані централізована оперативно-довідкова картотека та архів, з Головного управління міліції – алфавітна та дактилоскопічна картотеки централізованого обліку злочинців, з ГУЛАГу – картотеки централізованого обліку ув'язнених. Обліково-реєстраційні відділення й бюро, що перебували з 1918 року у складі підрозділів карного розшуку управлінь міліції областей і країв, були переведені в систему перших спецвідділів наркомату[51].

У 1952 році відбулося організаційне розмежування в рядах Всесоюзної наукової спілки судових медиків і криміналістів, що призвело до певної дезінтеграції наукових знань у зазначених областях[52].

*Третій етап* використання новітніх технологій у розслідуванні злочинів *становив середину 50-х рр. – початок 90-х рр.*

Із 1950-х років до 1981 року науково-технічні підрозділи органів внутрішніх справ функціонували як структурні підроз-

---

[49] Брусиловский А. Е., Строгович М. С. Свидетельские показания в качестве судебных доказательств. Методика и техника следственной работы / под ред. Г. К. Рогатинского и А. В. Викторова. Киев: Советское строительство и право, 1934. С. 161.

[50] Яковец Е. Н. Из истории развития информационно-аналитической деятельности органов политического и уголовного сыска России. Академия русской символики «Марс». Москва, 2008. № 7. URL: http://www.geraldika. jrg/07_2008_42.htm

[51] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И. И., 2005. С. 16.

[52] Там само.

діли різних служб МВС колишнього СРСР. Відповідно до наказу МВС СРСР № 474-1968 р., на науково-технічні підрозділи було покладено обов'язки розроблення криміналістичних методів і засобів під час ужиття оперативно-розшукових заходів, реалізації агентурних розробок оперативними підрозділами МВС[53].

Однією із форм участі експертів в оперативно-розшуковій діяльності було застосування спеціальних хімічних речовин для попередження і розкриття крадіжок й інших злочинів, так званих «хімічних пасток».

У 1970 році експертно-технічні підрозділи було об'єднано з підрозділами оперативної техніки та зв'язку. Наказом МВС СРСР від 06.03.1970 р. № 65 затверджено Положення про проведення експертиз у криміналістичних підрозділах органів МВС. У 1970-х роках активно розвивається портретна ідентифікація особи методом суб'єктивного портрета[54].

Наказом МВС СРСР № 0155-1973 р. було запроваджено в практику роботи криміналістичних підрозділів ІПС «Слід» для перевірки слідів пальців рук за масивами дактилокарт із використанням ЕОМ[55].

В органах внутрішніх справ із початку 70-х років минулого століття пішли шляхом створення алфавітних картотек на різні категорії осіб. Усього існувало до 70 видів алфавітних картотек. Із метою централізації оперативно-розшукової інформації було створено систему інформаційних центрів, що зосередили більше тридцяти картотек ручного пошуку (за кличками, п'яницями, небезпечними рецидивістами, власниками нелегальних квартир тощо)[56].

---

[53] Пєчніков В. С. Є така служба…; в 2 т. / за ред. І. П. Красюка. Київ, 2011. Т. 1. Ч. 1. С. 15.

[54] Зинин А. М. Фоторобот (история создания и внедрения в практику органов внутренних дел). 85 лет Экспертно-криминалистической службе органов внутренних дел России: сб. ст. Москва, 2004. С. 218–230.

[55] Пєчніков В. С. Є така служба… У 2 т. / за ред. І. П. Красюка. Київ, 2011. Т. 1. Ч. 1. С. 391.

[56] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И. И., 2005. С. 99.

Витоки ще однієї діагностичної складової сягають судової медицини. Суть будь-якої діагностики полягає в тому, що на основі розпізнавання об'єкта, схожого з уже відомими подібними об'єктами, визначаються його властивості, стан, зміни, зв'язки із зовнішнім середовищем тощо. Принциповою відмінністю діагностики від ідентифікації є та обставина, що «за ідентифікації робота на аналітичній стадії відбувається з урахуванням ступеня зіставлення двох об'єктів: шуканого і того, що перевіряють. У діагностиці об'єкта, котрий перевіряють, немає, його ще потрібно знайти. На аналітичній стадії діагностичного процесу йдеться про виокремлення ознак тільки шуканого об'єкта» [57].

Упровадження ЕОМ призвело до створення перших автоматизованих інформаційно-пошукових систем оперативно-розшукового призначення, таких як «Облік» (наказ МВС СРСР № 0483–75 р.) і «Розшук» (наказ МВС СРСР № 0375–70 р.), і підсистем «Сигнал», «Фільтр», «Мережа». Вони замінили наявні картотеки та облікові справи, увели єдину термінологію для опису оперативно-тактичних, криміналогічних і криміналістичних понять і явищ, детально програмували збирання інформації та індивідуально-профілактичну роботу з особами, поставленими на облік[58].

Істотний внесок у розроблення наукових методик, пов'язаних із аналізом оперативної обстановки та діагностичним аналізом злочину, – основними видами діагностичної складової дослідження предметів і документів – був здійснений у 70–80-і рр. відомими вченими Д. В. Гребельським[59],

[57] Корухов Ю. Г. Криминалистическое распознавание и криминалистическая диагностика: содержание и соотношение понятий. Уголовный процесс и криминалистика на рубеже веков. Москва: Академия управления МВД России, 2000. С. 112.

[58] Овчинский С. С. Оперативно-розыскная информация; под ред. А. С. Овчинского, В. С. Овчинского. Москва: ИНФА, 2000. С. 118.

[59] Гребельский Д. В. Теоретические основы и организационно-правовые проблемы оперативно-розыскной деятельности органов внутренних дел. Москва: РИО Акад. МВД СССР, 1977. 170 с.

В. А. Лукашовим[60], С. С. Овчинським[61], К. Г. Синіловим[62] та іншими.

На початку 80-х рр. була розроблена методика комплексного економіко-правового аналізу господарської діяльності об'єктів, об'єднань, галузей народного господарства, що передбачала вивчення проблем забезпечення збереження соціалістичної власності та розроблення заходів щодо попередження безгосподарності, розкрадань, посадових і господарських злочинів[63].

Водночас ставлення до АІС оперативно-розшукового призначення в державі було неоднозначним. Так, у 70-і роки була створена доволі ефективна інформаційно-аналітична система «Паспорт», яка давала змогу фіксувати й накопичувати інформацію про всі переміщення громадян через кордони СРСР. За допомогою цієї системи були розкриті резонансні злочини щодо незаконного вивозу антикваріату та ювелірних виробів із країни, а також контрабанди у великих розмірах, однак швидко система була ліквідована за вказівкою вищого керівництва держави як така, що «порушує права людини»[64].

За створення АІПС спеціалісти намагалися зважати на розумне поєднання технічних можливостей обчислювальних засобів та інтелектуально-логічного мислення людини. Н. Вінер писав: «...віддайте ж людині людське, а обчислювальній машині – машинне. У цьому й повинна, очевидно, полягати

[60] Лукашов В. А. Организация и методика информационно-аналитической работы в сфере оперативно-розыскной деятельности органов внутренних дел: лекция. Омск: ОВШМ МВД СССР, 1983. 32 с.

[61] Овчинский С. С. Оперативно-розыскная информация; под ред. А. С. Овчинского, В. С. Овчинского. Москва: ИНФА, 2000. 367 с.

[62] Синилов Г. К. Правовые, информационные и тактические основы ОРД советской милиции. Москва, 1975. 320 с.

[63] Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И. И., 2005. С. 21.

[64] Выступление начальника главного информационно-аналитического центра МВД России генерал-майора милиции Сергея Перова на страницах газеты «Щит и меч». URL: http://www.mvdinform.ru.

розумна лінія поведінки в організації спільних дій людей і машин»[65].

У 70-х роках минулого століття було створено Республіканський науково-дослідний інформаційний центр МВС УРСР, до основних напрямів діяльності якого належали: надання оперативно-довідкової, розшукової, статистичної та іншої інформації; збирання, обробка, зберігання, аналіз інформації про злочини та осіб, які їх учинили; розгляд матеріалів про оголошення та припинення розшуку осіб, які зникли безвісти, невпізнаних трупів, а також розшуку втрачених і виявлених номерних речей, зброї тощо. Першими автоматизованими інформаційними системами були «Профілактика-Розшук», «Розшук», «Статистика» та інші. У 90-і роки на озброєння правоохоронних органів України були взяті такі комп'ютерні мережні системи, як «Бінар», «Кронус», «Єрмак», «Кондор», «Аскрін», «Легенда» та інші, що мали значно вищі пошуково-аналітичні можливості[66].

Упродовж 1981–1991 років триває становлення і розвиток самостійних експертно-криміналістичних підрозділів у системі МВС. Зокрема, у листопаді 1981 року утворено Експертно-криміналістичне управління МВС УРСР, що створювало передумови для покращення використання наукових методів і технічних засобів у протидії злочинності.

У 1985 році в практику боротьби зі злочинністю втілено геномний метод ідентифікації людини за ДНК, який вважається одним із найбільш значних досягнень криміналістики XX ст.[67].

Для обробки, зберігання та використання оперативної інформації розпочали застосовувати потужні автоматизовані інформаційні системи. Особливо це виявилося в діяльності

---

[65] Овчинский С. С. Оперативно-розыскная информация под ред. А. С. Овчинского, В. С. Овчинского. Москва: ИНФА, 2000. С. 82–83.

[66] Департамент інформаційно-аналітичного забезпечення. URL: http://www.mvs.gov.ua/mvs/control/mai0n/uk/publish/article/544651.

[67] Берназ В. Д. Інтеграція досягнень сучасної науки в слідчу діяльність. *Південноукраїнський правничий часопис.* 2008. Вип. № 4. С. 189–191.

правоохоронних органів, пов'язаній з протидією організованій злочинності, що набуло значної актуальності в кінці 80-х – початку 90-х років минулого століття. Цей період відзначався бурхливими подіями в суспільно-політичному та економічному житті на теренах колишнього СРСР, зокрема й в Україні. Означені події супроводжувалися значним підвищенням рівня злочинності, особливо її організованих форм.

Характерною особливістю третього етапу стала комп'ютеризація криміналістичного та інформаційно-аналітичного забезпечення оперативних підрозділів і підрозділів досудового розслідування, запровадженням ДНК-аналізу, що ознаменувало революцію в технологіях отримання, обробки, систематизації, аналізу та використання криміналістичної, оперативно-розшукової та процесуальної інформації.

*Четвертий етап використання новітніх технологій у розслідуванні злочинів охоплював початок 90-х рр. – 19 листопада 2012 р.* Цей етап використання новітніх технологій у розслідуванні злочинів пов'язаний з проголошенням незалежності України, структурною перебудовою оперативних та експертно-криміналістичних підрозділів і підрозділів досудового розслідування.

З 1991 року започатковано сучасний розвиток Експертної служби МВС України. Наказом МВС України від 09.03.1992 р. № 140 затверджено Положення про діяльність експертно-криміналістичних підрозділів. У 1993 році ухвалено рішення про створення лабораторії молекулярно-генетичної експертизи. Для розслідування злочинів, учинених із застосуванням вибухових пристроїв, наказом МВС України від 13.06.1995 р. створено вибухотехнічні підрозділи.

У цей період в Україні були створені науково-дослідні інститути судових експертиз Міністерства юстиції в Києві, Харкові, Одесі, Львові, Донецьку, Дніпропетровську, Сімферополі, а також низка відділень НДІСЕ.

Постановою Кабінету Міністрів України від 20 червня 2000 р. № 988 утворено Експертну службу Міністерства внутрішніх справ як систему експертних підрозділів, до якої входи-

ли: ДНДЕКЦ МВС України, НДЕКЦ при ГУМВС АР Крим, у м. Києві та Київській області, УМВС в областях, м. Севастополі та на транспорті.

З огляду на важливу роль застосування оперативно-технічних заходів для протидії злочинності, у 1994 році було створено Оперативно-технічне управління МВС України, яке 2002 року реорганізовано в Департамент оперативно-технічних заходів при МВС України, та відповідні підрозділи на місцях, до основних функцій яких уходить виконання завдань оперативних підрозділів з провадження оперативних розробок і кримінальних справ із негласним використанням оперативно-технічних засобів. У 2011 році ДОТЗ реорганізовано в Головне управління оперативно-технічних заходів ДКМ МВС, а 2012 року знову перетворено в Департамент оперативно-технічних заходів.

У правоохоронних органах України було розроблено та затверджено низку відомчих інструкцій, які слугують нормативно-правовою базою для проведення експертних досліджень із використанням поліграфа.

Подальше дослідження проблем використання новітніх технологій у розслідуванні злочинів знаходимо в наукових працях Ю. П. Аленіна[68], О. М. Бандурки[69], В. П. Бахіна[70], О. А. Белова[71], В. Д. Берназа[72], В. В. Бірюкова[73], Т. В. Варфоло-

[68] Аленін Ю. П. Теоретичні та практичні основи розкриття і розслідування осередків злочинів: автореф. … д-ра юрид. наук: 12.00.09. Харків, 1997. 48 с.

[69] Бандурка А. М., Горбачев А. В. Оперативно-розыскная деятельность: правовой анализ. Киев: РИО МВД Украины, 1994.160 с.; Бандурка О. М. Оперативно-розшукова діяльність. Частина І: підруч. Харків: Видво Нац. ун-ту внутр. справ, 2002. 336 с.

[70] Бахин В. П. Криминалистика: проблемы и мнения (1962–2002 гг.). Киев: [б. и.], 2002. 266 с.

[71] Белов О. А. Информационное обеспечение раскрытия и расследования преступлений: монография. Москва: Юрлитинформ, 2009. 136 с.

[72] Берназ В. Д. Інтеграція досягнень сучасної науки в слідчу діяльність. *Південноукраїнський правничий часопис.* 2008. Вип. № 4. С. 189–191.

меєвої[74], А. Ф. Волобуєва[75], А. В. Іщенка[76], Н. І. Клименко[77], В. К. Лисиченка[78], В. Г. Лукашевича[79], Є. Д. Лук'янчикова[80], Д. Й. Никифорчука[81], А. С. Овчинського[82], В. С. Овчинсь-

[73] Бірюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: монографія. Луганськ: ЛДУВС, 2009. 664 с.

[74] Експертизи у судовій практиці / КНДІСЕ, Акад. адвокатури України: наук.-практ. посібник; за заг. ред. В. Г. Гончаренка. 2-ге вид., перероб. і доп. Київ: Юрінком Інтер, 2010. 400 с.

[75] Волобуєв А. Ф. Про використання поліграфа при розслідуванні злочинів. Криміналістика XXI століття: матеріали Міжнар. наук.-практ. конф. (Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 110–113.

[76] Див.: Іщенко А. В., Красюк І. П., Матвієнко В. В. Проблеми криміналістичного забезпечення розслідування злочинів: монографія. Київ: Нац. акад. внутр. справ України, 2002. 212 с.; Іщенко А. В. Методологічні проблеми криміналістичних наукових досліджень: монографія; за ред. І. П. Красюка. Київ: НАВСУ, 2003. 359 с.

[77] Клименко Н. І. Криміналістичні знання: поняття, структура, розвиток. Криміналістика XXI століття*:* матеріали Міжнар. наук.-практ. конф. (Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 29.

[78] Лисиченко В. К., Шехавцов Р. М. Проблеми теорії та практики подолання протидії розслідуванню окремих різновидів злочинів, вчинених організованими групами, злочинними організаціями: монографія; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. 2-ге вид., переробл. та доповн. Луганськ, 2012. 319 с.

[79] Лукашевич В. Г., Юнацький О. В. Моделювання у криміналістиці та пізнавальній діяльності слідчого: монографія. Київ, 2008. С. 6–7.

[80] Лук'янчиков Є. Д. Інформаційне забезпечення розслідування злочинів (правові і тактико-криміналістичні аспекти): автореф. дис. на здобуття наук. ступеня доктора юрид. наук: спец. 12.00.09. Київ, 2005. 38 с.; Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів: монографія. Київ: Нац. акад. внутр. справ України, 2005. 360 с.

[81] Никифорчук Д. Й., Бусол О. Ю. Проведення аналізу оперативно-розшукової інфомації: монографія. Кіровоград: ТОВ «Поліграф-Сервіс», 2010. 165 с.

[82] Див.: Овчинский А. С., Каретников М. К. Проблемы подготовки специалистов в области применения современных информационных технологий. Вестник МВД России, 2000. № 4–5. С. 130–131; Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. Москва: ИНФРА-М, 2000. 367 с.; Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / под ред. В. И. Попова. Москва: ИНФРА-М, 2002. 97 с.

кого[83], С. С. Овчинського[84], Ю. Ю. Орлова[85], В. Л. Ортинського[86], М. А. Погорецького[87], М. В. Салтевського[88], В. В. Тіщенка[89], Л Д. Удалової[90], В. Г. Хахановського[91], І. Ф. Харабе-рюша[92], В. М. Шевчука[93], В. Ю. Шепітька[94], Р. М. Шехавцова[95],

---

[83] Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. Москва: ИНФРА-М, 2000. 367 с.

[84] Там само.

[85] Орлов Ю. Ю. Застосування лазерного сканування під час огляду місця події. *Науковий вісник Національної академії внутрішніх справ*. 2011. № 4. С. 196–201.

[86] Ортинський В. Л. Протидія нелегальній економіці засобами оперативно-розшукової діяльності: монографія. Львів, 2004. 436 с.

[87] Див.: Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96; Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Харків: Арсіс ЛТД, 2007. 576 с.

[88] Салтевський М. В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2008. 588 с.

[89] Тищенко В. В. Система криминалистики: проблемы оптимизации. *Криміналістика XXI століття*: матеріали Міжнар. наук.-практ. конф. (Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 46–50.

[90] Удалова Л. Д. Теорія та практика отримання вербальної інформації у кримінальному процесі України: монографія. Київ, 2005. С. 171.

[91] Хахановський В. Г. Теорія і практика криміналістичної інформатики: автореф. дис. … д-ра юрид. наук: 12.00.09. Київ, 2011. 28 с.

[92] Харабе рюш І. Ф. Використання спеціальної техніки щодо протидії злочинності в Україні: теоретичні, правові та організаційні аспекти: монографія. Донецьк, 2011. 234 с.

[93] Шевчук В. М. Современные тенденции противодействия контрабанде наркотических средств в Украине (криминалистический анализ). *Збірник наукових праць Харківського Центру вивчення організованої злочинності спільно з Американським університетом у Вашингтоні*. 2004. Вип. 9. С. 230–277.

[94] Шепітько В. Ю. Природа і предмет вивчення криміналістики в системі наукового знання. Вибрані твори. Харків, 2010. С. 16.

[95] Шехавцов Р. М. Впровадження технологій 3D-моделювання у розслідуванні злочинів: правові та криміналістичні проблеми. Криміналістика XXI століття: матеріали Міжнар. наук.-практ. конф. (м. Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 167.

К. О. Чаплинського[96], С. С. Чернявського[97], О. М. Юрченка[98] та інших вчених.

Важливу роль у координації діяльності правоохоронних органів різних країн виконує Інтерпол – Міжнародна організація кримінальної поліції (International Criminal Police Organization), членами якої є понад 190 держав світу. Історія Інтерполу бере початок із першого з'їзду кримінальної поліції 14–18 квітня 1914 року в Монако, коли юристи та працівники поліції 14-ти держав досягли домовленості про створення центрального міжнародного банку даних і визначили процедуру передачі злочинців іноземній державі. Основу діяльності Інтерполу становлять потужні обчислювальні центри, які постійно накопичують і опрацьовують величезні масиви інформації[99].

У червні 1998 року уряди держав-членів Європейського Союзу ратифікували Конвенцію про заснування Європолу – Європейського поліцейського офісу (European Police Office). З метою запобігання та протидії злочинності в Європолі створено комп'ютеризовану інформаційну систему, в якій зберігаються неособисті та особисті дані. Угоду між Україною і Європолом про стратегічне співробітництво підписано 2009 року.

Цей етап характеризується створенням обліків міжвідомчого характеру, розвитком міждержавних обліків, використанням інтегрованих банків Інтерполу та Європолу; розвитком технологій аналітичної та комп'ютерної розвідки; створенням

[96] Чаплинський К. О. Тактичне забезпечення розслідування діяльності злочинних угрупувань: монографія. Дніпропетровськ: Ліра ЛТД, 2010. 304 с.

[97] Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ: Хай-Тек Прес, 2010. 624 с.

[98] Юрченко О. М., Стрельбицька Л. М., Вертузаєв О. М. Застосування новітніх інформаційних технологій в інформаційно-аналітичному забезпеченні оперативно-службової діяльності правоохоронних органів. *Науковий вісник Київського національного університету внутрішніх справ.* Київ, 2006. № 3. С. 40–49.

[99] Бельсон Я. М. Интерпол в борьбе с уголовной преступностью; отв. ред. И. И. Карпец. Москва: Наука, 1989. 240 с.

вибухотехнічних підрозділів; упровадженням в оперативну та слідчу практику мультимедійних технологій; використанням безпілотних літальних апаратів (дронів) у правоохоронній діяльності, розробленням технологій зняття інформації з транспортних телекомунікаційних мереж та електронних інформаційних систем.

*П'ятий етап використання новітніх технологій у розслідуванні злочинів – із 20 листопада 2012 р. – до наших днів.* Початок цього етапу використання новітніх технологій у розслідуванні злочинів пов'язаний з набранням чинності новим КПК України, запровадженням негласних слідчих (розшукових) дій. Це спричинило суттєві зміни в організації застосування новітніх технологій у розслідуванні злочинів.

У листопаді 2015 року відбулося реформування Експертної служби МВС України, яка нині безпосередньо підпорядковується Міністру внутрішніх справ України.

У 2017 році до трьох процесуальних кодексів (Цивільного процесуального Кодексу України, Господарського процесуального Кодексу України та Кодексу адміністративного судочинства України) була введена нова глава, яка розширила можливості сторін у справі, – електронні докази.

Для дослідження мобільних пристроїв правоохоронні органи України розпочали активно використовувати програмно-апаратні засоби компанії Cellebrite.

Проблеми використання новітніх технологій у розслідуванні злочинів у сучасних умовах досліджували Т. В. Авер'янова[100], А. В. Баб'як[101], Б. І. Бараненко[102], П. В. Бер-

[100] Криминалистика: учебник / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Ю. Г. Корухов. 4-е изд., перераб. и доп. Москва: Норма: НИЦ Инфра-М, 2019. 928 с.

[101] Баб'як А. В., Крєпаков І. О., Мазур Л. А., Стащак М. В. Наукові та організаційно-правові засади протидії підрозділами карного розшуку обігу майна, одержаного злочинним шляхом: монографія; за заг. ред. С. М. Гусарова, В. В. Шендрика. Львів: ВД «Панорама», 2014. 160 с.

[102] Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навч.-практ. посіб. / Б. І. Бараненко, О. В. Бочковий, К. А. Гусева та ін. ; МВС України, Луган.

наз[103], Р. С. Бєлкін[104], О. В. Бочковий[105], В. І. Василинчук[106], В. І. Галаган[107], В. Я. Горбачевський[108], М. В. Гребенюк[109], М. Л. Грібов[110], М. В. Даньшин[111], В. А. Журавель[112], В. П. Заха-

держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. 416 с.

[103] Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49.

[104] Див.: Белкин Р. С. История отечественной криминалистики. Москва: НОРМА, 1999. 496 с.; Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. Москва: НОРМА, 2001. 240 с.; Аверьянова Т. В., Россинская Е. Р., Белкин Р. С., Корухов Ю. Г. Криминалистика: учебник. 4-е изд., перераб. и доп. Москва: Норма: НИЦ Инфра-М, 2019. 928 с.

[105] Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навч.-практ. посіб. / Б. І. Бараненко, О. В. Бочковий, К. А. Гусева та ін.; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. 416 с.

[106] Василинчук В. І. Оперативно-розшукова профілактика злочинів у бюджетній сфері: монографія. Київ: ДП «Розвиток», 2011. 520 с.

[107] Галаган В. І., Саліхов І. Ю. Встановлення події кримінального правопорушення як обставини, яка підлягає доказуванню у кримінальному провадженні: монографія. Київ: УкрДГРІ, 2017. 198 с.

[108] Розкриття та розслідування умисних вбивств, учинених на замовлення: навч. посіб. / В. І. Василинчук, А. Ф. Волобуєв, В. Я. Горбачевський та ін. Київ: Упр. вид.-полігр. діяльності МВС України, 2010. 288 с.

[109] Гребенюк М. В., Швець В. К. Проблеми використання кримінального аналізу оперативними підрозділами правоохоронних органів у протидії організованій злочинності. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності*: тези III Всеукр. науково-практ. конф. (Хмельницький, 1 березня 2019 року). Хмельницький: Вид-во НАДПСУ, 2019. С. 616–619.

[110] Грібов М. Л. Зміст та основні напрями криміналістичного забезпечення негласних слідчих (розшукових) дій. *Вісник кримінального судочинства*. 2017. № 1. С. 35–41.

[111] Даньшин М. В. Криміналістика XXI століття: місце у системі наукового знання: монографія. Харків, 2013. С. 29.

[112] Практикум з криміналістики: навч. посіб. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. Київ, 2013. С. 11–12; Криміналістика: підруч. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітько. 5-те вид. переробл. та допов. Київ: Ін Юре, 2016. 640 с.;

ров[113], А. В. Іщенко[114], І. І. Когутич[115], В. О. Коновалова[116], Ю. Г. Корухов[117], О. І. Мотлях[118], О. Л. Мусієнко[119], В. С. Овчинський[120], С. В. Пеньков[121], М. А. Погорецький[122], В. В. Пясковсь-

---

Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. 260 с.

[113] Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посіб. 2-ге вид., доп. Львів: ЛьвДУВС, 2015. 492 с.

[114] Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін. Київ, 2015. С. 19–21.

[115] Когутич І. І. Проблеми методології криміналістики та інших її складових частин: навч. посіб. Тернопіль, 2016. С. 23.

[116] Практикум з криміналістики: навч. посіб. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. Київ, 2013. С. 11–12; Криміналістика: підруч. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітько. 5-те вид. переробл. та допов. Київ: Ін Юре, 2016. 640 с.

[117] Криминалистика: учебник / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Ю. Г. Корухов. 4-е изд., перераб. и доп. Москва: Норма: НИЦ Инфра-М, 2019. 928 с.

[118] Мотлях О. І. Поліграфологія та її місце в системі криміналістики. Актуальні питання кримінального процесу, криміналістики та судової експертизи: матеріали міжвід. наук.-практ. конф. (Київ, 24 листоп. 2017 р.): у 2 ч. Київ, 2017. Ч. 1. С. 179–180.

[119] Мусієнко О. Л. Новітні технології у криміналістиці: проблеми та перспективи. Правове життя сучасної України: матеріали Міжнар. наук. конф. проф.-викл. та аспірант. складу / відп. за вип. В. М. Дрьомін; НУ ОЮА, Півд. регіон. центр НАПрН України. Одеса: Фенікс, 2014. Т. 1. С. 757–759.

[120] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

[121] Пеньков С. В., Шендрик В. В. Впровадження Інтернет-технологій у діяльність Національної поліції України для отримання оперативно-розшукової інформації. Право і безпека. 2017. № 2 (65). С. 80–85. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/2410

[122] Див.: Погорецький М. А. Проведення негласних слідчих (розшукових) дій та використання їх результатів у доказуванні. Актуальні проблеми досудового розслідування слідчими органів внутрішніх справ: проблеми теорії та практики: матеріали всеукраїнськ. наук.-практ. конф., 18–19 квіт. 2013 р.: тези доп. Дніпропетровськ: ДДУВС, 2013. С. 186–192; Погорецький М. А. Впровадження інституту негласних (розшукових) слідчих дій в правозастосовну практику. Боротьба з організованою злочинністю і корупцією (теорія і практика): наук.-практ. журнал; Міжвід. наук.-

кий[123], О. В. Рибальський[124], О. Р. Россінська[125], В. В. Семенов[126], Д. Б. Сергєєва[127], В. В. Середа[128], Є. Д. Скулиш[129], М. В. Стащак[130],

досл. центр з проблем б-би з орг. злоч. при РНБО України. 2012. № 2 (28). С. 56–63; Погорецький М. А. Криміналістичне забезпечення досудового провадження: проблеми теорії та практики. Сучасні проблеми криміналістики: матеріали міжнародної науково-практичної конференції, присвяченої 100-річчю з дня народження д. ю. н., проф. В. П. Колмакова (м. Одеса, 27–28 вересня). Одеса, 2013. С. 250–253; Погорецький М. А. Використання матеріалів ОРД у кримінальному судочинстві: процесуальні та криміналістичні аспекти. Інформаційне забезпечення розслідування злочинів: матеріали Міжнародного круглого столу (м. Одеса, 29 травня 2015 р.) / відп. за вип. В. В. Тіщенко, О. П. Ващук; НУ ОЮА; ПРЦ НАПрН України. Одеса: Юридична література, 2015. С. 217–222; Погорецький М. А., Сергєєва Д. Б., Старенький О. С. та ін. Доказування слідчими Служби безпеки України контрабанди наркотичних засобів: монографія / за заг. ред. д. ю. н., проф. М. А. Погорецького. Київ: Нац. акад. СБ України, 2018. 238 с.

[123] Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін. Київ, 2015. С. 19–21.

[124] Рибальський О. В., Соловйов В. І., Журавель В. В., Шабля О. М. Деякі аспекти побудови вітчизняної системи інструментарія експертизи матеріалів та засобів цифрового звукозапису. Криміналістика і судова експертиза. 2018. Вип. 63(2). С. 81–92.

[125] Криминалистика: учебник / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Ю. Г. Корухов. 4-е изд., перераб. и доп. Москва: Норма: НИЦ Инфра-М, 2019. 928 с.

[126] Семенов В. В., Терешкевич А. І. Використання новітніх технологій та досягнень науки й техніки в кримінальному провадженні. Криминалистика и судебная экспертиза. 2015. Вып. 60. С. 117–125.

[127] Сергєєва Д. Б. Співвідношення пізнання і доказування у кримінальному процесі. Науковий вісник Київського національного університету внутрішніх справ. 2010. Вип. 4 (71). С. 144–149; Сергєєва Д. Б. Напрями використання результатів негласних слідчих (розшукових) дій у кримінальному процесуальному доказуванні. Вісник кримінального судочинства. 2018. № 2. С. 81–91.

[128] Див.: Середа В. В., Хатнюк Ю. А. Організаційно-правові основи діяльності підрозділів Національної поліції України, що здійснюють аналітичну роботу. Науковий вісник Львівського університету внутрішніх справ. Серія юридична. 2018. № 4. С. 189–198; Середа В. В. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія. Львів: ЛьвДУВС, 2016. 188 с.

[129] Скулиш Є. Д. Негласні слідчі (розшукові) дії за кримінально-процесуальним законодавством України. *Вісник Національної академії прокуратури України*. 2012. № 2. С. 15–23.

Р. Л. Степанюк[131], О. В. Таран[132], О. Ю. Татаров[133], В. В. Топчій[134], Ю. М. Чорноус[135], В. П. Шеломенцев[136], В. В. Шендрик[137], В. Ю. Шепітько[138], М. Є. Шумило[139], М. П. Яблоков[140], В. В. Юсупов[141] та інші вчені.

---

[130] Стащак Н. В., Перепелица Н. Н. Информационно-аналитическое обеспечение оперативной разработки лиц, которые готовятся к совершению преступлений в составе организованной группы. *Журнал научных публикаций аспирантов и докторантов*. 2014. Вып. 12. С. 67–71.

[131] Див.: Степанюк Р. Л., Лапта С. П. Новітні зарубіжні розробки та перспективні дослідження у галузі техніко-криміналістичного забезпечення протидії злочинності. Право і безпека. 2017. Вип. 2 (65). С. 96–101; Степанюк Р. Л. Деякі перспективні напрями розвитку криміналістики в Україні. Форум права: електрон. наук. фахове вид. 2017. № 5. С. 389–394. URL: http://nbuv.gov.ua/jpdf/FP_index.htm_2017_5_61.pdf.

[132] Таран О.В. Розслідування злочинів, пов'язаних з порушенням вимог законодавства про охорону праці: монографія. Київ: ДІА, 2012. 352 с.

[133] Татаров О. Ю. Досудове провадження в кримінальному процесі України: теоретико-правові та організаційні засади (за матеріалами МВС). Донецьк: Промінь, 2012. 640 с.

[134] Топчій В. В., Тичина Д. М. Запобігання використанню сучасних інформаційних технологій у злочинних цілях. *Правовий часопис Донбасу*. 2018. № 1. С. 159–166.

[135] Див.: Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін. Київ, 2015. С. 19–21; Чорноус Ю. М. Криміналістика: напрями розвитку та вдосконалення. *Актуальні питання кримінального процесу, криміналістики та судової експертизи*: матеріали міжвід. наук.-практ. конф. (Київ, 24 листоп. 2017 р.): у 2 ч. Київ, 2017. Ч. 1. С. 189.

[136] Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.

[137] Пеньков С. В., Шендрик В. В. Впровадження Інтернет-технологій у діяльність Національної поліції України для отримання оперативно-розшукової інформації. *Право і безпека*. 2017. № 2 (65). С. 80–85. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/2410

[138] Див.: Практикум з криміналістики: навч. посіб. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. Київ, 2013. С. 11–12; Криміналістика: підруч. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітько. 5-те вид. переробл. та допов. Київ: Ін Юре, 2016. 640 с.; Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. 260 с.

Водночас, ураховуючи кардинальні зміни у кримінально-процесуальному й оперативно-розшуковому законодавстві, стрімкий розвиток новітніх технологій та інновацій, зазначені проблеми потребують подальших глибоких і ґрунтовних досліджень. Підсумовуючи історію розроблення та використання новітніх технологій у розслідуванні злочинів, можна вирізнити кілька поворотних віх у її розвитку:

1) запровадження дактилоскопії в практику роботи поліцейських служб;

2) централізація обліків і створення реєстраційної мережі;

3) комп'ютеризація криміналістичного та інформаційно-аналітичного забезпечення оперативних підрозділів і підрозділів досудового розслідування;

4) запровадження молекулярно-генетичної експертизи;

5) створення обліків міжвідомчого характеру, розвиток міждержавних обліків, використання інтегрованих банків Інтерполу та Європолу;

6) розвиток технологій кримінального аналізу, що дозволяє здобувати нові знання шляхом систематизації та аналізу розрізнених фактів;

7) розвиток технологій комп'ютерної розвідки, що дає змогу негласно аналізувати величезні масиви даних і відомостей;

8) упровадження в ОРД та досудове розслідування мультимедійних технологій, що дозволяє отримувати оперативно значущу та процесуальну інформацію з аудіо- та відеозаписів,

---

[139] Про стан підготовки до розгляду у другому читанні Кримінального процесуального кодексу України (реєстр. номер 9700): стенограма круглого столу в Комітеті Верховної Ради України з питань законодавчого забезпечення правоохоронної діяльності (Київ, 29 лют. 2012 р.). URL: http://komzakonpr.rada.gov.ua/omzakonpr/control/uk/publish/article?art_id=51130&cat_id=49415

[140] Яблоков Н. П., Головин А. Ю. Криминалистика: природа, система, методологические основы. 2-е изд., доп. и перераб. Москва: НОРМА, 2009. 288 с.

[141] Юсупов В. В. Криміналістика в Україні у XX–XXI століттях: монографія. Київ: ФОП Маслаков, 2018. 556 с.

вирішувати ідентифікаційні та діагностичні завдання, здобувати криміногенно значущу інформацію, яка може стати основою для формування доказів у кримінальних провадженнях;

9) розроблення технологій здійснення оперативно-розшукових заходів і негласних слідчих (розшукових) дій у мережі Інтернет, що уможливлює розкриття кіберзлочинів;

10) розроблення технологій розпізнання події злочину, пов'язане з наявністю в осіб, причетних до його вчинення, засобів мобільного зв'язку;

11) використання безпілотних літальних апаратів (дронів) і роботів у правоохоронній діяльності;

12) створення й використання програмних та апаратних засобів для дослідження комп'ютерної техніки та програмних продуктів;

13) удосконалення способів і методів збирання, дослідження, оцінки, документування та використання цифрових доказів;

14) упровадження 3D-технологій у правоохоронній діяльності.

## 1.2. Поняття та сутність використання новітніх технологій у розслідуванні злочинів

Розуміння і використання новітніх технологій у контексті протидії злочинності має подвійний характер. З одного боку, сучасні технології використовуються злочинцями для вчинення кримінальних правопорушень. У цьому сенсі новітні технології входять до драйверів злочинності. З іншого боку, технології є інструментом, що дозволяє не тільки успішно боротися з кримінальними злочинами, але і запобігати їм[142].

[142] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

Якщо мовити про «розумну» поліцію, насамперед зазначимо про використання нових технологій у вигляді сучасних поліцейських патрульних автомобілів, оснащених новітніми інтегрованими ІТ-системами. Такі автомобілі можуть прибути до місця події оптимальним маршрутом за допомогою GPS-навігатора.

Крім того, слід згадати про нагрудні камери (портативні відеореєстратори) для поліцейських у комплекті з відеореєстратором для патрульних автомобілів. Під час здійснення повноважень поліцейськими портативний відеореєстратор закріплюється на його форменому одязі так, щоб не створювати перешкод діям поліцейського. Увімкнення портативного відеореєстратора відбувається з моменту початку виконання службових обов'язків або спеціальної поліцейської операції, а відеозйомка ведеться безперервно до її завершення, крім випадків, пов'язаних із виникненням у поліцейського особистого приватного становища.

Відеореєстратор може бути встановлений усередині салону службового патрульного автомобіля або зовні для максимальної фіксації навколишньої обстановки або внутрішньої частини салону в спосіб, що не заважає огляду водія. Відеореєстратор вмикається, коли поліцейський розпочинає виконувати службові обов'язки або стартує спеціальна поліцейська операція, а відеозапис триває безупинно до її завершення[143].

«Розумна» поліція активно використовує безпілотні літальні апарати (БпЛА, дрон) – повітряні судна, призначені для виконання польоту без пілота на борту, керування польотом якого і контроль за яким здійснюються за допомогою спеціальної станції керування, що розташована поза літальним апаратом[144]. Зокрема, компанія Amazon оформила патент на міні-

[143] 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.

[144] Там само.

дрон для патрульних поліцейських UAVA (Unmanned Aerial Vehicle Assistant) – безпілотний літальний апарат-асистент. БпЛА можуть бути обладнані системами (однією або декількома) фото- і відеозапису залежно від технічних характеристик повітряного судна.

У Дубаї на патрулювання вже вийшов перший робот-поліцейський. Криміналісти дедалі частіше залучають у свою професійну діяльність 3D-технології. На основі нейронних мереж розробляються нові поліграфи. Глобальні навігаційні системи стали невіддільним елементом у розслідуванні злочинів. Обсяжні масиви підозрюваних проходять через інтелектуальні системи розпізнавання образів. Нейромережі дають змогу із більшою ймовірністю прогнозувати злочинну поведінку конкретних осіб[145].

Водночас вивчення наукового рівня криміналістичного забезпечення діяльності з розслідування злочинів, використання інноваційних досягнень сучасної науки і техніки правоохоронними органами свідчать про певне їх відставання від кримінальної практики застосування новітніх засобів, методів і технологій у злочинній діяльності. Насамперед це виявляється у застосуванні злочинними угрупованнями сучасних інформаційних технологій для вчинення злочинів на національному та міжнародному рівнях[146].

Зважаючи на викладене, найперше проаналізуємо поняття «використання новітніх технологій у розслідуванні злочинів». Слід підкреслити, що у нормативно-правових актах і науковій літературі поряд із терміном «новітні технології»[147] часто

---

[145] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

[146] Берназ П.В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49.

[147] Див.: Юрченко О. М., Стрельбицька Л. М., Вертузаєв О. М. Застосування новітніх інформаційних технологій в інформаційно-аналітичному забезпеченні оперативно-службової діяльності правоохоронних органів. *Науковий вісник Київського національного університету внутрішніх справ*. Київ, 2006. № 3. С. 40–49; Задорожний Ю. А. Проблемы информационно-аналитического обеспечения ОРД в современных условиях. Вияв-

вживаються терміни «високі технології»[148], «інформаційні технології»[149], «інновації»[150].

---

лення, фіксація та використання доказів у процесі досудового слідства. *Вісник ЛАВД імені 10 річчя незалежності України.* Спеціальний випуск. Луганськ, 2005. С. 89–99; Халиков А. Н., Яковец Е. Н., Журавленко Н. И. Юридическое, техническое и информационно-аналитическое обеспечение оперативно-розыскной деятельности: учебное пособие; под редакцией А. Н. Халикова. Москва: Юрлитинформ, 2010. 472 с.; Хахановський В. Г. Інформаційно-аналітичне забезпечення ОРД: основні поняття та нормативно-правова база. Шляхи вдосконалення оперативно-розшукової діяльності ОВС. *Вісник ЛІВС.* Львів, 2002. № 2(1). С. 191–195; Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учеб. пособие. Москва: Щит-М, 2009. 464 с.; Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49.

[148] Див.: Белов О. А. Информационное обеспечение раскрытия и расследования преступлений: монография. Москва: Юрлитинформ, 2009. 136 с.; Захаров В. П., Рудешко В. І. Проблеми інформаційного забезпечення правоохоронних структур: навчально-практичний посібник. Львів: ЛьвДУВС, 2007. 372 с.; Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / под ред. В. И. Попова. Москва: ИНФРА-М, 2002. 97 с.; Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. Москва: ИНФРА-М, 2000. 367 с.; Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49.

[149] Див.: Юрченко О. М., Стрельбицька Л. М., Вертузаєв О. М. Застосування новітніх інформаційних технологій в інформаційно-аналітичному забезпеченні оперативно-службової діяльності правоохоронних органів. *Науковий вісник Київського національного університету внутрішніх справ.* Київ, 2006. № 3. С. 40–49; Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49; Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/98-ВР. *Відомості Верховної Ради України.* 1998. № 27–28. Ст. 181; Автоматизовані системи. Терміни та визначення: ДСТУ 2226–93. Чинний від 1994-07-01. Київ: Держстандарт України, 1993. 91 с. (Національні стандарти України); Овчинский А. С., Каретников М. К. Проблемы подготовки специалистов в области применения современных информационных технологий. *Вестник МВД России.* 2000. № 4–5. С. 130–131.

[150] Див.: Про інноваційну діяльність: Закон України від 05.12.2012 № 5460-VI. *Голос України* від 09.08.2002 № 144.; Інноваційні засади технічко-криміналістичного забезпечення діяльності органів кримінальної

*Високі технології* (англ. *high technology, high tech, hi-tech*) – найновіші і найпрогресивніші технології сучасності, до яких належать найбільш наукомісткі галузі промисловості. Термін «високі технології» розпочали вживати з кінця 60-х років минулого століття. Першим його застосував журналіст Роберт Мец у авторській колонці газети «New York Times»[151].

Згідно з визначенням Департаменту торгівлі США, галузі, в яких співвідношення витрат на НДДКР та обсягів збуту перевищує більше ніж у два рази середньостатистичні показники, класифікуються як високотехнологічні[152]. Визначення високотехнологічних галузей Організацією економічного співробітництва та розвитку (*OECD*) охоплює три складові – частку витрат на НДДКР у витратах підприємств галузі, частку високотехнологічної комплектації у складі виробів і частку персоналу НДДКР у складі підприємств[153]. До високих технологій зазвичай зараховують найбільш наукомісткі галузі промисловості: мікроелектроніку, інформаційні технології, обчислювальну техніку, програмування, робототехніку, нанотехнології,

---

юстиції: монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдеєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. С. 7–8; Шепітько В. Ю., Авдєєва Г. К. Інновації в діяльності органів кримінальної юстиції. Криминалистика и судебная експертиза: междуведомственный научно-методический сборник. Вып. 59 / отв. ред. И. И. Емельянова. 2014. С. 4; Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49.; Шепітько В. Ю. Природа і предмет вивчення криміналістики в системі наукового знання. Вибрані твори. Харків, 2010. С. 16.

[151] Metz R. Market Place: Collins Versus The Middle Man. The New York Times. April 24, 1969. P. 64; Metz R. Market Place: Keeping an Eye On Big Trends. The New York Times. November 4, 1969. P. 64.

[152] Shanklin W. L., Ryans J. K. Marketing high technology. Mass: Lexington Books, 1984. xix, 216 p.; John G., Weiss A., Dutta S. Marketing in Technology-Intensive Markets: Toward a Conceptual Framework. Journal of Marketing. Volume 63, no. Special. 1999. P. 78–91.

[153] Hatzichronoglou T. Revision of the High-Technology Sector and Product Classification. OECD library. OECD Science, Technology and Industry Working Papers. Paris: OECD Publishing, 1997. 1997/2. 26 p.

атомну енергетику, аерокосмічну техніку, біотехнології, фармацевтику, генну інженерію, штучний інтелект.

Для формулювання визначення поняття «інформаційні технології» розпочнемо з дослідження дефініції «інформація». У філософському розумінні *інформація* (від лат. *informatio* – ознайомлення, роз'яснення, викладення, обізнаність) – одне з найбільш загальних понять науки, що позначає деякі відомості, сукупність даних, знань[154].

Термін «інформація» інтерпретується у двох значеннях: у повсякденному – як відомості (повідомлення, звістки), що передаються людьми усним, письмовим або іншим способом (за допомогою умовних сигналів тощо) і повідомляють про що-небудь; і в науковому – як обмін цими відомостями між людьми, людиною й автоматом, автоматом і автоматом[155].

Чимало авторів, зокрема В. Ю. Голубовський та О. Ю. Шумілов, під інформацією розуміють сукупність певних відомостей, даних, знань[156].

Однією із загальноприйнятих форм подання інформації є повідомлення. У своїй фундаментальній праці «Інформатика» Ф. Л. Бауер уводить поняття «повідомлення» і «інформація» як невизначені основні поняття, маючи на увазі, що всі інші поняття інформатики є похідними від них[157].

У зв'язку з цим нагадаємо визначення інформації, яке запропонував «батько» кібернетики Н. Вінер, як «позначення змісту повідомлення, яке отримано із зовнішнього світу в про-

---

[154] Грицанов А. А. Новейший философский словарь. Минск, 1999. С. 112.

[155] Советский энциклопедический словарь / гл. ред. А. М. Прохоров. 3-е изд. Москва: Сов. Энциклопедия, 1984. С. 498.

[156] Див.: Голубовский В. Ю. Теоретические и правовые аспекты информационного обеспечения ОРД. Санкт-Петербург: Санкт-Петербургский университет МВД РФ, 2000. 152 с.; Шумилов А. Ю. Основы уголовно-правовой оценки сыскной информации. Москва: Изд-ль Шумилова И. И., 2000. 140 с.

[157] Бауэр Ф. Л., Гооз Г. Информатика. Вводный курс. В 2-х ч. Москва: Мир, 1990. С. 18–19.

цесі нашого пристосування до нього і пристосування наших почуттів»[158].

У Великому тлумачному словнику сучасної української мови термін «інформація» пояснено як відомості про якінебудь події, чиюсь діяльність; повідомлення про щось[159].

У нашому дослідженні ми керуватимемося визначенням інформації, наведеним у законодавчих актах, а саме у ст. 1 Закону України «Про інформацію» та ст. 20 Цивільного кодексу України, де під *інформацією* розуміються будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді[160].

Водночас у ст. 1 Закону України «Про телекомунікації» зазначено, що *інформація* – це відомості, подані у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб[161].

Способи і прийоми оволодіння інформацією дозволяють зробити висновок про існування двох її видів: гласної та негласної. За змістом інформація поділяється на такі види: інформація про фізичну особу; інформація довідково-енциклопедичного характеру; інформація про стан довкілля (екологічна); інформація про товар (роботу, послугу); науково-технічна інформація; податкова інформація; правова інформація; статистична інформація; соціологічна інформація; інші види інформації.

З уваги на тему монографії, нас найперше цікавить правова інформація, яка визначається як будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти,

---

[158] Винер Н. Мое отношение к кибернетике, ее прошлое и будущее. Москва: Советское радио, 1969. С. 23.

[159] Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В. Т. Бусел. Київ; Ірпінь: ВТФ: Перун, 2004. С. 403.

[160] Див.: Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650; Цивільний кодекс України. *Відомості Верховної Ради України.* Київ, 2003. № 40–44. Ст. 356.

[161] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. *Відомості Верховної Ради України.* 2004. № 12. Ст. 155.

правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо[162].

Термін «технологія» (від грецького *techne* – мистецтво, ремесло, наука та *logos* – вчення) виник у сфері матеріального виробництва і спочатку означав сукупність способів виробництва, а також їх наукове описання[163].

Великий тлумачний словник сучасної української мови визначає *технологію* як сукупність знань, відомостей про послідовність окремих виробничих операцій у процесі виробництва чого-небудь; сукупність способів обробки чи переробки матеріалів, інформації, виготовлення виробів, проведення різних виробничих операцій, надання послуг тощо[164].

У зв'язку з цим наголосимо на особливості використання терміна «технологія» відомим криміналістом В. О. Образцовим, який запропонував визначати науку криміналістику як «технологію розслідування»[165].

Професор Р. Є. Бєлкін із цього приводу зазначив, що схожу з технологією роль у криміналістиці у відомому сенсі виконують тактика і методика: як засіб організації, здійснення якого-небудь процесу з найбільшим ефектом вони також спрямовані на перетворення об'єкта впливу. Учений вважає, що у цьому значенні криміналістична методика – це своєрідна технологія процесу розслідування[166].

Під технологією розслідування злочину у науковій літературі розуміється функціонально зумовлена упорядкована

---

[162] Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

[163] Словарь иностранных слов / под ред. И. В. Лёхина, Ф. Н. Петрова. Москва: Гос. изд-во иностранных и национальных словарей, 1949. С. 785.

[164] Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В. Т. Бусел. Київ; Ірпінь: ВТФ: Перун, 2005. С. 1448.

[165] Криминалистика / под ред. докт. юрид. наук, проф. В. А. Образцова. Москва: Юринком, 1994. С. 10.

[166] Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. Москва: Инфра-М-НОРМА, 2001. С. 84.

сукупність дій (діяльність), що забезпечується необхідними ресурсами, та реалізується відповідним суб'єктом у процесі розслідування злочинів[167].

Процес (технологія) розслідування є цілеспрямованою людською діяльністю й охоплює такі елементи: суб'єкт розслідування, об'єкт розслідування, засоби розслідування[168].

Отже, з огляду на зазначене, можна підкреслити важливе значення широкого застосування комп'ютерних, інформаційних, комунікаційних, цифрових, судово-експертних та інших інноваційних технологій у практиці розслідування злочинів.

Одним із найбільш перспективних напрямів підвищення ефективності розкриття та розслідування злочинів уважається використання у слідчій та оперативно-розшуковій діяльності інформаційних технологій. Поняття «інформаційні технології» на законодавчому рівні розглядається як цілеспрямована організована сукупність інформаційних процесів із використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування[169].

Державний стандарт ДСТУ 2226-93 «Автоматизовані системи. Терміни та визначення» визначає *інформаційні технології* як технологічний процес, предметом перероблення й результатом якого є інформація[170].

Інформаційні технології широко застосовуються на початковому етапі розслідування злочинів під час планування роз-

---

[167] Моїсєєв О. Технології в криміналістиці та в судовій експертології: співвідношення та розмежування. *Правничий часопис Донецького університету: науковий журнал.* 2010. № 2(24). С. 127.

[168] Шмонин А. В. Методология криминалистической методики: монография. Москва: Юрлитинформ, 2010. С. 131.

[169] Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/98-ВР. *Відомості Верховної Ради України*. 1998. № 27–28. Ст. 181.

[170] Автоматизовані системи. Терміни та визначення: ДСТУ 2226–93. Чинний від 1994-07-01. Київ: Держстандарт України, 1993. 91 с. (Національні стандарти України).

слідування, формулювання робочих версій, одержання орієнтовної інформації, побудови діаграм, схем, таблиць, графіків, моделей тощо[171].

Ми поділяємо думку А. С. Овчинського та М. К. Каретнікова про те, що застосування сучасних інформаційних технологій у боротьбі зі злочинністю дає змогу внести нове наповнення як у традиційні напрями ОРД та досудового розслідування, так і безпосередньо в їх інформаційно-аналітичне забезпечення. Зокрема, застосування сучасних комп'ютерних технологій дозволяє не тільки накопичувати й аналізувати оперативну, криміналістичну, процесуальну, статистичну інформацію, але й безпосередньо здобувати її за допомогою електронних засобів, а також моделювати і прогнозувати розвиток ситуації[172].

У нинішніх умовах інформаційні технології ефективно використовуються у розслідуванні злочинів. Зокрема, вони дають змогу здійснювати фіксацію доказової інформації за допомогою цифрових засобів аудіозапису, відео- та фотозйомки, дистанційно (через дальноміри) вимірювати відстані між предметами під час огляду місця події та будувати плани і схеми місця події за допомогою програмних засобів тощо.

Зважаючи на викладене, визначимо *інформаційні технології у розслідуванні злочинів* як сукупність методів, технологічних процесів і програмно-технічних засобів, інтегрованих з метою збирання, обробки, систематизації, узагальнення, аналізу, зберігання та використання криміналістичної, оперативної та процесуальної інформації, зокрема обмеженого доступу, що має значення для вирішення завдань ОРД і досудового розслідування, забезпечення безпеки громадян, суспільства і держави.

---

[171] Шепітько В. Ю., Авдєєва Г. К. Інформаційні технології в криміналістиці та слідчій діяльності. Питання боротьби зі злочинністю / ред. кол.: В. І. Борисов та ін. Харків: Право, 2009. Вип. 19. С. 196–197.

[172] Овчинский А. С., Каретников М. К. Проблемы подготовки специалистов в области применения современных информационных технологий. *Вестник МВД России*. 2000. № 4–5. С. 130–131.

Віднедавна у вітчизняній правовій науці значна увага приділяється проблемам розроблення інновацій та впровадження їх у діяльність слідчих підрозділів[173]. Відповідно до ст. 1 Закону України «Про інноваційну діяльність», *інноваціями* є новостворені (застосовані) і (або) вдосконалені конкурентоздатні технології, продукція або послуги, а також організаційно-технічні рішення виробничого, адміністративного, комерційного або іншого характеру, що істотно поліпшують структуру та якість виробництва і (або) соціальної сфери. Інноваційним продуктом є результат науково-дослідної і (або) дослідно-конструкторської розробки[174].

Термін «інновація» походить від латинського слова *«innovato»* й означає оновлення або поліпшення. Сьогодні термін «інновація» (пізньолат. *inovatio*, англ. *innovation* – нововведення) застосовується як синонім дефініції «нововведення».

---

[173] Див.: Шепітько В. Ю. Природа і предмет вивчення криміналістики в системі наукового знання. Вибрані твори. Харків, 2010. С. 16; Практикум з криміналістики: навч. посіб. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. Київ, 2013. С. 11–12; Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. № 4. С. 49; Криміналістика: підруч. / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітько. 5-те вид. переробл. та допов. Київ: Ін Юре, 2016. 640 с.; Шепітько В. Ю., Авдєєва Г. К. Інновації в діяльності органів кримінальної юстиції. Криминалистика и судебная экспертиза: междуведомственный научно-методический сборник. Вып. 59 / отв. ред. И. И. Емельянова. Министерство юстиции Украины, 2014. С. 4; Інноваційні засади технікокриміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. 260 с.; Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін. Київ, 2015. С. 19–21; Чорноус Ю. М. Криміналістика: напрями розвитку та вдосконалення. Актуальні питання кримінального процесу, криміналістики та судової експертизи: матеріали міжвід. наук.-практ. конф. (Київ, 24 листоп. 2017 р.): у 2 ч. Київ, 2017. Ч. 1. С. 189; Юсупов В. В. Криміналістика в Україні у XX–XXI століттях: монографія. Київ: ФОП Маслаков, 2018. 556 с.

[174] Про інноваційну діяльність: Закон України від 05.12.2012 5460-VI. *Голос України* від 09.08.2002 № 144.

Сутність цього терміну полягає в комплексному процесі створення, розповсюдження та використання нового продукту, що призначений для задоволення потреб людини з урахуванням сучасного рівня розвитку науки і техніки. Обов'язковим завершальним етапом інноваційної діяльності є успішне впровадження її результатів в практику та ефективне їх використання[175].

Шепітько В. Ю. і Авдєєва Г. К. вважають, що головним постачальником інноваційного продукту в правозастосовну практику є криміналістика. Криміналістами створюються нововведення, які істотно поліпшують якість і повноту процесу доказування у справі, підвищують його науковий рівень, скорочують терміни досудового слідства, дозволяють урегулювати питання, що раніше не вирішувалися за відсутності належних методів і засобів. До інноваційних криміналістичних продуктів науковці зараховують розробки в галузі криміналістичної техніки, тактики та методики розслідування злочинів, а саме: нові або вже існуючі та прилаштовані до потреб слідчої практики техніко-криміналістичні засоби, сучасні інформаційні технології, електронні бази знань, методи фіксації, накопичення, аналізу та оцінки доказової інформації, нові тактичні прийоми, їх комплекси, тактичні комбінації та операції, алгоритми першочергових слідчих дій та перевірки типових слідчих версій, методики розслідування нових видів злочинів та ін.[176].

Професор В. Ю. Шепітько визначає *криміналістичні інновації* як розроблені та впроваджені в практику боротьби зі злочинністю нові сучасні методи, прийоми, технології, тех-

[175] Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдеєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. С. 7–8.

[176] Шепітько В. Ю., Авдєєва Г. К. Інновації в діяльності органів кримінальної юстиції. Криминалистика и судебная експертиза: междуведомственный научно-методический сборник. Вып. 59 / отв. ред. И. И. Емельянова. Министерство юстиции Украины, 2014. С. 4.

нічні засоби, прилади, апаратура, інструменти, метою яких є оптимізація розслідування злочинів та їх судового розгляду, підвищення якості правозастосовної діяльності. Вчений вважає розроблення та впровадження в діяльність правоохоронних органів новітніх прийомів, методів і засобів (інновацій) важливим напрямом сучасного розвитку криміналістики[177].

Упровадження інновацій сприяє оптимізуванню розслідування, уникненню слідчих помилок і може бути реалізовано за такими напрямами:

1) розроблення та використання нових науково-технічних засобів для виявлення, збирання й попереднього дослідження доказів;

2) використання новітніх інформаційних технологій в роботі слідчого;

3) розроблення і залучення до застосування нових прийомів, методів, методик проведення слідчих дій і розслідування злочинів[178].

Під *технологією розслідування злочинів* пропонується розуміти складову частину функціонального аспекту організації цієї діяльності, яка допускає можливість алгоритмізації дій слідчих, криміналістів та оперативних працівників у розслідуванні кримінальних правопорушень.

Великий тлумачний словник сучасної української мови визначає поняття «*новітній*» як такий, що охоплює сучасний період, стосується його; сучасний, теперішній; новий, що відповідає сучасним вимогам; найновішого типу, конструкцій та ін.[179].

---

[177] Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. С. 8.

[178] Шепітько В. Ю. Природа і предмет вивчення криміналістики в системі наукового знання. Вибрані твори. Харків, 2010. С. 16.

[179] Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В. Т. Бусел. Київ; Ірпінь: Перун, 2005. С. 789.

*Новітня технологія* – це будь-яка технологія найновішого типу, що відповідає сучасним вимогам і має високий потенціал.

Отже, ***новітні технології у розслідуванні злочинів*** – це сучасні, найновіші інноваційні методи, прийоми, технологічні процеси, програмні і технічні засоби, інструменти, які інтегровані з метою збирання, отримання, обробки, систематизації, аналізу, зберігання та використання криміналістичної, оперативної та процесуальної інформації, для алгоритмізації й оптимізації процесу розкриття і розслідування злочинів та їх судового розгляду, підвищення якості правозастосовної діяльності.

## 1.3. Новітні зарубіжні розробки та перспективні дослідження у галузі техніко-криміналістичного забезпечення протидії злочинності

У сучасному світі технології постійно розвиваються і змінюються: щороку виникають нові і через певний час вони стають буденною реальністю. Зокрема, фахівці виріз-няють новітні технології, якими незабаром користуватиметься кожен:

1) *розумні окуляри* (у 2019 році компанія Google випустила нову версію розумних окулярів Google Glass Enterprise Edition 2 – це окуляри доповненої реальності, також відомі як «EE». Доповнена реальність (AR) – це поєднання реальних і згенерованих комп'ютером зображень, які накладаються одне на одне, у результаті чого користувач поринає в інший світ. Завдяки зручній і легкій оправі пристрій майже не відчувається при носінні. Його можна використовувати цілий день, замінивши звичні засоби зв'язку (смартфон, ноутбук, смартгодинник). Користувачі можуть використовувати AR-окуляри для доступу до необхідної їм робочої інформації: контрольних спи-

ків, інструкцій, а також для надсилання фотографій або відео)[180];

2) *розумні дані* (низка компаній, зокрема RelateIQ, працюють над тим, щоб автоматизувати процес побудови списку контактів, поштових скриньок, повідомлень тощо. Достатньо буде назвати ім'я – і в телефоні утворюється новий контакт)[181];

3) *дисплеї без екранів* (голограми припинять бути частиною фантастики. З'являться контактні лінзи, що проектуватимують зображення на сітківку ока)[182];

4) *нейрокомп'ютерні інтерфейси* (можливо, у майбутньому нам не знадобиться комп'ютерна миша або клавіатура. Достатньо буде подумати про певні речі – і вони з'являться на екрані)[183];

5) *цифрові завантаження* (наближається кінець розповсюдження фізичних копій продуктів. Медіафайли і відеоігри поширюватимуться лишень цифровим шляхом. Музика і фільми також поступово зміщуються в бік поширення через платформи типу iTunes)[184];

6) *ро́боти будуть скрізь* (ро́боти починають зі складальних конвеєрів і поступово вчаться бути вмілими хірургами і саперами, бухгалтерами і космонавтами)[185];

---

[180] Google випустила розумні окуляри Glass Enterprise Edition 2. URL: https://tehnofan.com.ua/2019/05/21/google-has-released-glass-enterprise-edition-2-smart-glasses/

[181] 15 новітніх технологій, якими незабаром буде користуватися кожен. URL: http://brandstory.com.ua/15-novitnix-texnologij-yakimi-nezabarom-bude-koristuvatisya-kozhen/

[182] Новітні технології, якими незабаром буде користуватися кожен. URL: http://novi-tekhnolohiyi.blogspot.com/2018/11/blog-post_6.html

[183] 15 новітніх технологій, якими незабаром буде користуватися кожен. URL: http://brandstory.com.ua/15-novitnix-texnologij-yakimi-nezabarom-bude-koristuvatisya-kozhen/

[184] Новітні технології, якими незабаром буде користуватися кожен. URL: http://novi-tekhnolohiyi.blogspot.com/2018/11/blog-post_6.html

[185] 15 новітніх технологій, якими незабаром буде користуватися кожен. URL: http://brandstory.com.ua/15-novitnix-texnologij-yakimi-nezabarom-bude-koristuvatisya-kozhen/

7) *бездротова передача енергії* (зарядна станція Qi Wireless дозволяє заряджати деякі смартфони без кабелю. Електромобілю достатньо буде припаркуватись біля бездротової зарядної станції і він заряджатиметься. Можливо, навіть під час поїздки дорогами, покритими сонячними батареями)[186];

8) *графен* (графен у 100 разів міцніше сталі, він дасть нам швидкий інтернет, його можна використовувати як фільтр для води та очищення океану, його можна застосовувати в смартфонах тощо)[187];

9) *Touch ID і Face ID* (у 2010-х роках Apple змогла впровадити технологію сканування відбитків пальців у смартфони, щоби позбавити користувачів необхідності запам'ятовувати паролі. У липні 2012 року Apple викупила біометричну компанію AuthenTec, запровадивши датчики сканування відбитків пальців у кнопку Home на iPhone 5s. Це започаткувало біометричні системи безпеки, що стали повсякденним явищем. Під час цього процесу біометрія допомогла розвинути системи мобільних платежів NFC, які використовують додаткову безпеку для аутентифікації платежів.

Сьогодні сканування відбитків пальців є буденністю, а технологія розпізнавання осіб Face ID є її подальшим розвитком. Apple не відмовилася від Touch ID на користь розпізнавання особи. Компанія планує впровадити датчик відбитків пальців під сам екран. Пристрій може використовуватися в поєднанні з Face ID на майбутніх моделях iPhone 12 і навіть може бути на Apple Watch)[188];

10) *мобільна електроніка* (сьогодні ми щодня контактуємо з користувачами бездротових навушників, таких як Apple

[186] Новітні технології, якими незабаром буде користуватися кожен. URL: http://novi-tekhnolohiyi.blogspot.com/2018/11/blog-post_6.html

[187] 15 новітніх технологій, якими незабаром буде користуватися кожен. URL: http://brandstory.com.ua/15-novitnix-texnologij-yakimi-nezabarom-bude-koristuvatisya-kozhen/

[188] Apple запатентувала революційну функцію для iPhone 12. URL: https://techno.znaj.ua/283997-apple-zapatentuvala-revolyuciynu-funkciyu-dlya-iphone-12

AirPods. Причому цю ідею перейняли Samsung з Galaxy Buds, Xiaomi з Mi Air 2, а також безліч моделей від інших виробників. Приміром, використовуються навушники, які рахують частоту серцевих скорочень, контактні лінзи, які вимірюють рівень цукру в крові, тощо)[189].

Норвезька телекомунікаційна компанія Telenor і одна з найбільших міжнародних консалтингово-аудиторських компаній Deloitt опублікували списки головних технологічних трендів 2020 року, які, на їхню думку, стануть масовими в новому році і увійдуть у звичне життя багатьох людей, зокрема:

• *мобільна мережа 5G.* Deloitte прогнозує сплеск популярності комерційних мобільних мереж п'ятого покоління, які підлаштовуватимуться під конкретні потреби їх користувачів, залежно від виду діяльності і профілю компанії або організації. Водночас експерти всього світу наголошують на потенційних вразливостях п'ятого покоління, оскільки перевагами 5G також користуватимуться кіберзлочинці.

Із грудня 2019 року в шести містах України, а саме в Києві, Харкові, Одесі, Дніпрі, Черкасах і Львові, шведським виробником відповідного обладнання спільно з українським мобільним оператором передбачено тестування мобільного зв'язку п'ятого покоління. Повноцінний запуск 5G в Україні планується через три роки;

• *штучний інтелект.* Deloitte вважає, що 2020 року продажі чипів, які працюють із технологіями штучного інтелекту, становитимуть близько 750 млн штук на загальну суму в 2,6 млрд доларів. До 2024 року продажі чипів зі штучним інтелектом сягнуть 1,5 млрд штук, при цьому їхня вартість для споживачів постійно знижуватиметься;

• *супутниковий інтернет.* Deloitte вважає, що в 2020 році зросте кількість компаній, які пропонуватимуть доступ до інтернету зі супутників. Зараз таких супутників близько 200. Очікується, що їхнє число зросте до 700 завдяки здешевленню

[189] Що Apple збирається оголосити на своєму iPad та MacBook події наступного тижня? URL: https://upost.info/uk/

запусків на низьку орбіту – з 18,5 тис. до 2,7 тис. доларів за кілограм;

• *зелені технології*. Інтернет речей (Internet of Things), великі дані (Big Data) і технології штучного інтелекту дозволять оцінити споживання, знизити попит і значно скоротити викиди вуглекислого газу, зменшивши витрати.

Основою для бізнесу, переважно в Євросоюзі, стане перехід на повністю відновлювальну енергетику. Аналітики вважають, що на велосипед пересідатиме дедалі більше жителів мегаполісів. У Deloitte вважають, що високотехнологічні компанії захочуть скористатися цим трендом і почнуть упроваджувати у виробництво велосипедів такі процеси, як 3D-друк, займуться розробкою додатків і карт, які оптимально підійдуть для їзди на велосипеді.

Прогнозується різкий сплеск популярності електричних технологій у виробництві велосипедів, зокрема передбачається, що у 2020–2023 роках буде продано понад 130 млн електричних велосипедів;

• *інтернет тіл.* Масове поширення отримає так званий інтернет тіл (Internet of Bodies). Йдеться про гаджети і додатки (перше покоління), які не тільки моніторитимуть різні показники людського тіла, але і самостійно коригуватимуть показники. Скажімо, помпи з інсуліном, які вимірюватимуть цукор у крові і, якщо це потрібно, автоматично вводитимуть інсулін в організм (друге покоління). Третє покоління таких пристроїв підключатиметься до мозку, що забезпечить з'єднання в реальному часі з віддаленими комп'ютерами, куди надсилатимуться дані про чимало процесів в організмі.

Крім моніторингу здоров'я, такі девайси можуть спростити і підвищити кібербезпеку. У 2017 році було розроблено мікрочип, імплантувавши який під шкіру, можна відчиняти двері, проходити авторизацію за робочим комп'ютером або оплачувати покупки[190].

[190] Какие высокие технологии станут массовыми в новом году и войдут в привычную жизнь многих людей. URL: https://korrespondent.net/business/web/4171621-5G-yy-e-velosypedy-tekhnolohycheskye-trendy-2020

Розглядаючи проблеми застосування новітніх технологій у криміналістичній діяльності, науковці та практики також зважають на можливості використання методу сферичної панорами у криміналістичній фотографії, лазерного 3D-сканування, системи оптичної візуалізації RUVIS та інших сучасних досягнень у галузі науки й техніки[191].

Зокрема, однією з новітніх наукових розробок із використанням фотокамер є метод сферичної панорами. За його допомогою можна швидко і точно зафіксувати місце події і, застосовуючи спеціальне програмне забезпечення, виготовити його сферичний макет. Під час перегляду такого макету виникає враження присутності на місці події, оскільки сферична панорама відображає простір із максимальним кутом охоплення (360° по горизонталі та 180° по вертикалі), завдяки чому отримується можливість повністю відобразити навколишню обстановку місця, у якому встановлено цифрову фотокамеру[192].

Зарубіжні науковці здійснюють численні дослідження, спрямовані на вдосконалення методів ідентифікації за ДНК, за волоссям людини, методів дослідження слідів крові на місці події, слідів пострілу на різних перешкодах тощо[193].

Скажімо, 3D-модель пальця вбитої людини була використана поліцією США для розблокування його мобільного телефону. Слідчі вважали, що телефон жертви міг би допомогти знайти вбивцю, адже в ньому могла залишитися якась фото- або аудіоінформація, яка навела б поліцію на слід злочинця. Спочатку фахівці перетворили двовимірні відбитки пальців у

---

[191] Семенов В. В., Терешкевич А. І. Використання новітніх технологій та досягнень науки й техніки в кримінальному провадженні. Криминалистика и судебная экспертиза. 2015. Вып. 60. С. 117–125; Непорада А. С. Новітні технології в криміналістиці: 3D-сканування при огляді місця події. *Криміналістичний вісник.* 2016. № 2 (26). С. 141–143.

[192] Семенов В. В., Терешкевич А. І. Використання новітніх технологій та досягнень науки й техніки в кримінальному провадженні. *Криминалистика и судебная экспертиза.* 2015. Вып. 60. С. 117–125.

[193] Science Magazine. URL: http://search.sciencemag.org/?q=forensic

тривимірні. Коли копія пальця власника смартфона була готова, на її поверхню були нанесені найтонші шари срібла, золота і міді. Це було потрібно для відтворення електропровідності подібно до шкіри живої людини. Після цього копію пальця передали поліції для продовження розслідування[194].

Поліція в Австралії за допомогою портативного 3D-сканера може з високою точністю відновити комп'ютерні моделі внутрішніх і зовнішніх сцен злочину. Ретельне дослідження місць скоєння злочинів на відкритому повітрі (зокрема в густих лісах, печерах та інших великих територіях) зазвичай займає багато часу. За допомогою «Зеведея», також відомого як ZEB1, поліція тепер може легко отримати доступ до важкодоступних місць і обмеженого простору, де іноді складно встановити громіздке обладнання для камер і штативів. Під час обертання прилад випускає лазерні промені і безперервно сканує навколишнє середовище. Він здатний виконувати більше 40 000 кадрів у секунду. На відміну від колісних мобільних систем, «Зеведей» може збирати дані на сходах і на пересіченій місцевості, а також у районах, де немає GPS[195].

Програмісти з Університету Корнелла (США) навчили нейромережу за однією фотографією створювати точну 3D-модель обличчя людини (3DMM). Алгоритм сканує світлину, відразу ж виділяє основні риси обличчя (приміром, кінчик носа). Потім вирівнює скани за орієнтирами, якщо потрібно, шукає збіги в бібліотеці[196].

---

[194] Полиция может разблокировать iPhone пальцем или лицом умершего владельца. URL: https://www.iguides.ru/main/ security/politsiya_mozhetrazblokirovat_iphone_paltsem_umershego_vladeltsa_ili_litsom_s_pomoshchyu_face_id/

[195] Сканер воссоздает сцену преступления в формате 3D. URL: https:// ribalych.ru/2014/03/03/skaner-vossozdayot-scenu-prestupleniya-v-formate-3d/

[196] Американские учёные научили нейросеть создавать 3D-модель лица по фотографии. URL: https://pikabu.ru/story/ amerikanskie_uchyonyie_nauchili_neyroset_sozdavat_3dmodel_litsa_po_fotografii_4674545

Англійські вчені розробили метод повної автоматизації процесу складання 3DMM-моделей. Їх алгоритм автоматично вибудовує знімки обличчя однієї людини відповідно до їх просторової орієнтації і на їхній основі створює тривимірну модель[197].

Хізер Дьюї-Хагборг створила 3D-портрети з ДНК, знайдених на недопалках цигарок і жувальній гумці на вулиці. Послідовності ДНК вона вводить у комп'ютерну програму, яка створює образ людини зі зразка.

Зазвичай під час цього процесу видається 25-річна версія людини. Потім модель роздруковують у 3D-портреті в натуральну величину[198].

Криміналістична 3D-реконструкція обличчя дає змогу встановити зовнішність особи за знайденими останками[199]. Наразі тривають дослідження щодо можливостей використання тривимірного друкування для реконструкції обличчя за кістками черепа[200].

Секвенсер ДНК надає можливість досліджувати біологічні зразки високого ступеня деградації. Сьогодні під час генотипоскопічних досліджень переважно використовується те, що називається профілюванням ДНК за допомогою трасування доказів, таких як волосся або зразки шкіри.

У випадках, коли ці зразки мають високий ступінь деградації, доцільно залучати такий потужний інструмент, як секвенсер ДНК – він дозволяє аналізувати старі кістки або зуби, що-

---

197 Учёные добились создания максимально реалистичных 3D-моделей лиц. URL: https://apparat.cc/news/digital-human-face/

198 Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

199 Gupta S., Gupta V., Vij H., Vij R., Tyagi N. Forensic Facial Reconstruction: The Final Frontier. Journal of Clinical and Diagnostic Research. 2015 Sep. Vol. 9 (9).

200 Thimmesch D. 3D Printing Takes the Place of Traditional Clay Modeling in Forensic Facial Reconstruction // 3Dprint.com: site / 3DR Holdings, LLC. URL: https://3dprint.com/20664/3d-printing-facial-reconstruct/

би визначити конкретний порядок нуклеотидних ДНК людини та генерувати унікальний зразок ДНК. Це може допомогти визначити особу як можливого злочинця[201].

Донедавна змішані зразки ДНК кількох осіб уважалися непридатними для дослідження, оскільки не було можливості їх розділити. Група дослідників із Нової Зеландії розробила програмне забезпечення, відоме як STRmix, яке дозволяє виокремлювати ДНК до чотирьох осіб. Зараз технологія широко використовується у Новій Зеландії та Австралії[202].

Профайлінг ДНК доволі активно використовується під час розслідування злочинів, при цьому ДНК людини зазнає впливу навколишнього середовища та хімічних речовин, що може значно зменшити її ідентифікаційний період. Водночас у волоссі людини містяться протеїни, які є суттєво стабільнішими та більш екологічно стійкими.

Як установив Глендон Паркер із колегами з Lawrence Livermore National Laboratory (США), унікальні протеїнові маркери у волоссі можуть використовуватись разом із профайлінгом ДНК для ідентифікації людини. Наразі виявлено 185 протеїнових маркерів, комбінації яких забезпечують унікальний зразок, за яким можна встановити одну людину серед мільйона. Учені сподіваються вдосконалити свій метод так, щоби можна було встановити конкретну особу серед усього населення Землі лише за однією волосиною[203].

Значний інтерес становлять новітні технології, які використовуються в дактилоскопії. Ці технології спрямовані на розширення можливостей з виявлення папілярних візерунків

---

[201] Kreeger L. R., Weiss D. M. Forensic DNA Fundamentals for the Prosecutor. Be not Afraid / American Prosecutors Research Institute; National District Attorneys Association. Nov. 2003. III, 39 p. URL: http://www.ndaa.org/pdf/forensic_dna_fundamentals.pdf

[202] Steward I. New Kiwi crime tool unravels mixed DNA. URL: http://www.stuff.co.nz/science/9577038/NewKiwi-crime-tool-unravels-mixed-DNA

[203] Parker G. J., Leppert T., Anex D. S. and others. Demonstration of Protein-Based Human Identification Using the Hair Shaft Proteome. PLoS ONE. 11 (9): e0160653. 2016. DOI: 10.1371/journal.pone.0160653

на різних поверхнях, зокрема із застосуванням різних температурних і світлових режимів тощо. Так, англійськими фірмами Polyciano Foster+Freeman, SUPERfume Foster+Freeman і Natural l Foster+Freeman розроблені технології обкурювання слідів флуоресцируючим реагентом, використання ціанакрилату і ІК-флуоресцентного дактилоскопічного порошку.

Німецькою фірмою Nincha Attestor Forensics і англійськими фірмами TFD-2 Foster+Freeman і Crime-Lite Imager Foster+Freeman запропоновані відповідно технології виявлення слідів у кліматичних камерах у низькотемпературному режимі після обробки поверхні розчином нінгідрину, високотеплової обробки слідів на паперових носіях, а також система напівавтоматичного і автоматичного поліпшення якості слідів. Такі технології дають змогу значно розширити наявні можливості виявлення папілярних візерунків на різних поверхнях, зокрема на поліетилені, шкірі, металі, пінпласті і т. д.[204]

За допомогою технологій магнітного дактилоскопіювання та автоматичної дактилоскопічної ідентифікації техніки-криміналісти, судмедексперти та співробітники поліції можуть швидко й легко порівняти відбитки пальців на місці злочину з розширеною віртуальною базою даних. Використання безконтактного дактилоскопіювання допомагає дослідникам отримати на місці злочину відбитки пальців високої якості, без забруднення[205].

Дослідники із Laboratoire de Photophysique et Photochimie Supramoléculaire et Macromoléculaire (Париж, Франція) вважають, що сучасні засоби здійснення дактилоскопічних досліджень охоплюють люміцин – кращий, швидший і дешевший

[204] Соколова О. А. Некоторые направления использования инновационных технологий при получении диагностической информации о человеке. URL: https://cyberleninka.ru/journal/n/izvestiya-tulskogo-gosudarstvennogo-universiteta-ekonomicheskie-i-yuridicheskie-nauki

[205] Automated Fingerprint Identification System (AFIS). TechTarget: site. URL: http://searchsecurity.techtarget.com/ definition/Automated-Fingerprint-Identification-System

засіб виявлення маловидимих слідів рук. Завдяки флуоресцентному барвнику – теразину, що входить до його складу, ця речовина дозволяє «підсвічувати» відбитки пальців на непористих або напівпористих поверхнях і залишає сліди придатними до подальшого дослідження ДНК[206].

Учені з Sheffield Hallam University (Велика Британія) вважають, що куркумін – це поліфенол, який міститься у корені куркуми, може бути використаний під час масспектрометричного дослідження і допомогти у здійсненні аналізу молекулярних складових відбитків пальців, що, своєю чергою, може допомогти встановити такі дані, як стать особи, що залишила відбитки, та виявити на сліді залишки наркотичних засобів[207].

Дослідницька група з Teesside University (Мідлсбро, Велика Британія) винайшла метод гіперспектральної візуалізації видимої довжини хвилі, що дозволяє виявляти найменші сліди крові та відокремлювати їх від інших плям на місці події. Дослідники використовують камеру, обладнану налаштовувальним рідкокристалічним фільтром, що робить знімки у різних довжинах хвиль і дає змогу відокремити сліди крові від інших плям на місці події. Цей метод не передбачає фізичного контакту з досліджуваними поверхнями, що дозволить уникнути пошкодження слідів та об'єктів. Наразі вчені працюють над удосконаленням пристрою для визначення конкретного дня утворення плями крові, якщо вона виникла впродовж місяця[208].

---

[206] Coxworth B. New fingerprint-lifting compound could make life easier for CSIs // NEW ATLAS: site / Gizmag Pty Ltd. October 29, 2013. URL: http://newatlas.com/lumicyano-fingerprint-lifting/29582/

[207] Gebel E. Analyzing Fingerprints With A Dash Of Turmeric // c&en: Chemical & Engineering News: site. American Chemical Society. May 8, 2013. URL: http://cen.acs.org/articles/91/web/2013/05/Analyzing-Fingerprints Dash-Turmeric.html?h=-519488094

[208] Li B., Beveridge P., O'Hare W. T., Islam M. The application of visible wavelength reflectance hyperspectral imaging for the detection and identification of blood stains. Science & justice. 2014 Dec. Vol. 54, Iss. 6. P. 432–438. DOI: 10.1016/j.scijus.2014.05.003.

Рентгено-фотоелектронна спектроскопія (XPS) – технологія, яка перебуває на завершальній стадії розробки й дозволить «читати» «хімічний підпис» на волокнах тканин і, відповідно, ідентифікувати одяг злочинця за найменшими мікроволокнами, залишеними на місці події[209].

Криміналістичне радіовуглецеве датування становить скориговану технологію радіовуглецевого аналізу з урахуванням збільшення або зменшення рівня радіовуглецю щодо певних показників упродовж останніх 50 років[210].

Мас-спектрометрія з лазерною абляцією та індуктивно пов'язаною плазмою допомагає досліджувати виявлені на місці події частки скла практично будь-якого розміру на рівні його атомарної структури, що дає змогу встановити походження мікроскопічних часток скла на одязі злочинця від зразків, вилучених з місця події[211].

Магнітно-резонансна томографія (МРТ) як різновид методу променевої діагностики є найбільш перспективним напрямком для отримання діагностичної інформації за судово-медичних досліджень. Основною перевагою застосування такого методу є можливість тривалого зберігання об'єктивних результатів дослідження, зокрема в електронному вигляді. Крім того, за результатами МРТ можливо встановити зажиттєвий або посмертний характер колотих, вогнепальних та інших пошкоджень на трупі, виявити гематоми (крововиливи), переломи кісток у важкодоступних за звичайного розтину трупа

---

[209] Strohmeier B. Chemical Characterization of Material Surfaces Using X-ray Photoelectron Spectroscopy (XPS): The Perfect Complement to Electron Microscopy Techniques. Microscopy and Microanalysis. Vol. 20, Iss. S3. P. 2062–2063. DOI: 10.1017/S1431927614012045.

[210] Bulman Ph., McLeod-Henning D. Applying Carbon-14 Dating to Recent Human Remains. National Institute of Justice Journal. Iss. No. 269. March 2012. URL: https://www.nij.gov/journals/269/pages/carbon dating.aspx

[211] Dodds A.J., Pollock E.M. "Chip", Land D. P. Forensic Glass Analysis by LA-ICP-MS: Assessing the Feasibility of Correlating Windshield Composition and Supplier: final tech. rep. URL: http://www.ncjrs.gov/pdffiles1/nij/grants/232134.pdf

місцях, як-от в області обличчя, голови, внутрішніх органів тощо[212].

Фотографування з альтернативним освітленням допомагає виявити ушкодження на тілі потерпілого ще до того, як вони проявляться на шкірі. Спеціальна камера з використанням синього світла та помаранчевих фільтрів чітко вказує на підшкірні ушкодження, невидимі неозброєним оком[213].

Водночас, на думку Степанюка Р. Л. і Лапти С. П., доводиться констатувати ще доволі низький рівень використання новітніх досягнень криміналістичної техніки в практичній діяльності вітчизняних органів правопорядку. Зокрема, вчені зазначають, що деякі новітні галузі застосування техніко-криміналістичних засобів і методів, які сьогодні вважаються актуальними за кордоном, поки що не набули належного розвитку в Україні[214].

На наш погляд, вивчення практичного досвіду та теоретичних напрацювань зарубіжних колег уможливить підвищення якості криміналістичної діяльності в нашій країні.

[212] Соколова О. А. Некоторые направления использования инновационных технологий при получении диагностической информации о человеке. URL: https://cyberleninka.ru/ journal/n/izvestiya-tulskogo-gosudarstvennogo-universiteta-ekonomicheskie-i-yuridicheskie-nauki.

[213] Becker W.D. 10 Modern Forensic Science Technologies. Forensic Colleges: site. Sechel Ventures. URL: http://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

[214] Степанюк Р. Л., Лапта С. П. Новітні зарубіжні розробки та перспективні дослідження у галузі техніко-криміналістичного забезпечення протидії злочинності. *Право і безпека.* 2017. № 2 (56). С. 96–101.

## *Розділ 2*

# ХАРАКТЕРИСТИКА ТА ПРОБЛЕМИ ВИКОРИСТАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ

## 2.1. Комп'ютерні засоби біометричної ідентифікації особи

Будь-яке протиправне діяння залишає в навколишньому середовищі різні сліди. У процесі розкриття злочину виникає закономірна необхідність установити за цими слідами зв'язок людини, предмета чи іншого об'єкта з розслідуваною подією. Одним із основних засобів відшукання істини в цьому випадку є встановлення тотожності або ідентифікація[215].

Термін «ідентифікація» походить від латинського слова *identificare* – ототожнювати – і означає в перекладі «встановлення збігу чого-небудь з чим-небудь»[216].

Відомий криміналіст Р. С. Бєлкін визначає ідентифікацію як процес установлення тотожності об'єкта або особи за сукуп-

[215] Халиков А. Н., Яковец Е. Н., Журавленко Н. И. Юридическое, техническое и информационно-аналитическое обеспечение оперативно-розыскной деятельности: учеб. пособие / под ред. А. Н. Халикова. Москва: Юрлитинформ, 2010. С. 353.

[216] Словарь иностранных слов. 14-е изд., испр. Москва: Рус. яз., 1987. С. 183.

ністю загальних і приватних ознак шляхом порівняльного їх дослідження[217].

Особлива роль у криміналістиці відводиться спеціалізованим комп'ютерним системам ідентифікації людини. Ці системи дають змогу отримувати й аналізувати за декількома взаємопов'язаними параметрами інформацію, що прямо чи опосередковано спроможна призвести до розкриття злочину. Зокрема, останнім часом значного поширення в діяльності правоохоронних органів набули інформаційно-пошукові системи біометричної ідентифікації особи.

*Біометрична ідентифікація* – це засіб підтвердження особи; належності паспорта його власникові шляхом розпізнавання і зіставлення біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, рис обличчя тощо), що зафіксовані носіями цих даних, із особистими даними власника[218].

## *2.1.1. Класифікація найбільш поширених методів ідентифікації особи*

Найбільш поширені методи ідентифікації особи поділяються на дві групи: статичні і динамічні.

***Статичні методи*** ґрунтуються на фізіологічній (статичній) характеристиці людини, зокрема:

*1) ідентифікація особи за відбитками пальців.* В основі цього методу біометричної ідентифікації лежить унікальність папілярного узору дистальної фаланги пальця. Із зображення відбитка пальця, отриманого за допомогою спеціального сканера, формується цифровий код, який порівнюється з етало-

[217] Белкин Р. С. Криминалистическая энциклопедия: справ. пособие. Москва: БЕК, 1997. С. 78.

[218] Концепція створення Єдиного державного реєстру фізичних осіб, затверджена постановою Кабінету Міністрів України від 9 листопада 2004 р. № 1500. *Офіційний вісник України* від 26.11.2004. 2004. № 45. С. 25. Ст. 2972. Код акту 30621/2004.

ном, що був сформований раніше й знаходиться в базі даних біометричної системи ідентифікації[219];

*2) ідентифікація особи за формою обличчя.* За допомогою камери та спеціального програмного забезпечення на зображенні обличчя виділяються контури очей, брів, носа, губ, вух, підборіддя або інші параметри обличчя відповідно до вибраного алгоритму й вираховуються відстані між ними. Отримане зображення перетворюється в цифрову форму, яка зберігається в базі даних і слугує еталоном[220];

*3) ідентифікація особи за формою руки* ґрунтується на розпізнаванні геометрії кисті руки, яка також є унікальною біометричною характеристикою особи. У цьому разі отримують тримірне зображення кисті руки (розміри долоні, довжину і ширину пальців, зміну їх висоти та контури суглобів), яке фіксується спеціальною ПЗЗ-камерою з інфрачервоним підсвіченням[221];

*4) ідентифікація особи за характеристиками ока*. Око людини має дві унікальні складові: райдужну оболонку та сітківку, структури яких такі ж індивідуальні, як і будь-які інші частини людського тіла[222];

*5) ідентифікація особи за розташуванням вен на лицьовій стороні долоні.* За допомогою інфрачервоної камери прочитується малюнок вен на лицьовій стороні долоні або грона руки. Отримане зображення обробляється і за схемою розташування вен формується цифрова згортка[223];

---

[219] Don Braggins. Fingerprint sensing and analysis. *Sensor Review*. 2001. Vol. 21. № 4. P. 272–277.

[220] Сара Мюррей. Биометрия против терроризма. *Деловая неделя*. URL: http://www.dn-weekly.kiev.ua

[221] Марченко А. Идентификация по кисти руки. *ЭЛЕКТРОНИКА: Наука, Технология. Бизнес.* 2004. № 6. С. 18–19.

[222] Лосев М., Сидоров В. Интегрированные биометрические системы. Контроль доступа по радужной оболочке глаза. *ЭЛЕКТРОНИКА: Наука. Технология. Бизнес.* 2004. № 6. С. 13–15.

[223] Мороз А. О. Біометричні технології ідентифікації людини, огляд систем. *Математичні машини і системи.* 2011. № 1. С. 39–45.

*6) ідентифікація особи за ДНК.* Експерти використовують знайдені на місці злочину ДНК крові, сперми, шкіри, слини або волосся для ідентифікації злочинця. ДНК-аналіз уважається одним із найбільш дієвих методів розкриття злочинів, який дозволяє майже зі стовідсотковою вірогідністю ідентифікувати особу злочинця і ефективно доводити його причетність до скоєння протиправних дій. Крім того, за допомогою ДНК-аналізу можна ефективніше розшукувати безвісти зниклих осіб і встановлювати особи невпізнаних трупів, ідентифікувати жертв авто- і авіакатастроф.

Поміщення ДНК-профілів як ідентифікованих, так і неідентифікованих осіб до центрального обліку генетичних ознак людини дає змогу виявити зв'язки між різними злочинами. Сліди біологічного походження, вилучені на місці події, використовують для того, щоб установити ймовірність випадкового збігу генетичних ознак особи з генетичними ознаками слідів біологічного походження або виключити можливість походження цих слідів від конкретної особи[224].

***Динамічні методи*** біометричної ідентифікації ґрунтуються на поведінковій (динамічній) характеристиці людини. Це, зокрема:

*1) ідентифікація за рукописним почерком.* До цифрового коду може входити інформація графічних параметрів підпису, час підпису та динаміка натискання на поверхню, на якій цей підпис виконується. Для реалізації цього методу застосовуються різні планшети, плоскі екрани[225];

*2) ідентифікація особи за голосом*. За допомогою різних комбінацій частотних і статичних голосових характеристик формується код ідентифікації. За подальшого входження в систему відбувається порівняння «голосів». Метод дає змогу ідентифікувати особу на значній відстані[226];

---

[224] Експертна спеціальність 9.5 «Молекулярно-генетичні дослідження». URL: https://dndekc.mvs.gov.ua/

[225] Мороз А. О. Біометричні технології ідентифікації людини, огляд систем. *Математичні машини і системи.* 2011. № 1. С. 39–45.

[226] Там само.

*3) ідентифікація за клавіатурним почерком*. Для здійснення ідентифікації використовується комп'ютерна клавіатура та певне ключове слово. Основна характеристика, за якою формується еталон, – це динаміка набору ключового слова[227].

Мультимодальні біометричні системи (Multimodal Biometrics) можуть охоплювати як статичні, так і динамічні методи, що дозволяє одночасно ідентифікувати особу зразу за кількома біометричними параметрами.

## *2.1.2. Характеристика біометричних проїзних документів*

Біометрію особи як основну технологію ідентифікації було запроваджено Новоорлеанською угодою після подій 11 вересня 2001 року у США, її учасниками стали 188 країн світу[228].

Однією із актуальних проблем сьогодення є введення національних посвідчень (паспортів) громадян. Понад ста країн уводять так звані біометричні паспорти (ID cards). Біометричний паспорт відрізняється від звичайного тим, що в нього вбудований спеціальний чип, який містить двомірну фотографію його власника, а також його дані: прізвище, ім'я, по батькові, дату народження, номер паспорта, дату його видачі та закінчення терміну дії. Також на чипі міститься біометрична інформація: скан сітківки ока, відбитки пальців тощо.

Під електронними або біометричними проїзними документами розуміються всі документи, які дозволяють перетинати державний кордон (громадянські, службові та дипломатичні паспорти, візи, посвідчення особи, особи без громадянства,

---

[227] Мороз А. О. Біометричні технології ідентифікації людини, огляд систем. *Математичні машини і системи.* 2011. № 1. С. 39–45.

[228] Біометричні паспорти: кінця епопеї не видно. URL: http://www.bbc.co.uk/ukrainian/politics/2012/06/120531_biometric_passport_future_sd.shtml

біженця, дозволи на постійне проживання тощо), та до яких вмонтовано електронний носій біометричної та іншої інформації – мікрочип[229].

Практично «ID cards» з ідентифікаційним чипом дають змогу вмістити такий обсяг інформації, який уможливлює ідентифікування особи. Біометричні технології, такі як розпізнавання людини за відбитками пальців, долоней і губ, райдужною оболонкою ока, за формою голови, голосовими даними, здатні значно спростити пошук злочинців[230].

Питання збору, використання та обробки біометричних даних в Україні регулюється низкою нормативно-правових актів, а саме:

- Цивільним кодексом України;
- Законом України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»;
- Законом України «Про захист персональних даних»;
- Законом України «Про інформацію»;
- Законом України «Про правовий статус іноземців і осіб без громадянства»;
- Законом України «Про біженців та осіб, які потребують додаткового або особливого захисту»;
- Положенням про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства, затвердженим постановою Кабінету Міністрів України від 27 грудня 2017 р. № 1073;
- Інструкцією про порядок фіксації біометричних даних (параметрів) іноземців та осіб без громадянства посадовими особами Державної міграційної служби України, її територіальних органів і територіальних підрозділів, затвер-

[229] Біометричні паспорти: кінця епопеї не видно. URL: http://www.bbc. co.uk/ukrainian/politics/2012/06/120531_biometric_passport_future_sd.shtml

[230] Захаров В. П., Рудешко В. І. Проблеми інформаційного забезпечення правоохоронних структур: навчально-практичний посібник. Львів: ЛьвДУВС, 2007. С. 32.

дженою наказом МВС України від 23.11.2018 р. № 944 та зареєстрованою в Міністерстві юстиції України 17.12.2018 р. за № 1428/32880.

Зокрема, зважаючи на вимоги Євросоюзу щодо впровадження біометричних паспортів для надання безвізового режиму для українців та ІСАО щодо обов'язкового переходу країн-членів організації на використання машинозчитувальних проїзних документів[231], Верховна Рада України 20.11.2012 р. прийняла Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус»[232], яким запроваджено в Україні документи, до безконтактного електронного носія яких вноситься інформація стосовно біометричних параметрів особи, додаткових (факультативних) біометричних даних, а також даних щодо забезпечення захисту інформації.

Відповідно до п. 2 ст. 3 зазначеного Закону, *біометричні дані* – це сукупність даних про особу, зібраних на основі фіксації її характеристик, що мають достатню стабільність та істотно відрізняються від аналогічних параметрів інших осіб (біометричні дані, параметри – відцифрований підпис особи, відцифрований образ обличчя особи, відцифровані відбитки пальців рук)[233].

В Україні з початку оформлення біометричних документів із січня 2015 року оформлено понад 3,7 млн ID-карток

---

[231] За прогнозами Міжнародної організації цивільної авіації ІСАО до 2014 року майже всі паспорти у світі будуть біометричними. URL: http://www.dmsu.gov.ua/uk/home/716-za-prognozami-mizhnarodnoji-organizaciji-civilnoji-aviaciji-isao-do-2014-roku-majzhe-vsi-pasporti-u-sviti-budut-biometr ichnimi.html

[232] Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 № 5492-VI. *Голос України* від 05.12.2012. № 231.

[233] Там само.

і понад 15,6 млн паспортів громадянина України для виїзду за кордон[234].

Слід зазначити, що ще в червні 2006 року міністри внутрішніх справ, юстиції і генеральні прокурори країн «вісімки» виступили за відпрацювання єдиних критеріїв до документів із біометричними даними. Особливу увагу приділено питанню забезпечення сумісності систем ідентифікації документів нового покоління, що засвідчують особу, та їх взаємного зчитування[235].

Найбільш відомими в Європі правилами є Директива 95/46/ЄС Європейського Парламенту і Ради «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 р., а також GDPR (The General Data Protection Regulation, 2016/Загальний регламент захисту даних для європейських держав-членів), який застосовується з 25 травня 2018 року. Організації, які не є членами ЄС, потрапляють під дію GDPR, коли вони обробляють персональні дані суб'єктів даних ЄС.

У країнах Європейського Союзу впровадження в обіг проїзних документів здійснюється на підставі Правил із заходів безпеки та біометричної автентифікації, прийнятих Радою Європи 13.12.2004 р. за № 2252/2004, відповідно до яких усі нові паспорти ЄС повинні бути машинозчитувальними і мають охоплювати з 2006 року цифрові фотографії власника і з 2009 року – відбитки пальців. Біометрична інформація зберігається на чипі (електронний носій інформації) в паспорті і в національних базах даних, зокрема в Шенгенській інформаційній системі II (SIS II)[236].

У квітні 2019 року Європарламент схвалив створення однієї з найбільших у світі біометричної бази даних Common

[234] Біометричні паспорти в Україні набувають дедалі більшої популярності. URL: https://dmsu.gov.ua/news/dms/5295.html

[235] Руководители правоохранительных органов «осьмерки» высказались за выработку единых критериев к документам с биометрическими данными. ПРАЙМ-ТАСС. 2006.06.19. URL: http://www.bit.prime-tass.ru

[236] Глосарій PASOS. URL: http://novisa.com.ua/ua/glosariy-pasos.

Identity Repository (CIR), призначеної для об'єднання записів понад 350 млн осіб[237].

*Автентифікація* – це процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора[238]. Іншими словами, автентифікація – це шлях установлення вірогідності інформації, пред'явленої користувачем у разі звернення його до системи та відкриття йому доступу, якщо він має на це право[239].

Сьогодні в країнах Європи, Ізраїлі та США найбільш поширеними є два способи біометричної автентифікації: 1) за відбитками пальців; 2) за двомірним зображенням обличчя. Біометрична автентифікація за відбитками пальців вважається найбільш точною, а за двомірним зображенням обличчя може застосовуватися навіть негласно.

Крім високої надійності, на користь цих способів біометричної автентифікації також свідчить можливість їх використання практично в кожній країні. У разі відсутності в тій чи іншій країні бази даних щодо проїзних документів, джерелом порівняльних зразків для верифікації чи ідентифікації пред'явників проїзних документів можуть слугувати наявні бази даних кримінальної інформації, в яких містяться і відбитки пальців, і двомірні зображення обличчя осіб, причетних до вчинення правопорушень. Зазначені способи біометричної автентифікації застосовуються у Великобританії, Ізраїлі, Латвії, Молдові, Німеччині та США. З червня 2009 року в Греції та Фінляндії запроваджено біометричну автентифікацію за відбитка-

---

[237] EU votes for common identity repository with biometric data of non-EU citizens. URL: https://www.medianama.com/2019/04/223-eu-votes-for-common-identity-repository-with-biometric-data-of-non-eu-citizens/

[238] Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: постанова Кабінету Міністрів України від 29 березня 2006 р. № 373. *Урядовий кур'єр* від 18.04.2006. № 73–74.

[239] Концепція створення Єдиного державного реєстру фізичних осіб, затверджена постановою Кабінету Міністрів України від 9 листопада 2004 р. № 1500. *Офіційний вісник України.* 2004. № 45. С. 25. Ст. 2972.

ми пальців, а в Чехії – за відбитками пальців і за двомірним зображенням обличчя[240].

Розширення практики застосування біометричної автентифікації в країнах Євросоюзу пов'язується із запровадженням обов'язкової біометричної автентифікації іноземців (негромадян Європейського Союзу) в отриманні ними шенгенських віз.

Практика обов'язкової біометричної автентифікації іноземців під час отримання ними віз або при в'їзді на територію країни наявна у Великобританії, Ізраїлі та США. Так, у Великобританії скануються десять пальців, в Ізраїлі – лише вказівні, а в США – як вказівні (пункти пропуску через державний кордон), так і десять (дипломатичні установи за кордоном).

У найбільших пунктах перетину державного кордону Німеччини функціонують пілотні проєкти з перевірки власників віз за відбитками пальців і двомірним зображенням обличчя (проект BioDev).

У рамках проєкту «Trusted Traveler» («Надійний мандрівник») у найбільших пунктах перетину державного кордону Великобританії здійснюється додатковий контроль осіб, які в'їжджають на територію цієї країни, за райдужною оболонкою ока. У Німеччині цей спосіб біометричної автентифікації застосовується в міжнародному аеропорту м. Франкфурт[241]. Такий контроль може здійснюватися лише гласно, але, на відміну від перевірки за відбитками пальців, він не викликає в особи, що перевіряється, асоціацій з перевіркою потенційних правопорушників, тому сприймається нею значно спокійніше.

Як зазначалося, здійснення біометричної автентифікації можливо завдяки використанню спеціальних носіїв інформа-

[240] Мовчан А. В., Мовчан Д. А. Зарубіжний досвід застосування біометричної ідентифікації людини у протидії транснаціональній злочинності. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* Луганськ, 2009. № 1. С. 180–181.

[241] Там само.

ції – мікрочипів, умонтованих у ті чи інші проїзні документи. Зазвичай на мікрочип записуються відомості про проїзний документ, про власника проїзного документу, біометричні дані власника проїзного документу чи посилання на місце їх розміщення у відповідній базі даних.

Для перевірки за біометричними характеристиками осіб, що в'їжджають на територію країни, використовуються такі бази даних:

– біометричної інформації (Великобританія, Греція, Ізраїль, Норвегія);

– кримінальної інформації (наприклад, Automatic Fingerprints Identification Systems – автоматизовані системи ідентифікації відбитків пальців (Колумбія, Німеччина, США));

– біометричної і кримінальної інформації (Латвія, Фінляндія).

Вирізняють такі основні переваги впровадження паспортів із біометричною інформацією:

– використання захищених персональних даних підвищує довіру до документа з боку імміграційних і прикордонних служб;

– цим документом не можна скористатися сторонній людині;

– новий паспорт дозволяє підвищити ефективність боротьби з тероризмом і незаконною міграцією[242].

Підкреслимо, що підробити біометричний паспорт украй складно. Зокрема, внутрішні сторінки біометричного паспорта України захищаються водяними знаками з гербом і зображеннями на історичну тематику (від трипільської культури, скіфської пектораліе до перших років незалежності). Крім того, для захисту застосовуються жовто-блакитні волокна, для більшої надійності водяними знаками продубльовані номери сторінок, на другій сторінці червоним кольором надруковано номер паспорта.

[242] Захаров В. П., Рудешко В. І. Проблеми інформаційного забезпечення правоохоронних структур: навчально-практичний посібник. Львів: ЛьвДУВС, 2007. С. 33.

Сторінка з даними власника містить зображення, які видно лише під певним кутом. Неможливо підробити і саме фото, адже воно виконано за допомогою лазерного гравіювання, а інформація на електронному носії зашифрована. Чип сконструйований так, що за спроби відкріплення він просто припинить працювати[243].

Системи біометричної ідентифікації утворені із центральної бази даних і польових терміналів. Бази даних призначені для зберігання фотографій, реєстрації електронних відбитків пальців і долонь, ідентифікаційного пошуку за біометричними даними, мобільної автоматичної ідентифікації. Польовий термінал – це портативний блок біометричної ідентифікації, з'єднаний з центральною базою даних каналами радіозв'язку[244].

У зв'язку з простотою перевірки відповідності обличчя пред'явника двомірному цифровому зображенню офіційного власника проїзного документа спеціальні прилади для контролю цієї біометричної характеристики особи переважно не застосовуються. Водночас для перевірки пред'явників проїзних документів за відбитками пальців у Великобританії, Ізраїлі, США, у пунктах перетину кордону Євросоюзу застосовуються спеціальні сканери[245].

Слід зауважити, що за весь період застосування біометричних технологій створено велику кількість пристроїв (дактилоскопічних сканерів) отримання папілярних узорів пальців рук людини з використанням різних технологій, але багатьом із цих сканерів притаманна одна негативна особливість – неможливість визначити природне походження об'єкта скану-

---

[243] Особенности биометрического паспорта. URL: http://vesti-ukr.com/ infografika/81796-osobennosti-biometricheskogo-pasporta

[244] Полицейские Огайо получили новые средства биометрической идентификации. Biometrics.ru. 14.02.2006. URL: http://www.civil-identification.info

[245] Мовчан А. В., Мовчан Д. А. Зарубіжний досвід застосування біометричної ідентифікації людини у протидії транснаціональній злочинності. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* Луганськ, 2009. № 1. С. 183.

вання, тобто відрізнити справжній папілярний узор пальця від штучного (муляжу). Отже, існує ймовірність протизаконного використання папілярних узорів однієї людини, отриманих із будь-яких предметів, іншою, що дає змогу певним особам ідентифікувати себе як іншу людину. Зокрема, у 2002 році японський криптограф із національного університету Йокогами Ц. Мацумото опублікував результати своїх досліджень про те, як він із використанням желатину і пластикового шаблону виготовив підроблений палець, який успішно «проходив» через сканер у чотирьох випадках із п'яти[246].

Фахівці вважають, що є сканери, які виявляють більшість муляжів. Доволі ефективними вважаються сканери фірм Lumidigm (США) і NEC (Японія). Один сканер використовує багатоспектральне випромінювання, яке проникає під шкіру, а інший використовує не тільки зображення відбитка пальця, а й малюнок вен.

У сканерах компанії «Сонда Технолоджі» для захисту від муляжів використовується вимір пульсу. Крім того, слід ураховувати, що за накладання на палець муляжних плівок різко знижується освітленість[247].

Експерт у сфері інформаційної безпеки М. Роджерс провів експеримент, під час якого спробував «зламати» дактилоскопічний модуль Touch ID смартфона iPhone 6. Біометричний сканер iPhone 6 вмонтований в кнопку Home, для його використання необхідно попередньо створити резервний код ідентифікації і ввести зразки відбитків тих пальців, за допомогою яких користувач розблоковуватиме телефон.

Для «злому» Touch ID Роджерс сфотографував відбиток пальця власника iPhone, потім обробив фотографію в «фотошопі» – підчистив і інвертував за кольором. Відтак йому знадо-

---

[246] Михайлов М. А. Проблема идентификации личности выходит за пределы, определяемые предметом криминалистики. *Ученые записки Таврического национального университета им. В. И. Вернадского*. Серия «Юридические науки». Том 20 (59). № 2. 2007. С. 156.

[247] Биометрия 2013: пора отказываться от банковских карт. Мечта? URL: http://habrahabr.ru/post/174397/

билися плівка і лазерний принтер із роздільною здатністю 1200 dpi і товстим шаром тонера. Перед тим, як прикласти «зліпок» до кнопки iPhone, на паперову копію відбитка наноситься латексне молочко або білий столярний клей. Подібну техніку Роджерс застосовував для обходу сканера безпеки iPhone 5s.

Експерт з'ясував, що Touch ID другого покоління надійніший, ніж оригінальний модуль iPhone 5s. У нього більш висока роздільна здатність і ширше область сканування. Виготовлений зліпок повинен бути більш товстим, щоби не проступав чужий палець. Крім того, необхідна більш чітка фотографія папілярного узору.

Обійти захист iPhone 6 у домашніх умовах практично неможливо. Спосіб «злому» Touch ID набагато складніший застосовуваного для обману сканерів «силіконового» зліпка пальця, тобто від звичайних підробок сканер смартфона захищений[248].

Водночас є також організаційні методи боротьби з муляжами:

*по-перше*, необхідно встановлювати сканери за можливості в публічних місцях;

*по-друге*, для платіжних систем застосовувати спеціальний сканер, де використовується подвійне прикладання пальця, причому, вдруге сканер підказує, який саме палець потрібно докласти;

*по-третє*, використовувати так званий «тривожний палець» – його потрібно прикладати під примусом, у результаті рахунок буде заблокований і сигнал тривоги надійде правоохоронцям.

Для надійності й боротьби з помилковими спрацьовуваннями обов'язково слід використовувати два пальці. Під час проведення міжнародних тестів, де відбитки були отримані за допомогою оптичних сканерів, зафіксована ймовірність по-

[248] Обновленный Touch ID в iPhone 6 сложнее взломать, чем сканер отпечатков iPhone 5s. URL: http://www.macdigger.ru/iphone-ipod/touch-id-2-v-iphone-6-slozhnee-vzlomat-chem-skaner-otpechatkov-iphone-5s.html

милкового спрацьовування приблизно на рівні одна помилка на тисячу випадків, за використання двох пальців – одна помилка на мільйон випадків.

Відповідно до Плану заходів із створення системи контролю іноземців та осіб без громадянства, що в'їжджають на територію України, з фіксуванням їхніх біометричних даних, затвердженого розпорядженням Кабінету Міністрів України від 12 березня 2008 р. № 439-р, здійснено впровадження біометричних технологій в інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон (система «Аркан»), і у відповідні відомчі системи[249]. За інформацією Державної прикордонної служби України, для обслуговування пасажирів із біометричними паспортами технічно дообладнано 157 пунктів пропуску та 3 КПВВ на адміністративній межі з тимчасово окупованою територією АР Крим. Усього обладнано понад 1200 робочих місць і доукомплектовано більш як 400 автоматизованих робочих місць сканерами відбитків пальців. Крім того, розгорнуто понад 320 нових робочих місць на I та II лініях контролю, а також понад 420 у залізничних пунктах пропуску[250].

Наказом МВС України від 24 квітня 2019 р. № 310 затверджено Порядок фіксації біометричних даних іноземців та осіб без громадянства під час прикордонного контролю в пунктах пропуску (пунктах контролю) через державний кордон та у контрольних пунктах в'їзду-виїзду, а також здійснення провадження у справах про адміністративні правопорушення[251].

---

[249] Про затвердження Плану заходів із створення системи контролю іноземців та осіб без громадянства, що в'їжджають на територію України, з фіксуванням їх біометричних даних: розпорядження Кабінету Міністрів України від 12 березня 2008 р. № 439-р.

[250] Держприкордонслужба презентувала систему фіксації біометричних даних іноземців та осіб без громадянства. URL: https://dpsu.gov.ua/ua/news/ Derzhprikordonsluzhba-prezentuvala-sistemu-fiksacii-biometrichnih-danih-inoze mciv-ta-osib-bez-gromadyanstva/

[251] Порядок фіксації біометричних даних іноземців та осіб без громадянства під час прикордонного контролю в пунктах пропуску (пунктах

## *2.1.3. Особливості впровадження і використання біометричних систем ідентифікації особи*

Розпізнавання за допомогою біометричних технологій передбачає порівняння раніше виділеного біометричного зразка зі знову отриманими біометричними даними. Робота всіх біометричних систем заснована головно на типовому алгоритмі, який узагальнено можна відобразити так:

– *запис* – фізичний або поведінковий зразок запам'ятовується системою;

– *виділення шаблону* – унікальна інформація виділяється із зразка і створюється біометричний шаблон;

– *порівняння* – збережений зразок порівнюється з поданим;

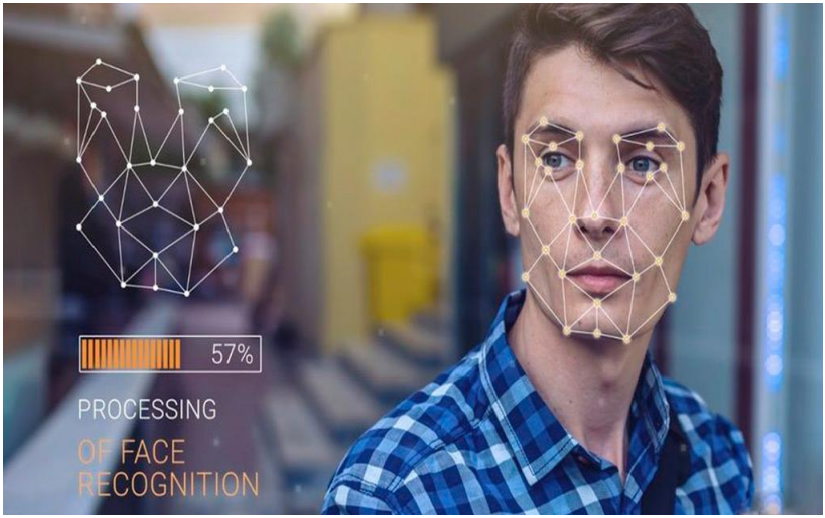
– *збіг/незбіг* – система вирішує, чи збігаються біометричні зразки, й ухвалює рішення.

Принцип роботи системи заснований на спеціальному алгоритмі переведення зображень у цифровий формат, при цьому здійснюється програмний пошук обличчя в кадрі і визначення характерних ознак його будови – так званих «реперних точок» (форма очей, вилиці, ширина перенісся, губ тощо). У результаті кожне обличчя описується унікальною сукупністю параметрів, причому навіть із незначним перебільшенням. Для ідентифікації з високим ступенем точності достатньо близько 40 характеристик, тоді як система задає декілька тисяч оціночних параметрів. Фотографія та цифровий опис обличчя заносяться в базу даних, у якій у подальшому здійснюється пошук[252] (рис. 1).

---

контролю) через державний кордон та у контрольних пунктах в'їзду-виїзду, а також здійснення провадження у справах про адміністративні правопорушення: наказ МВС України від 24 квітня 2019 року № 310. URL: https://zakon.rada.gov.ua/laws/show/z0496-19?lang=en

[252] Див.: Задорожный Ю. А. Проблемы информатизации органов внутренних дел. *Вісник Луганського державного університету внутрішніх справ*. 2007. № 2. С. 221–222; Бочковий О. В., Звонок Є. О. Віртуальні


57%
PROCESSING
OF FACE
RECOGNITION

– *цифровий «відеопотік»* (окремий фрагмент у вигляді медіафайлу або відеосигнал, який надходить у режимі on-line)[254].

Перспективним для оперативно-розшукової ідентифікації вважається використання відеоінформації з камер спостереження, встановлених на вулицях та інших місцях (супермаркети, крамниці, ринки, банківські установи, обмінні пункти валюти, вокзали, станції та вагони метрополітену, аеропорти, стадіони, спортивні комплекси, АЗС, розважальні заклади, ресторани, навчальні заклади, офіси фірм тощо), відеокамер банкоматів, автомобільних відеореєстаторів тощо.

Слід зазначити, що у нинішніх умовах протидії злочинності та тероризму біометрична ідентифікація за зображення обличчя опинилася на першому місці серед технологій розпізнавання осіб. Розпізнавання обличчя використовується під час видачі документів, що засвідчують особу, а також часто застосовується у поєднанні з іншими біометричними технологіями, як-от розпізнаванням за відбитками пальців. Розпізнавання особи також здійснюється в аеропортах за проходження митного контролю шляхом порівняння портрета у біометричному паспорті з обличчям особи власника.

У 2017 році компанія Gemalto, що спеціалізується на розробках у сфері цифрової безпеки, представила нову систему проходження контролю для аеропорту імені Шарля де Голля у Парижі на базі технології розпізнавання осіб. Зокрема, це рішення було розроблено для поступового переходу від сканування і розпізнавання відбитків пальців до розпізнавання осіб.

Упродовж останнього десятиліття алгоритмами автоматичного розпізнавання обличчя цікавилися фахівців у галузі біометрії. Наприклад, OpenFace – це інструментарій із відкритим кодом, що базується на алгоритмі FaceNet для автоматич-

[254] Задорожный Ю. А. Проблемы информатизации органов внутренних дел. *Вісник Луганського державного університету внутрішніх справ.* 2007. № 2. С. 223–224.

ної ідентифікації обличчя, створеного Google[255]. Він був розроблений та розповсюджений як програмне забезпечення з відкритим кодом Брендоном Амосом у дослідницькій групі Satya в університеті Карнегі Меллона[256]. Головні переваги OpenFace полягають у тому, що він, не потребуючи значних людських ресурсів, продемонстрував високі показники на еталоні Labeled Faces in the Wild (LFW)[257].

OpenFace може бути успішно застосований у криміналістиці, зокрема для розпізнавання обличчя підозрюваних у злочинах і людей, які зникли безвісти. Крім того, його можна використовувати для ідентифікації трупів.

Однак жоден із запропонованих проєктів поки що не зміг надати результати, які можна порівняти з ручним розпізнаванням обличчя людини[258].

Біометричну ідентифікацію за формою обличчя часто використовує поліція. У країнах Євросоюзу суворо контролюється правомірність її застосування. Приміром, у 2016 році «людину в капелюсі», яку було обвинувачено у вчиненні серії терактів у Брюсселі, викрили саме завдяки програмному забезпеченню з інтегрованою системою розпізнавання осіб ФБР. 2017 року поліція Південного Уельсу використовувала цю технологію під час фіналу Ліги чемпіонів УЄФА.

Згідно з інформацією наукового журналу Keesing Journal of Documents and Identity за червень 2018 року, використання дронів, обладнаних аерофотозйомкою, дає змогу застосувати розпізнавання осіб на великих площах під час масових заходів. Деякі безпілотники можуть переносити фотокамери

---

255 Schroff F., Kalenichenko D., Philbin J. FaceNet: A unified embedding for face recognition and clustering. IEEE Conf Comput Vis Pattern Recognit; 2015 Jun 8–10; Boston (MA). 2015. P. 815–823.

256 Amos B., Harkes J., Wang J., et al. OpenFace models. GitHub [Internet]; 2016 [cited 2016 Jan 27]. URL: https://github.com/cmusatyalab/openface/tree/master/models/openface

257 Fydanaki A. & Geradts Z. Evaluating OpenFace: an open-source automatic facial comparison algorithm for forensics. J Forensic Sci. 2018. № 33. P. 202–209.

258 Там само.

вагою до 10 кг, які можуть розпізнати потенційного злочинця на відстані 800 метрів зі 100-метрової висоти. При цьому зв'язок із наземним пунктом управління не можна перехопити[259].

У рамках реалізації програми «Безпечне місто» в Києві напередодні чемпіонату Європи з футболу 2012 року в Україні введена в експлуатацію автоматизована система централізованого управління нарядами патрульної служби «ЦУНАМІ», яка охоплює: геоінформаційну систему (електронну карту міста); систему супутникового GPS-позиціонування і мобільного комунікаційного обладнання; систему відеоспостереження; систему колективного відображення[260].

Сьогодні в Києві встановлено близько 7 тис. відеокамер: на об'єктах соціальної інфраструктури міста, у центрі міста і на автомобільних мостах через Дніпро. Смарткамери мають свій, заздалегідь запрограмований сценарій інцидентів, за виникнення яких система автоматично інформує ситуаційний центр, що дозволяє забезпечити оперативну реакцію відповідних служб[261].

«Наша правоохоронна система потребує впровадження новітніх технологій. Наразі ми масштабуємо програму «Безпечне місто» на територію всієї держави. Вона вже працює в Маріуполі, Києві та Дніпрі. Основа її діяльності – застосування сучасної інформаційно-комп'ютерної системи, яка надає можливість цілодобового моніторингу оперативної обстановки. Наші камери можуть тривалий час працювати без електрожив-

[259] Умный фейсконтроль: как технология распознавания лиц меняет мир. URL: https://psm7.com/technology/umnyj-fejskontrol-kak-texnologiya-raspoznavaniya-lic-menyaet-mir.html

[260] Міліція здатна забезпечити громадський порядок під час ЄВРО-2012. URL: http://mvs.gov.ua/mvs/control/main/uk/publish/article/445545.

[261] На вулицях Києва з'являться 600 нових камер відео спостереження. URL: https://hromadske.ua/posts/na-vulicyah-kiyeva-zyavlyatsya-600-novih-kamer-videosposterezhennya

лення, у нічний час та за будь-яких погодних умов», – зазначає А. Аваков[262].

У 2019 році Федеральне бюро розслідувань (ФБР) США оголосило про успішний запуск в експлуатацію системи розпізнавання нового покоління Next Generation Identification (NGI), яка збирає, обробляє і ідентифікує зображення обличчя, райдужну оболонку очей, татуювання та відбитки пальців.

Основною особливістю NGI є те, що вона автоматично отримує і обробляє біометричні дані з камер відеоспостереження у всій країні. Система виявляє унікальні риси обличчя тієї чи іншої людини і зберігає їх у базі даних.

У розслідуванні злочину NGI може провести швидкий аналіз зображень і виявити зловмисника. Приміром, за допомогою NGI в серпні 2019 року вдалося затримати відомого шахрая Ніла Стаммера, який переховувався від правоохоронних органів і спецслужб США упродовж чотирнадцяти років.

NGI має замінити систему IFAIS (інтегрована автоматизована система ідентифікації відбитків пальців). Якщо в IFAIS зберігалися тільки відбитки пальців, які збиралися правоохоронними органами, силовими відомствами і організаціями з підвищеним рівнем секретності, то в базу даних NGI потраплять ще й фотографії з посвідчень особи, робочих пропусків та інших документів.

База даних NGI уже містить понад 100 млн окремих записів, які пов'язують відбитки пальців людини, долонь, скан її райдужної оболонки ока, біометрії особи з особистою інформацією (домашня адреса, вік, правовий статус)[263].

Попри те, саме можливості системи з розпізнавання осіб спричиняють найбільшу критику серед правозахисників. Фактично будь-яка камера відеоспостереження з доволі високою роздільною здатністю може бути використана для негласного

[262] URL: https://www.kmu.gov.ua/news/arsen-avakov-nam-neobhidno-vprovaditi-suchasni-tehnologiyi-v-pravoohoronnu-sistemu-nashoyi-krayini

[263] ФБР запустило глобальную систему распознавания лиц. URL: https://www.gazeta.ru/tech/2014/09/16_a_6216693.shtml

збору даних про громадян, зокрема тих, хто ніколи не мав проблем із законом. Крім того, сканування профілів користувачів соціальних мереж здатне надати спецслужбам мільйони якісних світлин.

У ФБР стверджують, що проект NGI пройшов юридичну експертизу на предмет відповідності американським законам про захист приватного життя. Однак відомо, що в багатьох країнах, зокрема США, є настільки засекречені практики збору інформації спецслужбами, що навіть інформація про саме їх існування є секретною[264].

Поліція Китайської Народної Республіки також використовує систему розпізнавання осіб для розшуку і затримання підозрюваних у вчиненні злочинів. Зокрема, нещодавно за допомогою системи комп'ютерного розпізнавання осіб було впізнано в 60-тисячному натовпі чоловіка, якого підозрюють у скоєнні економічних злочинів. Поліція повідомила, що підозрюваного звати Ао, він приїхав із дружиною і друзями в місто Наньчан на концерт поп-зірки Джекі Чуна, де і був затриманий.

У березні 2019 року на залізничній станції в міському окрузі Чженчжоу поліція затримала 33 особи за підозрою в крадіжці дітей, втечі з місця ДТП і використанні фальшивих документів. Поліцейські використовували спеціальні окуляри з вмонтованим у них пристроєм, які можуть видавати інформацію про перехожого – достатньо просто на нього подивитися (рис. 2).

У серпні 2019 року на фестивалі пива в Циндао поліція Шаньдуна за допомогою цих технологій затримала 25 підозрюваних.

Китай лідирує в розробках технологій розпізнавання осіб за допомогою штучного інтелекту і регулярно нагадує своїм громадянам, що сховатися від поліції, яка має у своєму розпорядженні такі технічні засоби, практично

[264] Новая система распознавания лиц и биометрической идентификации ФБР готова к эксплуатации. URL: http://habrahabr.ru/company/nordavind/ blog/236993/

неможливо. Китайська влада стверджує, що в країні створюється найбільша в світі мережа камер відеоспостереження. Нині вже працюють близько 170 млн камер зовнішнього спостереження, до 2020 року планується встановити 600 млн відеокамер[265].


*Рис. 2. Для китайської поліції розробили окуляри з технологією розпізнавання осіб. Фото: medium.com*

У Великобританії з 2012 року діє законодавство, яке регулює роботу з камерами вуличного спостереження, а також збереження та доступ до інформації. Технологія розпізнавання осіб використовується в Британії з 2016 року, зокрема у Лондоні і населених пунктах навколо нього встановлено 500 тисяч

[265] Распознавание лиц: почему в Китае не скрыться даже в 60-тысячной толпе. URL: https://www.bbc.com/russian/news-43751391

відеокамер. З літа 2019 року технологія розпізнавання осіб розпочала працювати в аеропорту Хітроу.

У засобах масової інформації регулярно з'являються фото і відео підозрюваних у різних злочинах – із вуличних відеокамер. Скажімо, 15 вересня 2017 року Ахмед Хассан влаштував вибух на станції метро «Парсонс-грін» – поліція зуміла встановити всі його дії того дня.

Також за допомогою відеокамер поліція ідентифікувала «Олександра Петрова» і «Руслана Бошірова», яких вважають виконавцями замаху на колишнього співробітника російських спецслужб Сергія Скрипаля в Солсбері.

29 травня 2019 року під час судового процесу, у якому розслідується теракт на Лондонському мосту 3 червня 2017 року, слідство показало не тільки мінівен, на якому пересувалися нападники, але і їхні переговори напередодні[266].

Ефективність застосування систем біометричної ідентифікації в правоохоронній діяльності залежить від багатьох чинників. Так, поліція графства Лестершир (Великобританія) заявила про успішне впровадження системи NeoFace компанії NEC. Позитивний результат цього експерименту обумовлений високою якістю зображень у базі даних поліцейського управління графства, в якій на момент упровадження системи зберігалося 92 тис. записів. Для формування цієї бази було придбано спеціальне програмне забезпечення.

Водночас лондонські поліцейські вважають, що за зображенням, знятим у вуличних умовах, проводити ідентифікацію набагато складніше і ефективність її істотно знижується. Якщо в аеропортах якість зображення доволі висока, то вже в супермаркетах можуть спостерігатися збої. Результат розпізнавання може бути негативним, якщо камера не мегапіксельна, освітлення компромісне, ракурс зйомки не фронтальний, а на задньому плані є джерела світла.

[266] Система распознавания лиц. Как она работает на примере Москвы и Лондона. URL: https://www.bbc.com/russian/features-48478959

Системи розпізнавання за зображенням особи, що знаходяться на озброєнні лондонської поліції, за півтора року роботи зуміли ідентифікувати ледь десяток розшукуваних. Для порівняння: штатні лондонські розпізнавачі упізнають упродовж тижня до півтори сотні людей. У розслідуванні так званих «лондонських бунтів» (серпень 2011 року) один із суперрозпізнавачів зумів упізнати 180 осіб, у той час як система зуміла знайти лише один збіг[267].

Зараз у великих містах практично не залишилося місць, які опинилися поза полем зору однієї або декількох камер – поліцейські і муніципальні камери на вулицях і площах, приватні системи відеоспостереження в крамницях і кафе, відеореєстратори в автомобілях, камери смартфонів, Google Glass та інших подібних гаджетів – часто за нами можуть спостерігати кілька об'єктивів одночасно. Якщо додати до цього функції розпізнавання осіб у соціальних мережах і просунуті системи відеоаналітики – отже, майже кожен наш крок записується і аналізується.

Кожна дія породжує протидію, і віднедавна один за одним почали з'являтися проєкти, мета яких – захиститися від тотального спостереження або хоча б привернути увагу суспільства до цієї проблеми.

Наприклад, Ісао Етідзен, професор Токійського національного інституту інформатики, і Сейіті Госі, професор технологічного університету Токіо Когакуін, пропонують носити окуляри, в які вмонтовані інфрачервоні світлодіоди. Їхнє світло невидиме для очей, але більшість камер чутливі в ближньому інфрачервоному діапазоні. Увімкнені світлодіоди суттєво ускладнюють розпізнавання особи або навіть перетворюють його в розпливчасту пляму світла.

Нью-йоркський художник і хакер Адам Харві в своєму проекті CV Dazzle з допомогою бібліотеки OpenCV і скриптів на Java і Processing підібрав кілька варіантів зачісок і макіяжу, які значно ускладнюють роботу алгоритмів розпізнавання осіб.

[267] Мнения правоохранителей о распознавании лиц разделились. URL: http://www.secnews.ru/digest/ 21049.htm.

За даними Державної служби статистики, в Україні лише в метро впродовж року перевозиться 726 млн пасажирів (Київ – 504, Харків – 215, Дніпро – 7), для перевезення пасажирів використовується 1190 вагонів метрополітену (Київ – 824, Харків – 321, Дніпро – 45)[270].

Попри те, за останні десятиліття здійснено низку терористичних актів у метрополітені найбільших міст світу. Зокрема, 25 липня 1995 р. на станції метро в центрі Парижа вибухнув газовий балон, начинений цвяхами, – вісім людей загинули і 117 були поранені. У результаті теракту 3 грудня 1996 р. – четверо загиблих, 100 поранених.

20 березня 1995 р. терористи з радикального руху «Аум Сінрікьо» на п'яти станціях токійського метро застосували отруйний газ зарин. У результаті газової атаки загинуло 12 осіб, 5,5 тис. отримали отруєння.

Уранці 7 липня 2005 р. у лондонському метро з інтервалом в 50 сек. сталися три вибухи, через годину смертник підірвав автобус. У результаті терактів загинули 52 людини, 700 отримали поранення.

У московському метрополітені скоєно 8 терористичних актів, під час яких 116 осіб загинуло, 419 – поранено. 11 квітня 2011 року на станції метро «Жовтнева» в Мінську скоєно терористичний акт, у результаті якого 15 людей загинуло, 203 – поранено[271].

З огляду на те, що аеропорти, вокзали, станції метрополітену є місцем масового перебування людей, проблеми своєчасної ідентифікації терористів і вибухових пристроїв є надзвичайно актуальними в сучасних умовах. Одним із напрямів підвищення безпеки пасажирів є застосування сучасних біометричних систем. Подібні системи вже впроваджуються в аеропорту Хітроу (Великобританія), аеропорту імені Джона Кеннеді (США) і в інших транспортних вузлах.

---

[270] Транспорт і зв'язок України – 2015: статистичний збірник. Київ: Державна служба статистики України, 2015. С. 181.

[271] Теракты в московском метро: длинная история взрывов. URL: http://www.chuchotezvous.ru/social-disasters/24.html

Біометрична інформаційно-пошукова система відеоспостереження дозволяє в автоматичному режимі проводити ідентифікацію в потоці людей, здійснюючи перевірку отриманих зображень за базами даних осіб, які перебувають у розшуку. Виділені зображення осіб передаються на сервери розпізнавання (які можуть бути як локальними, так і віддаленими), в яких здійснюється миттєва, за частки секунди, перевірка зображень осіб із фотографіями розшукуваних терористів, злочинців, правопорушників. У разі подібності фотозображення людини, знятої відеокамерою в натовпі, з розшукуваною особою, система сповіщає в установленому порядку уповноважений правоохоронний орган, який і ухвалює рішення щодо подальших оперативних заходів. Таким чином, система вирішує такі завдання: розпізнавання осіб у потоці людей, пошук осіб у відеоархіві, пошук осіб у базі даних, що містить фотозображення та персональні дані[272].

Зокрема, у червні 2017 року розпочалися перші випробування системи розпізнавання осіб у кількох аеропортах США. Пасажирам авіакомпанії Jet Blue Airways, що стала ініціатором експерименту, не доведеться навіть діставати свої паспорти та інші документи, щоби потрапити на борт літака. Новій системі достатньо глянути на обличчя людей, щоб перевірити їх через бази даних служб безпеки і зареєструвати на рейс[273].

Однією з ключових проблем у впровадженні та експлуатації систем біометричної ідентифікації за зображенням особи є складні умови роботи. На ефективність роботи алгоритмів ідентифікації, а, отже, і на ефективність пошуку в потоці людей, безпосередньо впливають такі чинники, як умови освітлення (рівень і рівномірність), ракурси осіб, якість контрольних світлин, швидкість, щільність, напрямок потоку людей і низка інших.

2012 року японська компанія «Хітачі Кокусай Електрик» представила систему з камерою прихованого спостереження,

[272] «Сова-видеопоток». URL: http://www.ladacom.ru/ site/node/18

[273] Как умнеет полиция. URL: https://www.kommersant.ru/doc/3390024

що дозволяє обробляти базу даних у 36 млн осіб за 1 секунду. Система об'єднує осіб, які повертаються в межах 30 градусів і мають мінімальний розмір на зображенні 40 на 40 пікселів. Це допомагає виявити зловмисників, чиї фотографії занесені в базу даних осіб, які знаходяться в розшуку[274].

У рамках міжнародної конференції World Robot-2015 у Пекіні (Китай) відбулася презентація трьох бойових роботів китайського виробництва, призначених для боротьби з тероризмом. Один із них виконує функцію хіміка-розвідника і сапера. В його обов'язки входить виявлення отруйних і вибухових речовин, після чого він негайно передає інформацію військовослужбовцям спецпідрозділів. Інший робот займатиметься утилізацією виявлених боєприпасів. Він важить лишень 12 кг і може транспортуватися на спині бійця. Основне його призначення – допомога в індивідуальних місіях. У разі виникнення «гарячих» ситуацій за справу береться третій робот-боєць, який оснащений зброєю невеликого калібру і гранатометом. Із сучасними прицілами, робот зможе знищувати терористів на далекій відстані.

Розробником роботів є компанія з Харбіна HIT Robot Group. Серед потенційних покупців бойових роботів – пекінська поліція. Набір із трьох машин може обійтися в 1,5 млн юанів (235 тис. доларів)[275].

Окремий тип роботів допомагає поліції оцінювати обстановку в умовах дуже поганої видимості, приміром, в абсолютній темряві. Перед тим, як направити наряд поліції в темну квартиру, де можуть ховатися підозрювані, активують робота Throwbot XT (довжина – 36 см, вага – 0,5 кг, шум – лишень 22 дБ).

Завдяки спеціальній оптичній системі він дозволяє оператору, що сидить за пультом управління, чітко бачити те, що

[274] Как умнеет полиция. URL: https://www.kommersant.ru/doc/3390024

[275] В Китае создали трио боевых роботов. URL: https://rg.ru/2015/12/ 07/robot-site-anons.html

недоступно людському погляду. Це істотно спрощує проведення ризикованих поліцейських операцій[276].

Однією із передових у протидії тероризму є технологія зворотньо-розсіяного рентгенівського випромінювання (ЗРРП). У використанні технології ЗРРП рентгенівські промені від джерела не проходять крізь об'єкт, а відбиваються. Об'єкт не потрібно просвічувати наскрізь, тому можна використовувати випромінювання з інтенсивністю на кілька рівнів нижче, ніж за проникаючого. До речовин із малою атомною масою належать вибухові і наркотичні речовини, спиртовмісні рідини, тканини тіла людини. Це дає змогу легко ідентифікувати приховані органічні матеріали або людей, які можуть становити загрозу безпеці[277].

Переносний радар «Голограф» працює за допомогою надкоротких радіоімпульсів на частоті від 1 до 4 ГГц, пропускаючи їх через будь-які матеріали та приймаючи відбитий сигнал, і виявляє рух на відстані до 6,5 м. Пристрій має невеликі габарити і вагу 4,5 кг, витримує падіння на бетон із висоти 1 м і може використовуватися за температур від -20°С до +50°С. «Голограф» здатний розпізнавати рух крізь цеглу, бетон, дерево, гіпс, глину, сухий ґрунт і штукатурку, головне – щоби матеріал не містив води[278].

Компанія Technische Universitat Ilmenau (ФРН) створила в 2017 році унікальний високочутливий компактний прилад, який дозволяє з високим ступенем деталізації спостерігати крізь перешкоди. Розробники пристрою стверджують, що він дає змогу заглянути за бетонні й цегляні стіни багатометрової товщини. Фахівці компанії переконані, що їх «всевидюче око» допоможе в поліцейських і рятувальних операціях, а також у боротьбі з тероризмом. Однак новина про створення «всевидючого» пристрою не викликала особливого захвату у грома-

[276] Каких роботов используют полицейские из разных стран. URL: https://ubr.ua/ukraine-and-world/power/kakih-robotov-ispolzuut-policeiskie-iz-raznyh-stran-417564

[277] URL: http://www.rosscan.com/orri

[278] URL: http://jre.cplire.ru/jre/jan12/3/text.html

дян. Багато хто побоюється, що прилад німецької компанії може бути використаний не тільки правоохоронцями та рятувальниками, але і терористами, злодіями, комерційними агентами, співробітниками політичного нагляду, збоченцями і просто неадекватними особами[279].

Видання USA Today повідомило, що практично всі американські спецслужби для виявлення людей всередині будівель застосовують радар RANGE-R, вартість якого становить 6 тис. доларів. В описі приладу зазначається, що запатентована L-3-технологія ступінчастої частоти безперервної хвилі (SFCW) і власні алгоритми виявлення мети дозволяють радару працювати, як високочутливий детектор руху Доплера, хоча американці продають RANGE-R як типовий авторадар[280].

Фізики Массачусетського технологічного інституту (MTI) придумали в 2016 році, як за допомогою звичайного Wi-Fi-передавача можна спостерігати людей крізь стіни. Вчені впевнені, що нова технологія знадобиться спецслужбам і правоохоронним органам. Технологія працює вельми просто: Wi-Fi-маршрутизатор передає через стіну Wi-Fi-сигнали, які відбиваються від предметів і повертаються, відображаючи картинку на екрані комп'ютера. Потім учені «налаштували» модифіковані передавачі на розпізнавання людських силуетів, а подальше поліпшення алгоритму призвело до того, що маршрутизатори навчилися визначати точний зріст і вагу людини[281].

Новітній радар-стеновізор РО-900, розроблений групою компаній «Логис-Геотех», здатний визначати місцезнаходження людини, яка рухається, на відстані до 21 м, при цьому він «бачить» крізь кілька цегляних або бетонних стін загальною товщиною до 60 см. Це дозволяє з безпечної відстані виявити терористів не тільки всередині будівель, але і на найдальшої

[279] Немецкие разработчики изобрели устройство, которое видит сквозь стены. URL: http://nalatty.com/hand-made/nemeckie-razrabotchiki-izobreli-ustrojstvo-kotoroe-vidit-skvoz-steny/

[280] URL: https://svpressa.ru/society/article/173166/

[281] Там само.

їхньому боці, визначити траєкторію руху, а бойовиків, що стоять нерухомо, радар виявить за диханням. Водночас стеновізор дуже компактний, його вага не перевищує кілограма[282].

Професор В. Овчинський зазначає, що на початку XXI століття облаштована тотальна система спостереження за людиною, яка переслідує дитину і дорослого, живого і мертвого. Одна річ, коли джерела інформації існували окремо, в різних органах і організаціях, і інша, коли їх можна зібрати воєдино, проаналізувати і скласти інформаційний портрет людини. Така унікальна можливість з'явилася зі створенням новітніх інформаційних технологій, що базуються на електронних цифрових пристроях, які здійснили революцію в зборі всіх даних завдяки системі спостереження за людиною, причому таємно від неї. Цю інформацію можна передати безоплатно або продати, у той час як джерела цієї інформації – приватні особи – навіть не підозрюють про цей процес[283].

Нині арсенал засобів стеження охоплює практично всі можливі способи ідентифікації та супроводу людини: від класичних сканерів відбитків пальців і райдужної оболонки ока до теплової сигнатури конкретної людини і мікроскопічного пилу, що розпилюється з безпілотних літальних апаратів і світиться в променях радарів.

Зокрема, компанія Voxtel готує продукт під назвою NightMarks. Це прозора рідина з крихітних нанокристалічних квантових точок на основі селеніду кадмію. Такий матеріал здатний поглинати ультрафіолетове (200-400 нм) або інфрачервоне (700-1600 нм) випромінювання, а потім ефективно передавати енергію на спеціальні нанокристалічні люмінофори, які світяться як у видимій (400-700 нм), так і в ближній інфрачервоній області спектра. Достатньо нанести таку рідину на одяг або шкіру людини (простим рукостисканням, за допомогою

[282] В России разработан портативный радар, «видящий» сквозь стены. URL: http://vegchel.ru/index.php?newsid=29609

[283] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

БпЛА або іншим способом) – і безпілотний розвідник зможе надійно відстежувати яскраву мітку з великої відстані[284].

Фахівці Sandia National Laboratories розробили RFID-мітки, які здатні реагувати на радіолокаційний імпульс і з високою точністю визначати місце розташування об'єкта стеження. Наприклад, звичайні чипи, які використовуються в крамницях, мають дальність дії в кілька метрів, а у RFID-міток від Sandia радіус до 20 км. Особливістю технології є висока прихованість: мітки «відгукуються» тільки після опромінення спеціальним радіолокаційним імпульсом. Подібні RFID-чипи можна використовувати не тільки для оперативного стеження за людьми і автотранспортом, а й як превентивний захід із контролю за зброєю, вибуховими пристроями та наркотичними засобами[285].

Технологія компанії Tracer Detection Technology передбачає використання унікальних запахів, що дозволяють безпомилково виділити шуканий об'єкт із натовпу. Фахівці компанії винайшли спеціальний парафіновий олівець, наповнений перфторвуглеродами– термічно стабільними сполуками, які використовуються повсюдно: від виробництва холодильників до парфумерії. Пари перфторвуглеродів можуть відстежуватися за допомогою різних датчиків, як-от газового хроматографа. Достатньо провести олівцем по об'єкту стеження – і він упродовж кількох годин виділятиме специфічний, непомітний для людського носа аромат[286].

Компанія Photon-X розробляє технологію 3D-моделювання обличчя людини за кількома знімками з оптичних і інфрачервоних камер безпілотників. Спеціальне програмне забезпечення дає змогу створити детальний профіль голови людини

[284] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

[285] Технологии слежки: как идет охота на людей. URL: https://zoom.cnews.ru/rnd/article/item/tehnologii_slezhki_kak_idet_ohota_na_lyudej

[286] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

за допомогою мультиспектральних датчиків і аналізу руху лицьових м'язів. Нова система дозволить ідентифікувати людину в натовпі і супроводжувати її без необхідності встановлення будь-яких маяків. Зрозуміло, оптичні сенсори не можуть стежити за людиною всередині будівлі, проте вони здатні легко знайти її навіть на велелюдній вулиці великого міста[287].

Дослідники з Оксфордського університету за підтримки DeepMind і NVIDIA розробили машинний алгоритм читання по губах LipNet. На відміну від няавних алгоритмів читання по губах, LipNet розпізнає не слова окремо, а фрази і пропозиції цілком. Як продемонстрували випробування програми на базі даних GRID, її точність досягає 93,4%. За даними розробників, це на 40% перевищує середній результат людей з порушеннями слуху, які використовують читання по губах у повсякденному житті як метод комунікації (52,3% точності). Машинне читання по губах має величезний потенціал для використання в боротьбі зі злочинністю: розпізнавання мови в галасливій обстановці, біометрична ідентифікація і реставрація аудіозаписів[288].

Спецслужби і правоохоронні органи різних країн світу давно використовують програми, які за рухами губ, щелеп і м'язів обличчя людини можуть розпізнати слова, які вона вимовляє. Але інтонації та емоційна складова таким програмам були не доступні. Використовуючи високошвидкісну камеру, що робить тисячі кадрів у секунду, дослідникам з Університету Васеда в Токіо вдалося зробити запис навіть найменших коливань поверхні шкіри обличчя і шиї людини, якими супроводжуються звуки, які виходять від голосових зв'язок. Після зйомки спеціалізована комп'терна програма, заснована на складних алгоритмах, перетворила зняті коливання шкіри в голос людини. При цьому збереглися не тільки зміст,

[287] Технологии слежки: как идет охота на людей. URL: https://zoom.cnews.ru/rnd/article/item/tehnologii_slezhki_kak_idet_ohota_na_lyudej

[288] В Оксфорде научили нейросеть читать по губам с точностью 93%. URL: https://apparat.cc/news/lip-reading-ai/

а й всі інтонації, що визначають емоційне забарвлення мови[289].

Для проведення оперативних і пошукових заходів підрозділи поліції використовують також рентгенотелевізійні комплекси, доглядові відеокомплекси, портативні металодетектори, сканери, комбіновані доглядові пристрої, пошукові радіометри тощо. У боротьбі з «поштовим» тероризмом найбільш часто використовуються стаціонарні рентгенотелевізійні установки, портативні рентгенотелевізійні установки, настільні рентгенотелевізійні установки, які дозволяють оглядати і виявляти вибухові та інші потенційно небезпечні речовини в багажі, листах, бандеролях, контейнерах, у залишених сумках, пакетах тощо.

Під час виявлення знарядь злочину та інших предметів «подвійного» призначення можуть залучатися спеціальні технічні засоби. Наприклад, для розпізнавання вибухових речовин використовуються ручні детектори, які виявляють сліди вибухових речовин: зокрема, аналізатори парів вибухових речовин, детектори годинникових механізмів, набори спреїв. У зв'язку з поширенням останніми роками пластикової вибухівки, яка фактично не має запаху, найбільш ефективним способом її виявлення, крім маркування, є пошук інших компонентів, що, зазвичай, застосовуються у вибухонебезпечних посилках, – батарей, детонаторів, проводів тощо.

Одним із надійних способів виявлення вибухових і деяких наркотичних речовин є застосування службових собак, здатних розпізнати ті чи інші предмети і речовини за їх запаховими слідами.

Дослідники з Університету Вашингтона в американському Сент-Луїсі на замовлення ВМС США перетворюють комах у кіборгів, яких можна застосовувати для пошуку вибухівки. Встановлено, що сарана може ідентифікувати конкретні запахи, які її навчили виявляти навіть за наявності

[289] Лучшие технологии чтения чужих мыслей. URL: https://www.dsnews. ua/future/luchshie-tehnologii-chteniya-chuzhih-mysley-05112014144700

сторонніх запахів. Комахи-кіборги можуть бути більш ефективними, ніж роботи, тому що вони використовують чимало природних датчиків, тоді як навіть найбільш передові мініатюрні хімічні пристрої використовують лише кілька датчиків.

Аби перетворити звичайну сарану в пристрій з пошуку вибухівки, інженери планують імплантувати в їхній мозок електроди. На приймачі загорятиметься червоний світлодіод за наявності вибухових речовин, а зелене світло сигналізуватиме про відсутність загрози. Дослідники планують нанести татуювання на крила комах за допомогою біосумісного шовку, здатного перетворювати світло в тепло. Лазер допоможе оператору контролювати дії кіборга: фокусування на лівому крилі забезпечить рух комахи вліво, і навпаки. Передбачається, що комаха функціонуватиме так само, як дистанційно керований дрон[290].

### *2.1.5. Особливості проведення криміналістичного аналізу ходи*

У судовій криміналістиці застосовують криміналістичний аналіз ходи. Хода визначається як схема руху, що використовується під час руху особи[291]. Це циклічна активність, яка легко знімається на відео, навіть здалеку.

Оскільки в громадських місцях населених пунктів установлено велику кількість камер відеоспостереження, зростають шанси отримати відеокадри злочинців чи підозрюваних, які пересуваються пішки. Криміналістичний аналіз ходи здебільшого використовується, якщо відеоматеріали не містять біометричних підказок для ідентифікації. Присутність, відсут-

[290] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

[291] Birch I., Vernon W., Walker J., et al. Terminology and forensic gait analysis. Sci Justice. 2015; 55: 279–284.

ність чи розмір ознак, похідних від ходи злочинця чи підозрюваного, можуть слугувати доказом. Однак методи криміналістичного аналізу ходи ще не здатні до ідентифікації. Тому результати аналізу ходи використовуються лише як підтверджувальний доказ[292].

Судово-медичний аналіз ходи застосовується як підтверджувальний доказ у кримінальних розслідуваннях низки країн: зокрема, у Великобританії – більше 15 років[293], у Данії – понад 10 років[294].

У науковій літературі запропоновано різні підходи до криміналістичного аналізу ходи. Так, комп'ютерний аналіз ходи полягає у розробці алгоритмів автоматизованого розпізнавання ходи з відеоматеріалів[295]. Не вимагаючи жодного або обмеженого втручання користувача, алгоритм обчислює особливості ходи та порівнює їх між злочинцем і підозрюваним.

У методах, що ґрунтуються на спостерігачах, аналітики ходи систематично оцінюють наявність чи відсутність певних ознак ходи та порівнюють їх між злочинцем і підозрюваним. Останній підхід застосовувався у кількох кримінальних справах[296].

---

[292] Nina M. Van Mastrigt, Kevin Celie, Arjan L. Mieremet, Arnout C. C. Ruifrok &Zeno Geradts. Critical review of the use and scientific basis of forensic gait analysis. J Forensic Sci. 2018; 33: 183-193.

[293] Birch I., Gwinnett C., Walker J. Aiding the interpretation of forensic gait analysis: development of a features of gait database. Sci Justice. 2016; 56: 426–430; Bouchrika I., Goffredo M., Carter J., et al. On using gait in forensic biometrics. J Forensic Sci. 2011; 56: 882–889.

[294] Larsen P. K., Simonsen E. B., Lynnerup N. Gait analysis in forensic medicine. J Forensic Sci. 2008; 53: 1149–1153.

[295] Bouchrika I., Goffredo M., Carter J., et al. On using gait in forensic biometrics. J Forensic Sci. 2011; 56: 882–889; Nixon MS, Bouchrika I, Arbab-Zavar B, et al. On use of biometrics in forensics: gait and ear. Eur Signal Process Conf. 2010; 44: 1655–1659.

[296] Larsen P.K., Simonsen E.B., Lynnerup N. Gait analysis in forensic medicine. J Forensic Sci. 2008; 53: 1149–1153; Larsen P.K., Simonsen E.B., Lynnerup N. Gait analysis in forensic medicine. SPIE-IS&T. 2007; 6491.

Золотим стандартом вимірювання ходи є 3D-аналіз руху в лабораторії[297]. Швидкість ходи є важливим чинником, що впливає на кути суглоба. Збільшення швидкості ходи супроводжується значно збільшеним згинанням, але зменшенням розгинання у стегні та коліні. У коліні значно посилюються фаза позиції згинання та зовнішнє обертання, а також підошовне згинання голеностопа. Мінімальне обертання тазу та косоокість значно збільшується[298].

У криміналістичному контексті спостереження за ходою використовується не для прямого розпізнавання, а для порівняння винного та підозрюваного. Криміналістичний аналіз ходи на основі спостерігачів охоплює систематичну оцінку наявності чи відсутності певних ознак ходи з відеоматеріалів.

У більшості випадків аналітики ходи отримують від поліції запитання, чи можуть ознаки ходи, які спостерігаються у запитуваних (злочинця) та посилальних (підозрюваних) кадрах, надходили від одних і тих же або різних осіб.

Приміром, уранці 20 липня 2016 року в Києві, на розі вулиць Богдана Хмельницького та Івана Франка, вибухнув автомобіль, у якому перебував відомий журналіст Павло Шеремет (автомобіль належав його цивільній дружині, співзасновниці видання «Українська правда» Олені Притулі). Він помер від ран майже відразу після вибуху.

За даними слідства, вибухівку під автомобіль Шеремета в ніч перед убивством заклали чоловік і жінка – вони потрапили на записи камер відеоспостереження.

Британський експерт-криміналіст професор І. Бірч, який співпрацює з поліцейськими як своєї країни, так і зарубіжжя, здійснює близько 30 аналізів ходи на рік. Саме до нього надійшов запит від українських спецслужб із проханням визначити –

[297] Bouchrika I., Goffredo M., Carter J., et al. On using gait in forensic biometrics. J Forensic Sci. 2011;56:882–889.

[298] Bejek Z., Paróczai R., Illyés Á., et al. The influence of walking speed on gait parameters in healthy people and in patients with osteoarthritis. Knee Surgery, Sport Traumatol Arthrosc. 2006;14:612–622.

хто потрапив в об'єктиви відеокамер у матеріалах у справі Шеремета[299].

12 грудня 2019 року керівництво Національної поліції України провело брифінг, на якому оголосило про затримання підозрюваних у вбивстві Павла Шеремета. За версією слідства, саме Андрій А. та Юлія К. заклали вибухівку під авто журналіста. Це підтвердили експерти Київського науково-дослідного інституту судових експертиз, а також незалежний експерт І. Бірч (Ivan Birch). Вирішальною для висунення обвинувачень А. і К. стала саме експертиза ходи[300].

## *2.1.6. Особливості ідентифікації одягу за допомогою глибокого навчання*

Сьогодні методи розпізнавання обличчя є технічно вимогливими, їх важко застосувати на практиці і вони не завжди дають бажані результати, особливо коли зображення отримуються в неідеальних умовах, коли якість відео недостатньо висока або обличчя людини прикрите[301]. Для вирішення цієї проблеми та підвищення ефективності й точності виявлення осіб, які становлять оперативний інтерес, учені проводили дослідження, спрямовані на розробку біометричних методів, які спираються на такі характеристики, як відбитки пальців, візе-

[299] URL: https://kp.ua/incidents/654930-mahystr-byolohyy-ekspert-po-pokhodke-chto-yzvestno-ob-anhlyiskom-analytyke-yz-dela-sheremeta

[300] У вбивстві Шеремета для дестабілізації ситуації в Україні підозрюють учасників АТО і кардіохірурга. URL: https://gordonua.com/ukr/publications/-u-vbivstvi-sheremeta-dlja-destabilizatsiji-situatsiji-v-ukrajini-pidozrjujut-uchasnikiv-ato-i-kardiohirurga-golovne-1479185.html

[301] Jain A. K., Klare B., Park U. Face recognition: Some challenges in forensics. IEEE International Conference on Automatic Face & Gesture Recognition and Workshops; 2011 March 21–25; Santa Barbara, CA: IEEE Press; 2011; p. 726–733.

рунки долонь і голос[302]. Однак у випадках, коли біометричних даних немає, загальним атрибутом для полегшення процесу ідентифікації осіб є одяг.

Традиційно одяг часто слугує вагомим наочним доказом, який використовується не лише для опису людей, але і для визначення особистої інформації, такої як вік, стать і соціальний статус. Останні дослідження підкреслюють важливість одягу для встановлення підозрюваних і виявлення безвісти зниклих осіб. Крім того, розпізнавання одягу може бути дуже ефективним, якщо йдеться про відео в режимі реального часу, зокрема, з камер відеоспостереження, де деталі одягу можуть бути використані для точного виявлення підозрюваних злочинців або зниклих безвісти[303].

Наприклад, у терористичному нападі в Бостоні у квітні 2013 року розпізнавання одягу виконало ключову роль у виявленні підозрюваних. Безпосередньо після нападу поліція провела розслідування на основі численних свідчень жертв теракту, щоб остаточно визначити двох підозрюваних злочинців як братів Тамерлана та Джохара Царнаєва. Під час розслідування цього злочину поліція надала громадськості детальний опис одягу, який носили підозрювані, попросивши свідків звернутися до поліції, якщо вони бачили когось, хто відповідає опису. Ураховуючи цю подію, Р. Феріс, Р. Боббітт, Л. Браун та ін. висловлюють припущення, що розслідування могло б бути ще ефективнішим, якби в поліції була система пошуку, яка спеціально розроблена для розпізнавання атрибутів (приміром, одягу) з використанням наявних кадрів відеоспостереження[304].

---

302 Hossain M. A., Makihara Y., Wang J., et al. Clothing-invariant gait identification using part-based clothing categorization and adaptive weight control. Pattern Recogn. 2010;43:2281–2291.

303 Chen Q., Huang J., Feris R., et al. Deep domain adaptation for describing people based on fine-grained clothing attributes. IEEE Conference on Computer Vision and Pattern Recognition; 2015 Jun 7–12; Boston, MA, USA: IEEE Press; 2015; p. 5315–5324.

304 Feris R., Bobbitt R., Brown L., et al. Attribute-based people search: Lessons learnt from a practical surveillance system. International Conference on Multimedia Retrieval; 2014 Apr 1-4; Glasgow, UK: ACM Press; 2014; p. 153–160.

Крім того, ідентифікація одягу може допомогти батькам знайти своїх дітей, які загубились у місцях великого скупчення людей, просто виконавши автоматизований пошук на основі конкретних ознак за допомогою камер спостереження. Скажімо, якщо зникла дитина носила червоне пальто і синій рюкзак, автоматизована система шукала би лише відповідність на основі цих деталей[305].

Нині розпізнавання одягу широко сприймається як один із найскладніших прийомів візуального дослідження, що привертає увагу численних дослідників глибокого навчання[306]. Глибоке навчання – це підклас машинного навчання, що використовує штучні нейронні мережі для таких завдань, як візуальне розпізнавання. Дослідження розпізнавання одягу на основі нейронної мережі часто зосереджуються на класифікаціях моди або виявленні одягу шляхом обробки відео з камер спостереження.

На думку М. Беделі, З. Герадса та Е. ван Ейка, поки що ідентифікація одягу в режимі реального часу з використанням систем відеоспостереження залишається дуже складною через труднощі, пов'язані з досягненням надійного виявлення та представлення атрибутів одягу[307].

Водночас фахівцям-криміналістам досі не вистачає надійних інструментів для ідентифікації одягу, що створює проблеми в процесі розслідування. Зображення різних нарядів використовуються як дані для навчання комп'ютера для ідентифікації людей на основі атрибутів одягу.

---

[305] Bedeli M., Geradts Z. & Eijk E. Clothing identification via deep learning: forensic applications. J Forensic Sci. 2018;33:219-229.

[306] Lao B., Jagadeesh K. Convolutional neural networks for fashion classification and object detection [cited 2016 June 26]. Available from: http://cs231n.stanford.edu/reports/BLAO_KJAG_CS231N_ FinalPaperFashion-Classification.pdf; Yang M., Yu K. Real-time clothing recognition in surveillance videos. 18th IEEE International Conference on Image Processing (ICIP); 2011 Sept 11–14; Brussels, Belgium: IEEE Press; 2011; p. 2937–2940; Li F.F., Karpathy A., Johnson J. CS231n: Convolutional neural networks for visual recognition; University Lecture; 2015.

[307] Bedeli M., Geradts Z. & Eijk E. Clothing identification via deep learning: forensic applications. J Forensic Sci. 2018;33:219–229.

## *2.1.7. Організаційні засади впровадження біометричних систем ідентифікації особи*

Успіх оперативного розпізнання предметів, викрадених за вчинення злочинів корисливої спрямованості або тих, які незаконно переміщуються через митний кордон, залежить від наявності в оперативних працівників професійних навичок, пов'язаних із проведенням оглядів, обшуків і спостереженням.

До документів-об'єктів оперативного розпізнання слід віднести лише ті з них, які мають очевидний зв'язок із правопорушеннями (наприклад, однозначно належать підозрюваному, містять явні ознаки підробки, позначені сигналітичними речовинами тощо), а також виявляються й оцінюються емпіричним шляхом. Важливо оперативне розпізнання грошових знаків і цінних паперів, що мають ознаки підробки.

Зважаючи на те, що процес ідентифікації передбачає встановлення тотожності невідомого об'єкта відомому на підставі збігу ознак, будь-якому фотозображенню, що братиме участь у процесі біометричного впізнання, повинні бути встановлені унікальні атрибути. У зв'язку з цим фотозображення перед виділенням унікальної інформації для створення біометричного шаблона (процес кодування) заноситься до інтегрованого банку даних із обов'язковою прив'язкою до категорійного об'єкта обліку[308].

Як засвідчує аналіз, більшість систем, що використовують біометричні технології, функціонально обмежені виконанням завдань ідентифікації або верифікації об'єкта, без можливості отримання більш повної інформації про об'єкт аналізу. Це значно знижує ефективність використання подібних систем.

[308] Задорожный Ю. А. Проблемы информатизации органов внутренних дел. *Вісник Луганського державного університету внутрішніх справ.* 2007. № 2. С. 225.

Верифікація уможливлює порівняння двох фотозображень із метою визначення ступеня схожості і відповіді на запитання «Ви дійсно той, за кого себе видаєте?».

Одним із перспективних напрямів використання систем біометричної ідентифікації особи є *здійснення пошукових заходів у кіберпросторі*. Адже соціальні мережі – це величезний архів оцифрованих зображень, які зазнають комп'ютерної обробки за допомогою відповідних систем. При цьому об'єктом дослідження може бути не тільки зображення користувача, а також особи, які були зафіксовані на передньому чи задньому плані зображення.

Маючи зображення особи, яка становить оперативний інтерес, за допомогою біометрії можливо встановити її місцезнаходження, зв'язки, або хоча б напрямок для подальшого пошуку[309].

Для урегулювання зазначених проблем Кабінетом Міністрів України схвалено *Концепцію Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року*[310].

Відповідно до *Плану заходів із виконання Концепції реалізації державної політики у сфері профілактики правопорушень на період до 2015 року*[311], передбачено встановлення систем візуального спостереження за дотриманням правопорядку та

---

[309] Бочковий О. В., Звонок Є. О. Віртуальні соціальні мережі як джерела оперативно значимої інформації для підрозділів карного розшуку МВС України. URL: http://it-crime.at.ua/publ/pitannja_ord_ta_kriminalistiki/zbirnik_ materialiv_konferenciji_u_khmelnicku_ 2010_roku/3-1-0-3.

[310] Про схвалення Концепції Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року: розпорядження Кабінету Міністрів України від 6 лютого 2013 р. № 51-р. *Урядовий кур'єр.* 2013. № 29.

[311] Про затвердження плану заходів з виконання Концепції реалізації державної політики у сфері профілактики правопорушень на період до 2015 року: постанова Кабінету Міністрів України від 8 серпня 2012 р. № 767. *Урядовий кур'єр.* 2012. № 159.

забезпеченням безпеки громадян у громадських місцях, зокрема місцях масового перебування населення на об'єктах залізничного, повітряного транспорту та зупинках громадського транспорту.

На нашу думку, у рамках виконання Державної цільової правоохоронної програми необхідно здійснити заходи за такими пріоритетними напрямами:

*1) організаційно-правовий:*

– підвищення ефективності управління та діяльності із запобігання терористичній загрозі шляхом унесення змін до законодавчих і нормативно-правових актів у сфері протидії тероризму з метою оптимізації структур суб'єктів боротьби з тероризмом і підвищення відповідальності за стан цієї діяльності керівників усіх рівнів управління;

– прийняття регіональних програм установлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) з елементами аналітичної обробки інформації;

– формування організаційної структури системи державних органів забезпечення антитерористичної безпеки, що входять до складу суб'єктів боротьби з тероризмом, розподіл їхніх функцій;

– комплексне забезпечення життєдіяльності складових (структурних елементів) системи: кадрове, фінансове, матеріальне, технічне, інформаційне тощо;

– підготовка сил і засобів системи до їх застосування згідно з призначенням;

– розроблення стратегії та планування конкретних заходів щодо забезпечення антитерористичної безпеки;

*2) організаційно-технічний:*

– створення систем відеоспостереження з елементами аналітичної обробки інформації за центральними, криміногенно активними та людними місцями міст; у закритих об'єктах (супермаркети, навчальні заклади, вокзали, аеропорти, стадіони, спортивні споруди, станції та вагони метро; за станом транспортних комунікацій);

– організація системи відстежування рухомих об'єктів із використанням глобальної системи позиціонування (GPS);

– встановлення систем безпеки на об'єктах транспортної інфраструктури шляхом розгортання при вході в пасажирську зону станцій метрополітену, залізничних вокзалів доглядової зони;

– упровадження в діяльність чергових частин органів Національної поліції апаратно-програмних комплексів;

– організація систем цифрового радіозв'язку та проводового зв'язку;

– організація каналів передачі даних (безпроводових – WI-FI, WI-MAX, 3G, 4G; проводових та оптичних)[312].

Підсумовуючи, зазначимо, що використання сучасних інформаційно-пошукових систем ідентифікації особистості може значно спростити пошук та ідентифікацію злочинців і терористів.

## 2.2. Способи і методи збирання, дослідження, оцінки та використання цифрових (електронних) доказів

### *2.2.1. Поняття комп'ютерного злочину*

Термін «кіберзлочинність» (cybercrime) доволі часто вживається поряд із дефініцією «комп'ютерна злочинність» (computer crime). Буває, що ці поняття використовуються як синоніми. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», ***кіберзлочин (комп'ютерний злочин)*** *– це суспільно небезпечне винне діяння*

[312] Проект Концепції Державної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування.

*у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України*[313].

Згідно з розділом XVI Кримінального кодексу України, до злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж або мереж електрозв'язку входять:

• несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку (ст. 361 КК України);

• створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України);

• несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України);

• несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України);

• порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363 КК України);

• перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1)[314].

---

[313] Про основні засади забезпечення кібербезпеки України: Закон України. *Відомості Верховної Ради України.* 2017. № 45. С. 42. Ст. 403.

[314] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

Одним із суб'єктів протидії кіберзлочинності в Україні є підрозділи кіберполіції. Зокрема, основним завданням Департаменту кіберполіції Національної поліції України є участь у формуванні та забезпеченні реалізації державної політики щодо запобігання та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку.

Приміром, у вересні 2019 р. поліцейські Департаменту кіберполіції викрили хакера, який за час своєї злочинної діяльності отримав несанкціонований доступ до тисяч серверів постраждалих із більш ніж 100 країн світу. Отримані інструменти він використовував як для продажу даних, так і для отримання доступу до банківських акаунтів і платіжних систем. Для залучення клієнтів 29-річний житель Харкова розміщував на спеціалізованих сайтах і форумах оголошення про продаж доступів до віддалених серверів. Для оплати таких послуг використовувалися електронні платіжні системи[315].

Також кіберполіцейські викрили злочинну групу з п'яти осіб, які впродовж останніх двох років створювали і продавали в мережі шкідливі технічні засоби, призначені для несанкціонованого втручання в роботу систем постачання та обліку спожитої електроенергії. Надалі ці апаратні комплекси налаштовувалися і використовувалися для блокування роботи процесора електролічильника, у результаті чого енергопостачальні підприємства зазнавали мільйонних збитків. Для збуту цих пристроїв організатор злочинної групи створив окремий інтернет-сайт. Залежно від виду електролічильника вартість кожного такого технічного засобу коливалася від

[315] Кіберполіція викрила злочинну групу у створенні приладів для блокування роботи лічильників. URL: https: //www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-zlochinnu-grupu-u-stvorenni-priladiv-dlya-blokuvannya-roboti-lichilnikiv/

3 до 15 тис. гривень. Отож, зловмисники заробили понад один млн гривень[316].

11 вересня 2019 р. під час проведення в Києві форуму «Cellebrite User Forum Kyiv 2019» фахівці компанії Cellebrite і Лабораторії комп'ютерної криміналістики ЕПОС розповіли учасникам конференції про свої напрацювання і поділилися передовими практиками останніх досягнень цифрової криміналістики. У сучасних умовах боротися з комп'ютерною злочинністю державі самостійно важко, адже технології розвиваються щохвилини, а злочинці постійно вдосконалюють свої схеми, щоби максимально приховати сліди. Нині злочинці припиняють користуватися аналоговими каналами зв'язку і класичними місцями для збереження інформації. Дедалі частіше вони використовують хмарні сервіси збереження інформації і абузостійкі хостинги, які не контролюються з боку держави.

Тому для кіберполіції важливо використовувати сучасні високотехнологічні інструменти для отримання доказової бази. Завдяки співпраці з приватними організаціями кіберполіцейським вдається отримувати дані, які в подальшому використовуються як цифрові докази. Крім того, за допомогою якісної аналітики Національна поліція отримує не тільки докази протиправної діяльності, а й виявляє нові злочини[317].

### *2.2.2. Поняття цифрових (електронних) доказів згідно із законодавством України. Характеристика і види цифрових доказів*

Відповідно до ст. 84 КПК України, ***доказами в кримінальному провадженні*** є фактичні дані, отримані у передбаче-

[316] Кіберполіція викрила хакера у зламі більше двох тисяч комп'ютерів українців. URL: https://www.npu.gov.ua/news/ kiberzlochini/ kiberpolicziya-vikrila-xakera-u-zlami-bilshe-dvox-tisyach-komp-yuteriv-ukraj

[317] Для протидії сучасній злочинності правоохоронці потребують якісних інструментів реверсної інженерії. URL: https://cyberpolice.gov.ua/news/sergij-demedyuk-dlya-protydiyi-suchasnij-zlochyn-nosti-pravooxoronnczi-potre i-

ному цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд установлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів[318].

У 2017 році до трьох процесуальних кодексів (Цивільного процесуального кодексу України, Господарського процесуального кодексу України та Кодексу адміністративного судочинства України) була введена нова глава, яка розширила можливості сторін у справі, – електронні докази.

Кримінальний процесуальний кодекс України і Кодекс України про адміністративні правопорушення інституту електронних доказів не отримали.

Такий вибірковий підхід викликає подив у науковців і практиків з огляду на наявність у Кримінальному кодексі України розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а також наявність відповідальності за незаконні дії з електронними грошима (ст. 200 КК України) або за шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ст. 190 КК України).

Тим паче, що злочини у сфері кібербезпеки віднедавна значно поширилися[319].

***Цифровими (електронними) доказами*** є інформація в електронній (цифровій) формі, яка містить дані про обставини, що мають значення для справи, зокрема електронні документи (текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки),

[318] Кримінальний процесуальний кодекс України. URL: https://zakon.rada.gov.ua/laws/main/4651-17

[319] Електронні докази в судовій практиці. URL: https://sud.ua/ru/news/publication/138970-elektronni-dokazi-v-sudoviy-praktitsi

текстові, мультимедійні та голосові повідомлення, метадані, бази даних й інші відомості в електронній формі[320].

Зазначені дані можуть зберігатися на портативних пристроях (картах пам'яті, мобільних телефонах тощо), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (зокрема в мережі Інтернет).

*Особливості цифрового (електронного) доказу* полягають у тому, що він є прихованим (як відбитки пальців або ДНК); легко перетинає кордони юрисдикції; може бути змінений, пошкоджений або знищений; може бути вразливим, чутливим до часу.

*Цифровий (електронний) доказ* характеризується такими ознаками: неможливістю безпосереднього виявлення людиною на фізичному рівні; нестійкістю; зміною або знищенням у процесі звичайної експлуатації пристрою; можливістю копіювання без втрати якості.

*Загальними принципами роботи з цифровими (електронними) доказами є:* кваліфіковане поводження; постійний перегляд і оновлення процедур, методів та інструментів; використання належних процедур, методів та інструментів; забезпечення допустимості цифрових доказів; забезпечення належності цифрових доказів.

Видами цифрових (електронних) доказів є:

– *локальні сліди:* сліди прямого впливу; докази опосередкованого впливу; викривлення інформації; знищення інформації; блокування інформації; відсутність доступу; порушення конфіденційності; порушення роботи комп'ютера;

– *мережні сліди:* дані про користувача (контактні дані, адреса, телефон, ім'я тощо); дані про повідомлення (номер телефону, лог-файли реєстрації доступу до тих чи інших інформаційних систем);

---

[320] Господарський процесуальний кодекс України: Закон України від 06.11.1991 № 1798-XII; Цивільний процесуальний кодекс України; Закон від 18.03.2004 № 1618-IV; Кодекс адміністративного судочинства України: Закон від 06.07.2005 № 2747-IV. URL: https://zakon.rada. gov.ua/laws/term/40260

– *електронна інформація:* цифрові фотозображення; відеоконтент; текстові документи; веб-сайти (сторінки); метадані; бази даних.

Відповідно до ч. 2 ст. 96 ГПК України, електронні докази подаються в оригіналі або в електронній копії, засвідченій електронним цифровим підписом (ЕЦП)[321].

Приміром, 14 лютого 2019 р. Велика Палата Верховного Суду, переглядаючи справу № 9901/43/19 (П/9901/43/19), ухвалила, що саме ЕЦП є головним реквізитом такої форми подання електронного доказу.

Відсутність такого реквізиту в електронному документі виключає підстави вважати його оригінальним, а отже, належним доказом у справі[322].

21 грудня 2019 р. Верховний Суд у складі колегії суддів Касаційного господарського суду в рамках справи № 910/12245/19 (ЄДРСРУ № 86504091) досліджував питання щодо альтернативи подання позову/скарги в електронному, а не в паперовому вигляді та наявності/відсутності електронного цифрового підпису.

Процесуальні документи в електронній формі мають подаватися учасниками справи до суду з використанням Єдиної судової інформаційно-телекомунікаційної системи шляхом заповнення форм процесуальних документів відповідно до Положення про Єдину судову інформаційно-телекомунікаційну систему.

Надсилання у встановленому порядку процесуальних документів в електронному вигляді передбачає використання сервісу «Електронний суд», розміщеному за посиланням https://cabinet.court.gov.ua/login, за умови попередньої реєстрації офіційної електронної адреси (Електронного кабінету) та

---

[321] Господарський процесуальний кодекс України: Закон України від 06.11.1991 № 1798-XI. URL: https://zakon.rada.gov.ua/laws/show/1798-

[322] Ухвала від 14.02.2019 № 9901/43/19 Верховного Суду. Велика Палата. URL: https://verdictum.ligazakon.net/document/79883385

з обов'язковим використанням такою особою власного електронного підпису.

10 вересня 2019 р. Верховний Суд у складі колегії суддів Касаційного адміністративного суду в рамках справи № 640/1374/19, адміністративне провадження № К/9901/16734/19, К/9901/19224/19, К/9901/19231/19 (ЄДРСРУ № 84134028), чітко вказав, що процесуальні документи, що надійшли до суду із застосуванням сервісу «Електронний суд», вважаються такими, що подані з використанням власного електронного підпису[323].

Чимало дискусій спричиняє питання щодо необхідності ЕЦП у разі подання до суду доказів електронного листування. Раніше суди не вважали поштові повідомлення електронними доказами та не вимагали засвідчувати їх за допомогою ЕЦП.

Однак у Постанові Верховного Суду від 27.11.2018 р. колегія суддів зазначила, що висновки судів щодо неналежності роздруківок електронного листування суперечать приписам ст. 8 Закону України «Про електронні документи та електронний документообіг», оскільки сила електронного документа як доказу не може бути заперечена винятково через те, що він має електронну форму та додатково не підтверджується показами свідків (учасників листування)[324].

Доволі часто сторони посилаються на інформацію із соціальних мереж опонента як доказ. Зазвичай суди використовують такі докази. Приміром, негативні висловлювання у Twitter стали підставою для рішення про відмову у визнанні позивача біженцем або особою, яка потребує додаткового захисту (Постанова Шостого апеляційного адміністративного суду від 19.03.2019 р. у справі № 826/18174/16).

---

[323] Альтернатива подання позову/скарги в електронному, а не в паперовому вигляді. URL: https://alibi.dp.ua/1218-alternativa-podannya-pozovu-skargi-v-elektronnomu-a-ne-v-paperovomu-viglyadi

[324] Електронні докази в суді: вирішення проблем доказування чи поле для фальсифікацій. URL: http://kdkako.com.ua/elektronni-dokazi-v-sudi-virishennya-problem-dokazuvannya-chi-pole-dlya-falsifikaciy/

В ухвалі Апеляційного суду м. Києва у справі № 757/16817/16 від 17.05.2017 р., спростовуючи доводи відповідача про його скрутне майнове становище, суд послався на роздруківку з його соціальної мережі, з якої вбачається, що відповідач багато подорожує.

Розглядаючи справу про скасування рішень Центральної виборчої комісії (справа №855/35/19), суд послався на відомості з офіційної сторінки Президента України у Facebook[325].

## *2.2.3. Пристрої, які можуть зберігати цифрові (електронні) докази*

Комп'ютерна система містить апаратне та програмне забезпечення, які обробляють дані і охоплюють, зокрема:

1) *контейнер*, який містить плати, мікропроцесори, жорсткий диск, пристрої пам'яті та інтерфейсні підключення;

2) *монітор* або *відеодисплей*;

3) *пристрої зберігання даних*:

– *жорсткі диски* (SCSI, SATA, IDE, жорсткі диски ноутбуків, IDE 40-контактний, 2.5 IDE 44-контактний, IDE з'єднання для живлення і передачі даних, Serial ATA (SATA), SCSI HD 68-контактний, SCSI IDC 50-контактний);

– *зовнішні жорсткі диски* (3.5 «жорсткий диск»; 2.5 «жорсткий диск»; мережевий запам'товувальний пристрій);

– *знімні носії* (дискети; Zip-диски; компакт-диск; Digital Versatile Disc);

– *флеш-накопичувачі* (звичайні флеш-накопичувачі; USB 2.0; USB 3.0; USB Type C; інші види флеш-накопичувачів);

---

[325] Електронні докази в суді: вирішення проблем доказування чи поле для фальсифікацій. URL: http://kdkako.com.ua/elektronni-dokazi-v-sudi-virishennya-problem-dokazuvannya-chi-pole-dlya-falsifikaciy/

– *карти пам'яті* (Smart Media (SM) карта; Secure Digital (SD); міні-надійної цифрової карти; мікронадійної цифрової карти; компактні флеш-карти);

4) *портативні пристрої* (дані або цифрові докази можуть бути втрачені, якщо не підтримується живлення; дані або цифрові докази на деяких пристроях, як-от мобільні телефони або смартфони, можуть бути перезаписані або видалені, коли пристрій залишається увімкненим; мобільні телефони і смартфони можуть мати програмне забезпечення, яке може бути активовано віддалено);

5) *периферійні пристрої* (клавіатура і миша; принтер; сканер; мікрофони; USB хаби і FireWire; веб-камери; читачі карти пам'яті; VoIP пристрої);

6) *інші пристрої* (стрічкові накопичувачі даних; обладнання для спостереження; цифрові фотоапарати; відеокамери; цифрові аудіорекордери; цифрові відеореєстратори; MP3-плеєри; супутникові аудіо, відеоресивери, карти доступу; відеоігрові приставки; гарнітура комп'ютерного чату; клавіатура, миша, і відео (КМ) перемикач обміну; сімкарт-рідер; приймач Глобальної системи позиціювання (GPS); зчитування відбитків великого пальцю; довідковий матеріал);

7) *комп'ютерні мережі* (мережевий концентратор; мережева карта ноутбуку і мережевий кабель; Інтернет-модеми; мережевий комутатор і блок живлення; бездротові точки доступу; бездротовий мережевий сервер; бездротові карти і пристрої; бездротова карта для ПК; бездротовий USB-пристрій; спрямована антена для бездротової карти).

Корисними для розслідування доказами можуть бути об'єднані в мережу комп'ютери з підключеними до них пристроями, а також дані, які вони містять, а саме: програмне забезпечення; документи, фотографії, файли зображень; повідомлення електронної пошти та додатки; бази даних; фінансова інформація; історія відвідувань Інтернет-сторінок; файли журналів подій, логи чатів, списки друзів; дані, що зберігаються на зовнішніх пристроях. Як докази також можуть бути використа-

ні: функції і можливості пристроїв; будь-яка інформація ідентифікації, пов'язана з комп'ютерною системою; компоненти і з'єднання, зокрема Інтернет-протоколу (IP) та адреси локальної мережі (LAN), пов'язані з комп'ютерами і пристроями; налаштування трансляцій; адреси карти доступу до середовища (MAC) або мережевої карти (NIC).

### *2.2.4. Організаційно-технічні особливості пошуку і вилучення електронно-обчислювальної техніки*

Сучасний світ неможливо уявити без щохвилинного застосування користувачами пристроїв електронно-обчислювальної техніки (ЕОТ), смартфонів, розумних годинників тощо.

Саме тому працівники Національної поліції мають володіти актуальними знаннями щодо видів ЕОТ, особливостей її використання, наявності можливостей зняття інформації з електронних інформаційних систем, обсягу та характеристики інформації, що передається з ЕОТ на зовнішні сервери.

Наразі лише найбільш підготовлені працівники оперативних і слідчих підрозділів мають достатній рівень навичок і досвіду, щоби спланувати, підготувати, провести та оформити результати таких заходів щодо ЕОТ без участі спеціалістів у галузі комп'ютерно-технічної експертизи НДЕКЦ, приватних експертних установ, спеціальних агентів або інспекторів Департаменту кіберполіції.

За власником та основним користувачем можливий розподіл ЕОТ, відповідно, на:

1) *особисту, або персональну ЕОТ*, зокрема: телефони; смартфони; планшети, електронні книжки; GPS-навігатори, GPS-трекери; фотоапарати; мережеві роутери; персональні комп'ютери (ноутбуки, десктопи, моноблоки); відеореєстратори;

2) *мережеві накопичувачі інформації*, як частини ЕОТ – флешносії інформації; карти пам'яті mini-, microSD; зовнішні накопичувачі магнітних дисків; оптичні диски; магнітні стримерні касети LTO;

3) *літальні дрони*;

4) *спільну ЕОТ*, а саме: сервери веб-додатків, баз даних, спільних файлових сховищ; сервери управління загальної системи доступу до приміщень, загальної охоронної сигналізації, відеоспостереження; сервери офісної телефонії; сервери систем електронного документообігу та спільного планування і контролю за станом виконання; мережеве маршрутизуюче, проксуюче обладнання, обладнання віртуальних приватних мереж (VPN).

Перелічені пристрої ЕОТ взаємодіють між собою через обмін даними стандартизованими і загальновідомими протоколами (технічними правилами) фізичних і віртуальних каналів передачі інформації, зокрема:

• WiFi – протокол передачі цифрових даних радіоканалами;

• GSM – стандарт для мобільного цифрового стільникового зв'язку;

• Bluetooth – технологія бездротового радіозв'язку;

• Ethernet – протокол передачі цифрових даних дротовими каналами;

• IR-технологія бездротового зв'язку із використанням інфрачервоного випромінювання;

• GPS – стандарт передачі даних супутникового зв'язку;

• USB – протокол передачі даних через універсальну послідовну шину.

Кожний пристрій, залежно від наявності та кількості мережевих інтерфейсів для взаємодії, має свої ідентифікатори. Найвідомішими із них є: IP-адреса, MAC-адреса, IMEI-номер, мережеве ім'я хоста (hostname/netname).

Огляд приміщення з метою виявлення комп'ютерної техніки, електронних пристроїв і носіїв інформації розпочинається

із візуального пошуку, за якого особлива увага приділяється під'єднаним до приладів дротам електроживлення та мережевим дротам.

Особливу увагу слід приділяти сучасним персональним пристроям, механізм блокування яких передбачає ідентифікацію користувача за параметрами обличчя (смартфони та планшети) – такі пристрої потрібно оглядати максимально обережно та під кутом до фронтальної (передньої) камери, з метою уникнення блокування.

Водночас потрібно визначити ступінь заряду батареї виявленого пристрою з метою забезпечення його доступності в розблокованому стані.

Окремо слід зафіксувати наявність на пристроях, що оглядаються, інформації щодо резервних копій файлів на віддалених хмарних сховищах, а також облікових записів користувача у хмарних сховищах: для IOS – це ICloud, для Andriod – це Google Drive. За виявлення персональних комп'ютерів перед початком їх огляду слід упевнитися, що персональний комп'ютер (ноутбук чи десктоп) не заблокований паролем.

Якщо ноутбук розблокований, слід одразу переконатися: чи не запущено програми віддаленого управління персональним комп'ютером TeamViewer, RDP, SSH; чи не запущено програми шифрування даних або логічних дисків; чи не відбувається завантаження/вивантаження файлів на віддалені сервери із допомогою веб-браузерів, або програми клієнтів File transport protocol.

Опісля слід перевірити наявність інстальованих програм для відвідування веб-сайтів Mozilla Firefox, Microsoft Explorer, Microsoft EDGE, Opera, Google Chrome, Apple Safari.

Також необхідно перевірити наявність інстальованих програм для перегляду отриманих і відсилки власних електронних поштових повідомлень Microsoft Exchange, Apple Mail, TheBat, Mozilla Thunderbird.

Слід перевірити наявність інстальованих програм для обміну миттєвими повідомленнями Telegram, Skype, Viber,

WhatsApp, Jabber, а також програми синхронізації із смартфонами та планшетами IOS ITunes. Під час виявлення мережевих роутерів найперше слід з'ясувати, чи під'єднані до нього персональні комп'ютери, смартфони, планшети або інші електронно-обчислювальні засоби.

### *2.2.5. Способи і методи збирання, дослідження, оцінки, документування та використання цифрових (електронних) доказів*

Основні принципи роботи з цифровими (електронними) доказами полягають у такому:

1) необхідно забезпечити цілісність відібраного матеріалу та збереження історії його передачі шляхом безперервного інструментального контролю за вилучення даних;

2) необхідно документувати будь-які дії, які виконуються щодо цифрових (електронних) доказів, щоби незалежна третя сторона могла, повторивши ці дії, отримати аналогічний результат;

3) необхідна підтримка спеціалістів, які повинні мати: спеціальні знання і досвід у відповідній сфері; досвід і навички поводження із цифровими джерелами інформації; розуміння досліджуваного питання; необхідні правові знання; відповідні комунікаційні навички (що дозволяють їм давати усні та письмові пояснення); достатні і необхідні мовні навички; правові підстави для залучення у процесуальні дії;

4) якщо під час огляду не присутні спеціалісти із цифрових джерел інформації, то особи, які виконують слідчі дії на місці огляду/обшуку, повинні володіти необхідними знаннями для виявлення і збору доказів;

5) органи і особи, які ведуть розслідування, зобов'язані дотримуватися законодавства, загальних криміналістичних і процесуальних принципів. Для того, щоби розумно задоку-

ментувати відомості з цифрових джерел, потрібно враховувати функціональні особливості технологій, з використанням яких їх було створено, збережено, передано тощо.

Особливості вжиття оперативно-технічних заходів і негласних слідчих (розшукових) дій з цифровими (електронними) доказами:

1) *зняття інформації з транспортних телекомунікаційних мереж* – полягає у спостереженні та фіксації змісту інформації уповноваженими оперативними підрозділами:

– за адресою в мережі передачі даних із комутацією пакетів (IP-адреса в мережі Інтернет);

– за апаратною адресою пристрою, приєднаного до мережного середовища (MAC-адреса);

– за адресою електронної пошти;

2) *зняття інформації з електронних інформаційних систем* – полягає у виявленні і фіксації відомостей, що містяться в електронній інформаційній системі шляхом:

– безпосереднього (фізичного) доступу;

– віддаленого (програмного) проникнення.

Одним із програмних продуктів, що допомагає отримати відомості щодо власника домену (сайту), його IP-адреси та дізнатися, де розміщено сервер із сайтом (хостінг або Colocation), є програма IP-Tools.

Крім того, у мережі Інтернет є безкоштовні сервіси, за допомогою яких можна отримати інформацію щодо ресурсів мережі (сайтів) (SmartWhois, Mod IP City тощо).

Для встановлення IP-адреси сайту, доменне ім'я якого відоме, можна використати програму Ping, що входить у комплект Windows.

Для отримання інформації про трафік ініціатор направляє провайдеру ухвалу слідчого судді про зняття інформації з технічних каналів зв'язку, комп'ютерних систем та інших технічних засобів, а також запит на офіційному бланку з грифом.

Провайдер самостійно здійснює підготовку інформації про здійснені з'єднання відповідно до вимог запиту і направляє відповідь ініціатору заходу.

Закріплення цифрових (електронних) доказів, одержаних у результаті передбачених КПК України слідчих (розшукових) дій чи негласних слідчих (розшукових) дій, виконується з дотриманням певних вимог до форми і змісту, зокрема:

– процесуальне оформлення протоколів, залучення спеціаліста, понятих, ужиття заходів із належного збереження цифрових носіїв даних;

– змістовне наповнення інформації, якісна та кількісна складові, повнота одержаних відомостей.

В окремих слідчих діях участь понятих не є обов'язковою, проте вона надає більшої вагомості одержаним доказам.

У межах фіксації електронних доказів слід орієнтувати слідчого на застосування носіїв інформації, які не можуть бути повторно перезаписані.

Експертиза має вирішувати питання щодо наявності в електронних доказах ознак стороннього втручання, що регулюється відповідними нормами КПК України:

• огляд, обшук, слідчий експеримент тощо – у рамках слідчих дій, відповідно до ст. 104 КПК України, супроводжується позначками атрибутів, зазначенням джерел походження даних і об'єктів;

• у рамках негласних слідчих (розшукових) дій (відповідно до ст. 246-275 КПК України);

• у результаті проведеного експертного криміналістичного дослідження.

Криміналістичне дослідження – це основний напрям документування електронних доказів. Криміналістичний процес характеризується такими стадіями:

1) *збирання інформації* – супроводжується помітками атрибутів, зазначенням джерел походження даних і об'єктів;

2) *дослідження експертами* – передбачає зчитування її з носіїв, декодування та вилучення необхідної інформації, що стосується справи;

3) *аналіз інформації* – аналізується для отримання відповідей на поставлені експерту чи спеціалісту запитання;

4) *оформлення результатів* – оформлення результатів дослідження і аналізу у встановлений законом і зрозумілій формі документ (висновок).

Технічна реалізація документування та фіксації електронних доказів здійснюється шляхом: фіксації вихідного коду веб-сторінки; зйомки відеокамерою; відеозахоплення екрану.

Отже, працівники правоохоронних органів мають бути належно фахово підготовленими, аби бути в змозі ефективно та якісно документувати протиправну діяльність як окремих правопорушників, так і організованих злочинних груп.

## 2.3. Програмні та апаратні засоби для дослідження комп'ютерної техніки та програмних продуктів

### *2.3.1. Апаратні засоби мобільної криміналістики*

Комп'ютерна експертиза досліджує велику кількість різноманітних цифрових пристроїв і джерел даних. У дослідженнях можуть використовуватися як програмні, так і апаратні засоби.

Розглянемо найбільш поширені ***апаратні засоби мобільної криміналістики.***

***Cellebrite UFED Touch 2*** – це продукт, який спочатку розроблявся для роботи в польових умовах (рис. 3).

*Рис. 3. Комплекс Cellebrite UFED Touch 2 для дослідження комп'ютерної техніки та програмних продуктів*

Концептуально розділений на дві частини:

• фірмовий планшет ***Cellebrite UFED Touch 2*** (або ***UFED 4PC*** – програмний аналог ***Cellebrite UFED Touch 2***, що встановлюється на комп'ютер або ноутбук фахівця): використовуються тільки для отримання даних;

• ***UFED Physical Analyzer*** – програмна частина, призначена для аналізу даних, витягнутих із мобільних пристроїв.

Концепція використання обладнання передбачає, що за допомогою Cellebrite UFED Touch 2 фахівець отримує дані в польових умовах, а потім у лабораторії здійснює їх аналіз за допомогою UFED Physical Analyzer.

Відповідно, лабораторний варіант становить два самостійні програмні продукти UFED 4PC і UFED Physical Analyzer, які встановлені на комп'ютері дослідника. Цей комплекс забезпечує отримання даних із максимально можливої кількості мобільних пристроїв.

Під час аналізу частина даних може бути втрачена програмою UFED Physical Analyzer. Тому рекомендується проводити контроль повноти аналізу даних, здійснений цією програмою[326].

***MSAB XR / MSAB XRY Field*** – аналог продуктів Cellebrite, що розробляється шведською компанією Micro Systemation (рис. 4). На відміну від парадигми Cellebrite, компанія Micro Systemation передбачає, що в більшості випадків їхні продукти використовуватимуться на стаціонарних комп'ютерах або ноутбуках. До продукту додається фірмовий USB-хаб, який називають на сленгу «шайба», та комплект ерехідників і дата-кабелів для підключення різних мобільних пристроїв[327].


*Рис. 4. Комплекс MSAB XR / MSAB XRY Field для дослідження комп'ютерної техніки та програмних продуктів*

[326] UFED Touch 2. URL: http://aimtech.ru /catalog/155

[327] MSAB XR/MSAB XRY Field. URL: https://www.msab.com/ products/xry/

Компанія також пропонує версії ***MSAB XRY Field*** і ***MSAB XRY Kiosk*** – апаратні продукти, призначені для отримання даних із мобільних пристроїв, реалізовані у вигляді планшета і кіоску. ***MSAB XRY*** добре зарекомендував себе за отримання даних із застарілих мобільних пристроїв.

Віднедавна набули популярності апаратні засоби для проведення chip-off (метод отримання даних безпосередньо з чипів пам'яті мобільних пристроїв), розроблені польською компанією Rusolut. За допомогою цього обладнання можна отримувати дані з пошкоджених мобільних пристроїв і пристроїв, заблокованих PIN-кодом або графічним паролем. Rusolut пропонує кілька наборів адаптерів для отримання даних із певних моделей мобільних пристроїв. Скажімо, комплект адаптерів для отримання даних із чипів пам'яті, які переважно використовуються в «китайських телефонах». Однак широке використання виробниками мобільних пристроїв шифрування даних користувача в топових моделях призвело до того, що це обладнання поступово втрачає актуальність. Витягти дані з чипа пам'яті з його допомогою можна, але вони будуть у зашифрованому вигляді[328].

## *2.3.2. Програмні засоби мобільної криміналістики*

Спостерігаючи за розвитком мобільної криміналістики, можна побачити, що в міру розвитку функціональних можливостей мобільних пристроїв відбувається і розвиток програм для їх аналізу. Якщо раніше слідчі або оперативні працівники задовольнялися даними з телефонної книги, SMS, MMS, викликами, графічними і відеофайлами, то зараз фахівців просять «витягти» більшу кількість даних, зокрема:

• дані з програм обміну повідомленнями;

[328] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

• дані з електронної пошти;
• історію відвідування ресурсів мережі Інтернет;
• дані про геолокацію;
• видалені файли й іншу видалену інформацію тощо.

Усі ці відомості можна витягти спеціальним програмним забезпеченням.

***«Мобільний криміналіст»*** – сьогодні одна з найкращих програм для аналізу даних, отриманих із мобільних пристроїв. Інтегровані переглядачі баз даних ***SQLite*** і ***plist-файлів*** дозволяють більш досконально досліджувати певні SQLite-бази даних і plist-файли вручну.

Спочатку програма розроблялася для використання на комп'ютерах, тому використовувати її на нетбуці або планшеті (пристроях із розміром екрану 13 дюймів і менш) буде некомфортно.

Особливістю програми є жорстка прив'язка шляхів, за якими розташовані файли – бази даних додатків. Тобто, якщо структура бази даних будь-якої програми залишилася незмінною, але змінився шлях, яким база даних знаходиться в мобільному пристрої, «Мобільний криміналіст» просто пропустить таку базу даних під час аналізу. Тому дослідження подібних баз даних доведеться проводити в ручному режимі, використовуючи файловий браузер «Мобільного криміналіста» і допоміжні утиліти[329].

Тенденцією останніх років є «змішання» функціоналу програм. Зокрема, виробники, які традиційно розробляли програми для мобільної криміналістики, впроваджують у свої продукти функціонал, що дає змогу досліджувати жорсткі диски. Виробники криміналістичних програм, орієнтованих на дослідження жорстких дисків, додають у них функціонал, необхідний для дослідження мобільних пристроїв. І ті, і інші додають функціонал із вилучення даних із хмарних сховищ тощо. У підсумку виходять універсальні «програми-комбайни», за допомо-

[329] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

гою яких можна здійснювати і аналіз мобільних пристроїв, і аналіз жорстких дисків, і вилучення даних із хмарних сховищ, і аналітику даних, отриманих із цих джерел.

У переліку програм для мобільної криміналістики саме такі програми посідають два місця: ***Magnet AXIOM*** – програма канадської компанії Magnet Forensics і ***Belkasoft Evidence Center*** – розробка компанії Belkasoft.

Ці програми за функціональними можливостями щодо отримання даних із мобільних пристроїв дещо поступаються програмним і апаратним засобам, описаним вище. Але вони добре здійснюють їх аналіз і можуть використовуватися для контролю повноти вилучення різних типів даних. Обидві програми активно розвиваються і стрімко нарощують свій функціонал у дослідженні мобільних пристроїв[330].

## *2.3.3. Апаратні блокіратори запису*

***Tableau T35U*** – апаратний блокіратор компанії Tableau, який дозволяє безпечно підключати досліджувані жорсткі диски до комп'ютера дослідника по шині USB3 (рис. 5)[331].


*Рис. 5. Апаратний блокіратор Tableau T35U*

[330] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

[331] Tableau T35U. URL: https://siliconforensics.com/tableau-t35u-forensic.

Цей блокіратор має роз'єми, які дозволяють підключати до нього жорсткі диски за інтерфейсами IDE і SATA (а за наявності перехідників – і жорсткі диски з іншими типами інтерфейсів). Особливістю цього блокіратора є можливість емуляції операцій «читання-запис». Це буває корисним у дослідженні накопичувачів, заражених шкідливим програмним забезпеченням[332].

***Wiebitech Forensic UltraDock v5*** – апаратний блокіратор компанії CRU. Має функціонал, аналогічний блокіратору Tableau T35U (рис. 6)[333].


*Рис. 6. Апаратний блокіратор Wiebitech Forensic UltraDock v5*

Додатково цей блок можна з'єднати з комп'ютером дослідника по більшій кількості інтерфейсів. Якщо до цього блокіратора буде підключено жорсткий диск, доступ до даних на

[332] Tableau T35U. URL: https://siliconforensics.com/tableau-t35u-forensic-bridge.html

[333] Wiebitech Forensic UltraDock v5. URL: https://www.cru-inc.com/pro ducts/wiebetech/forensic-ultradock-v5-5/

якому обмежений ATA-паролем, на дисплеї блокіратора з'явиться відповідне повідомлення. Крім того, у підключенні жорсткого диска, що має технологічну зону DCO (Device Configuration Overlay), ця зона автоматично буде розблокована для того, аби фахівець міг скопіювати дані, що знаходяться в ній.

Обидва блокіратори запису як основне підключення використовують підключення до комп'ютера дослідника по шині USB3, що забезпечує комфортні умови роботи дослідника за клонування й аналізу носіїв інформації[334].

## *2.3.4. Програмні засоби комп'ютерної експертизи*

Ще 15 років тому безперечними лідерами комп'ютерної експертизи були програми ***Encase Forensics*** і ***AccessData FTK***. Їх функціонал природним чином доповнював один одного і давав змогу отримувати максимальну кількість різних типів даних із досліджуваних пристроїв. У наші дні функціональність Encase Forensics значно відстає від пропонованих сьогодні вимог до програмного забезпечення для дослідження комп'ютерів і серверів під управлінням Windows. Використання Encase Forensics актуально в «нестандартних» випадках: коли необхідно досліджувати комп'ютери під управлінням ОС MacOS або сервера під керуванням ОС Linux, витягувати дані з файлів рідкісних форматів. Умонтована в Encase Forensics макромова Ensripts містить величезну бібліотеку готових скриптів, реалізованих виробником і ентузіастами, за допомогою яких можна здійснити аналіз великої кількості різних операційних і файлових систем[335].

---

[334] Wiebitech Forensic UltraDock v5. URL: https://www.cru-inc.com/produ cts/wiebetech/forensic-ultradock-v5-5/

[335] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL**:** https://habr.com/ru/company/group-ib/blog/454672/

***Access Data FTK*** намагається підтримувати функціональність продукту на необхідному рівні, але час обробки накопичувачів значно перевищує розумну кількість часу, яку може дозволити собі витратити середньостатистичний фахівець на подібне дослідження.

До особливостей ***Access Data FTK*** слід віднести:

• пошук за ключовими словами реалізований на дуже високому рівні;

• аналітика різних кейсів, що дозволяє виявляти взаємозв'язки в пристроях, вилучених у різних справах;

• можливість налаштування інтерфейсу програми під себе;

• підтримка файлів рідкісних форматів (приміром, баз даних Lotus Notes).

Encase Forensics і AccessData FTK можуть обробляти величезні масиви вихідних даних, що вимірюються сотнями терабайт[336].

***Magnet Axiom*** є безперечним лідером програмних засобів для комп'ютерної криміналістики. Ця програма покриває функціоналом цілі сегменти: дослідження мобільних пристроїв, витяг із хмарних сховищ, вивчення механізмів під управлінням операційної системи MacOS тощо. Програма має зручний і функціональний інтерфейс, у якому все під рукою, і може застосовуватися для розслідування інцидентів інформаційної безпеки, пов'язаних із зараженням комп'ютерів або мобільних пристроїв шкідливим програмним забезпеченням або з витоками даних[337].

Аналогом ***Magnet AXIOM*** є ***Belkasoft Evidence Center***. Belkasoft Evidence Center дозволяє витягувати і аналізувати дані з мобільних пристроїв, хмарних сховищ і жорстких дисків. При аналізі жорстких дисків здійснюється вилучення даних із веб-браузерів, чатів, інформації про хмарні сервіси, детектування зашифрованих файлів і розділів, витяг файлів за заданим

---

[336] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL**:** https://habr.com/ru/company/group-ib/blog/454672/

[337] Там само.

розширенням, даних про геолокацію, електронної пошти, даних із платіжних систем і соціальних мереж, мініатюр, системних файлів, системних журналів тощо. Має гнучкий функціонал щодо вилучення віддалених даних.

Переваги програми Belkasoft Evidence Center такі:

• широкий спектр даних із різних носіїв інформації;

• вмонтований переглядач баз даних SQLite;

• збір даних із віддалених комп'ютерів і серверів;

• інтегрований функціонал щодо перевірки виявлених файлів на Virustotal.

Недоліками програми є незручний інтерфейс і неочевидність виконання окремих дій в програмі. Для ефективного використання програми необхідно пройти відповідне навчання[338].

Поступово ринок завойовує ***X-Ways Forensics***. Особливістю цієї швейцарської програми є велика швидкість обробки даних (порівняно з іншими програмами цієї категорії) та оптимальний функціонал, що задовільняє основні потреби фахівця з комп'ютерної криміналістики. Програма має вмонтований механізм, що дозволяє мінімізувати хибнопозитивні результати. Тобто дослідник, здійснюючи відновлення файлів із жорсткого диска обсягом 100 Гб, бачить не 1 Тб відновлених файлів (велика частина з яких є хибнопозитивними результатами, як це зазвичай відбувається у використанні програм відновлення), а саме ті файли, які реально були відновлені.

За допомогою програми X-Ways Forensics можливо:

• знаходити й аналізувати дані електронної пошти;

• аналізувати історію веб-браузерів, журнали ОС Windows та інші системні артефакти;

• відфільтрувати результати, залишити тільки цінні й актуальні відомості;

---

[338] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL**:** https://habr.com/ru/company/group-ib/blog/454672/

• побудувати тимчасову шкалу і переглянути активності в період, що цікавить;

• реконструювати RAID;

• монтувати віртуальні диски;

• здійснювати перевірку на наявність шкідливого програмного забезпечення.

Ця програма дуже добре зарекомендувала себе у ручному аналізі жорстких дисків, витягнутих із відеореєстраторів. За допомогою функціоналу X-Tension є можливість підключення в програмі модулів сторонніх розробників.

До недоліків X-Ways Forensics слід віднести: аскетичний інтерфейс; відсутність повноцінного вбудованого переглядача баз даних SQLite; необхідність глибокого вивчення програми: виконання деяких дій, необхідних для отримання потрібного фахівцю результату, не завжди очевидно[339].

### *2.3.5. Апаратні засоби відновлення даних*

Нині на ринку домінує компанія ***ACELab***, яка виробляє апаратні засоби для аналізу, діагностики та відновлення жорстких дисків (комплекси PC-3000 Express, PC-3000 Portable, PC-3000 UDMA, PC-3000 SAS) (рис. 7), SSD накопичувачів (комплекс PC-3000 SSD), флеш-накопичувачів (комплекс PC-3000 Flash), RAID (комплекси PC-3000 Express RAID, PC-3000 UDMA RAID, PC-3000 SAS RAID)[340].

Домінування ACELab на ринку апаратних рішень із відновлення даних обумовлено високою якістю перелічених продук-

[339] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

[340] Технология восстановления данных. URL: https://www.acelab.ru/dep.pc/SCSItesterHDD.php

тів і ціновою політикою ACELab, яка не дозволяє конкурентам увійти на цей ринок.

Незважаючи на велику кількість різних програм відновлення, як платних, так і безкоштовних, дуже важко знайти програму, яка б коректно і повно здійснювала відновлення різних типів файлів у різноманітних файлових системах.


*Рис. 7. Засіб для аналізу, діагностики та відновлення жорстких дисків PC-3000 SAS*

Тепер існують тільки дві програми, що мають приблизно однаковий функціонал, які дають змогу це робити: ***R-Studio*** і ***UFS Explorer***. Тисячі програм відновлення інших виробників або не дотягують за своїми функціональними можливостями до зазначених програм, або істотно поступаються їм[341].

[341] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

### *2.3.6. Відкрите програмне забезпечення*

***Autopsy*** – зручний інструмент для аналізу комп'ютерів під управлінням операційної системи Windows і мобільних пристроїв під управлінням операційної системи Android, що має графічний інтерфейс. Може бути використаний у розслідуванні комп'ютерних інцидентів.

***Photorec*** – одна з ліпших безкоштовних програм для відновлення даних.

***Eric Zimmerman Tools*** – комплект безкоштовних утиліт, кожна з яких дає змогу досліджувати якийсь окремий артефакт Windows. Як засвідчила практика, використання Eric Zimmerman Tools підвищує ефективність роботи фахівця за реагування на інцидент у «польових умовах». Нині ці утиліти доступні у вигляді пакету програм ***Kroll Artifact Parser and Extractor (KAPE)***[342].

### *2.3.7. Дистрибутиви на основі Linux*

***SIFT – Linux-дистрибутив*** розроблений і підтримуваний комерційною організацією SANS Institute, яка спеціалізується на підготовці фахівців у галузі кібербезпеки і розслідуванні інцидентів. SIFT містить велику кількість актуальних версій безкоштовних програм, які можуть бути використані як для отримання даних із різних джерел, так і для їх аналізу. SIFT використовується під час проведення компанією SANS Institute навчань і його вміст постійно актуалізується.

Зручність роботи з цим дистрибутивом визначається конкретним інструментом, із яким доводиться працювати досліднику.

---

[342] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

***Kali Linux*** – унікальний Linux-дистрибутив, який використовується фахівцями для проведення аудиту безпеки і розслідування інцидентів. У 2017 році видавництво «Packt Publishing» опублікувало книгу Шива В. Н. Парасрама (Shiva V. N. Parasram) «Digital Forensics with Kali Linux», у якій наводяться практичні поради про те, як проводити копіювання, дослідження і аналіз комп'ютерів, окремих накопичувачів, копій даних із оперативної пам'яті і мережевого трафіку за допомогою утиліт, що входять у цей комплект[343].

## 2.4. Особливості використання програмно-апаратного засобу для дослідження мобільних пристроїв Cellebrite UFED Touch2

Продукти компанії Cellebrite активно використовуються правоохоронними органами Європи та США. Лишень у Лондоні за рік аналізується близько 50 тис. телефонів за допомогою UFED.

Авторизованим партнером Cellebrite в Україні є компанія ЕПОС, а офіційним дистриб'ютором рішень Cellebrite в Україні, Молдові, країнах Кавказу і Середньої Азії – міжнародна група компаній БАКОТЕК. Віднедавна в центрі уваги комп'ютерних криміналістів постали методи отримання даних не лише із смартфонів, ноутбуків і десктопів, але і з хмарних сервісів, які стають дедалі важливішим джерелом інформації, необхідної під час розслідування злочинів[344].

Компанія Cellebrite спеціалізується в галузі отримання даних із електронних пристроїв. На шпальти світової преси

[343] Ключ на старт: лучшие программные и аппаратные средства для компьютерной криминалистики. URL: https://habr.com/ru/company/group-ib/blog/454672/

[344] От взлома нет приема. URL: https://ko.com.ua/ot_vzloma_net_priema_120621

вона потрапила у зв'язку з гучним інцидентом близько трьох років тому, коли ФБР намагалося отримати в компанії Apple інструменти для злому iPhone 5S з операційною системою iOS 9, який належав одному з виконавців теракту в Сан-Бернардіно Сайеду Фаруку.

Агентство національної безпеки (АНБ) США визнало, що не змогло «зламати» смартфон терориста, хоча АНБ, за твердженням колишнього агента Едварда Сноудена, може прослуховувати навіть вимкнені смартфони.

Однак компанія Apple принципово відмовилась співпрацювати з правоохоронними органами США, яким довелося шукати експертів для розблокування iPhone терориста. Це коштувало їм близько одного млн доларів. Офіційного підтвердження того, як це було реалізовано, немає, але, враховуючи, що в активі Cellebrite є сервіс для розблокування смартфонів лінійки iPhone, уважають, що саме на рахунку цієї компанії отримання доказів у згаданій справі[345].

Компанія Cellebrite була заснована в 1999 році вихідцями з підрозділів 8200 і Мамре Армії оборони Ізраїлю, які відповідали за радіоелектронну розвідку і комп'ютерну безпеку.

Спочатку компанія Cellebrite розробила технологію резервного копіювання даних із телефонів, за допомогою якої створюється фізична копія пам'яті телефону, що дозволяє потім відновлювати дані. Зазначена технологія зацікавила спочатку приватних детективів, а пізніше – правоохоронні органи[346].

Відомою широкому загалу компанія Cellebrite стала після того, як італійські правоохоронні органи зламали iPhone міланського біржового агента Олександра Ботчера. Ботчер був затриманий після того, як 28 грудня 2014 року його подруга Мартіна Ловато облила кислотою колишнього нареченого. Слідчі підозрювали, що Ловато виконувала наказ Ботчера

[345] Российские силовики закупают оборудование для взлома любых моделей iPhone. URL: https://www.bbc.com/russian/news-43298602

[346] Там само.

і в момент злочину перебувала у нього в психологічному рабстві. Існувала версія, що Ботчер вимагав, аби Ловато приводила в будинок інших чоловіків і жінок для спільних садомазохістських оргій. Колишній наречений Ловато таке запрошення відхилив – після чого на нього було скоєно напад.

Однак Ботчер заперечував свою вину, хоча докази могли зберігатись у листуванні пари. Підозрюваний заявив, що не може розблокувати свій iPhone і показати листування, оскільки забув захисний код.

Вирішити проблему слідчі доручили судовому експерту Матті Епіфані, який передав iPhone 5 із операційною системою iOS 8, що належав Ботчеру, у мюнхенський офіс Cellebrite, де iPhone розблокували за два дні. З'ясувалося, Ботчер «забув» код «5555». У подальшому слідчі встановили, що Ботчер і Ловато планували облити кислотою і навіть каструвати ще кількох знайомих. За результатами судового розгляду зловмисники отримали вирок по 14 років позбавлення волі[347].

На сучасному етапі розвитку новітніх технологій на глобальному рівні частка платформи Android охоплює 87,8 %, тоді як iOS займає 11,5 %. Але це співвідношення значно відрізняється в різних регіонах. Зокрема, у США iOS належить частка 42,7 %, а в Китаї – лише 8,2 %, тоді як Android тут охоплює 78,9 %[348].

Саме тому сьогодні значна увага приділяється смартфонам, оскільки вони постійно супроводжують своїх власників, зберігаючи значні обсяги даних щодо їх місцезнаходження, листування, фотографії тощо.

Водночас навколо нас збільшується перелік «розумних» пристроїв. Це і годинники, і автомобілі, і маршрутизатори тощо. Відповідно, збільшується кількість форматів інформації, яка на них зберігається. Окреслене змушує фахівців Cellebrite постійно працювати над розширенням функціональності своїх

[347] Российские силовики закупают оборудование для взлома любых моделей iPhone. URL: https://www.bbc.com/russian/news-43298602

[348] От взлома нет приема. URL: https://ko.com.ua/ot_vzloma_net_priema_120621

пристроїв. Зокрема, в арсеналі Cellebrite з'явилося рішення UFED Chinex спеціально для аналізу китайських телефонів, де непередбачувано реалізована схемотехніка порту microUSB[349].

Правоохоронні органи України в своїй практичній діяльності також використовують пристрої Cellebrite, зокрема, мобільне робоче місце криміналістичної експертизи мобільних пристроїв «UFED Touch 2» вартістю 172 тис. грн. Річна ліцензія для робочого місця «UFED Touch 2» коштує 113 тис. грн.

«UFED Touch 2» – це портативний апаратно-програмний комплекс для криміналістичних досліджень, який дає змогу отримувати, декодувати і аналізувати доказові дані з різних моделей мобільних пристроїв.

Зокрема, пристрій «UFED Touch 2» дозволяє:

• вилучати і декодувати дані з обходом блокування пристроїв на базі операційних систем Android, Apple, BlackBerry, Windows Phone;

• отримувати вільний доступ до пристрою шляхом обходу і відключення систем блокування;

• відновлювати видалені з пристроїв дані;

• дешифрувати базу даних історії WhatsApp;

• отримувати дані на логічному рівні (додатки, паролі, миттєві повідомлення, контакти, SMS, MMS, електронну пошту, календар, мультимедіа, журнали викликів, інформацію про місцезнаходження телефону з різними системами тощо).

Для «злому» не потрібні спеціальні навички – тільки фізичний доступ до пристрою і час. Для «злому» застарілих моделей необхідні лічені секунди, деякі більш сучасні моделі можуть «протриматися» кілька днів[350].

Лінійка Cellebrite включає платформи для отримання даних у лабораторних умовах, а також оптимізовані пристрої для оперативної роботи. Cellebrite пропонує інструменти криміналістики і пакет аналітики, призначені для слідчих

[349] От взлома нет приема. URL: https://ko.com.ua/ot_vzloma_ net_ priema_120621

[350] URL: http://z-city.com.ua/18-12-18-13-18.12.2018

і аналітиків. Так, планшет UFED Touch2 і програмне забезпечення UFED 4PC рекомендуються для стаціонарних лабораторій. Планшет UFED Touch2 з установленим програмним забезпеченням випускається самостійно Cellebrite. Причому апарат доступний як у стандартному, так і в захищеному виконанні. А UFED для вилучення даних у відділенні поліції і в умовах оперативної роботи пропонується у варіантах моноблока UFED INFIELD, який можна застосовувати в приміщенні, і комплекту UFED TK, що включає захищений ноутбук сімейства Panasonic Toughbook і валізу.

Компанія Cellebrite також надає сервіс CAIS для вилучення інформації із заблокованих Apple iPhone. Аби скористатися ним, досліджуваний смартфон необхідно передати в сертифікований сервісний центр Cellebrite.

В Україні ЕПОС стала першою комерційною організацією, в якій була організована лабораторія кіберрозслідувань. 2007 року вона взяла на озброєння аналізатор Cellebrite UME Pro.

У рамках одного з недавно виконаних замовлень фахівці ЕПОС здійснили вилучення даних із iPhone 7 за допомогою UFED, що дає змогу відновлювати навіть видалену користувачем інформацію. У результаті фахівці отримали близько 6,3 тис. контактів. Журнал викликів містив 11 106 дзвінків і 967 SMS. Кількість облікових даних користувача в різних службах, що містять логін і пароль, дорівнює 26, прочитано 335 повідомлень у чатах у Viber, WhatsApp тощо. Кількість відновлених місць розташування становить 5588, медіа-колекція охоплює 27175 зображень і 1613 відеозаписів. Відновлена інформація про 91 бездротову мережу і 10 паролів.

Для отримання місця знаходження мобільного пристрою не обов'язково мати дані GPS. Це успішно робиться як на основі аналізу інформації про підключення до базових станцій мобільного провайдера, так і у зонах доступу Wi-Fi, база яких постійно поповнюється[351].

[351] От взлома нет приема. URL: https://ko.com.ua/ot_vzloma_ net_ priema_120621

За результатами опитування фахівців із галузі комп'ютерної криміналістики, найскладнішим завданням в їхній роботі вважається подолання блокування мобільного телефону. Сьогодні за допомогою рішень компанії Cellebrite можливо обійти захист 4172 мобільних пристроїв. У своїй діяльності компанія використовує постійно поповнюваний склад мобільних телефонів, обсяг якого досяг 25 тис. шт. Серед останніх досягнень – реалізація обходу захисту для платформ на базі чипів MediaTek MT6735 і MT6753. Подолання блокування можливе для 26 популярних моделей Motorola, для Samsung S6, S6 Edge і Note 5, Google Pixel[352].

Попри те, що Huawei використовує власні процесори Hisilicon, в яких вмонтовано доволі потужний захист, експерти Cellebrite змогли знайти спосіб обійти і його. А для лінійки смартфонів LG розроблено обхід блокування моделі G5. У найближчих планах виробника – вхід у «розумні» годинники Apple iWatch[353].

Нова можливість у лінійці Cellebrite – витяг приватних даних із хмарних сервісів. У міру зростання популярності соціальних мереж дедалі більше різноманітної інформації накопичується в акаунтах їхніх користувачів. Установлено, що близько 88 % із них уходять у ці сервіси за допомогою смартфонів і в середньому витрачають на це 1 год. 43 хв. у день. Тому інформація, яка зберігається в акаунтах, може серйозно допомогти в розслідуваннях.

Для правоохоронних органів важливо отримати доступ до облікового запису за рішенням суду в тій країні, де проводиться розслідування. У разі позитивного рішення суду є можливість зробити це за ключем, який зберігається на мобільному терміналі, або добровільно отриманий від самого користувача. Причому нещодавно було розроблено метод подолання двофакторної аутентифікації, якщо вона активована.

---

[352] От взлома нет приема. URL: https://ko.com.ua/ot_vzloma_net_priema_120621

[353] Там само.

Зазвичай час життя ключа відкритої сесії входу до соціальної мережі обмежений. Приміром, для Facebook – це три місяці, впродовж яких можна увійти в обліковий запис для створення його знімка. Пакет UFED Cloud Analyzer в своїй останній версії підтримує роботу з 26 джерелами (Gmail та Facebook) і може витягувати 13 ключів із Android і 11 – із iOS[354].

Національне антикорупційне бюро України у розслідуванні кримінальних правопорушень використовує кілька рішень Cellebrite сімейства UFED: 4PC, Infield Kiosk 2 і Touch 2. Найбільш затребуваними є функції вилучення даних на рівні файлової системи і фізичному рівні, оскільки вони надають найповнішу для розслідувань інформацію.

Серед успішно застосовуваних функцій відзначається можливість роботи з резервною копією iPhone (backup), завдяки чому вдається отримувати дані з відповідних резервних копій, які зберігаються на комп'ютерах. За інформацією експертів, застосовуючи модуль UFED User Lock Code Recovery Tool у підборі пароля смартфона, необхідно використовувати камеру, яка фіксує успішну спробу введення[355].

Пакет UFED Analytics дозволяє в стислі терміни проводити всебічний аналіз даних, отриманих у межах різних кримінальних правопорушень. Так, в автоматичному режимі аналізується зміст фото і відео з широкого спектру ключових понять, включаючи зброю, наркотики тощо. А на підставі листування, геолокаційних даних і інших чинників будуються графіки взаємних зв'язків фігурантів у кількох розслідуваннях[356].

Національна поліція України також використовує у практичній діяльності програмно-апаратні комплекси Cellebrite UFED Touch2 Ultimate в межах оперативно-розшукових справ і кримінальних проваджень у проведенні оперативно-технічних заходів і негласних слідчих (розшукових) дій зі

[354] От взлома нет приема. URL: https://ko.com.ua/ot_vzloma_ net_ priema_120621

[355] Там само.

[356] URL: https://habr.com/ru/company/group-ib/blog/454672/

зняття інформації з електронних інформаційних систем і в межах кримінальних проваджень при проведенні слідчої (розшукової) дії – огляду речі (мобільного терміналу та/або SIM-картки).

Проблема безпеки смартфонів Apple полягає в чипі Apple Secure Enclave, який відповідає за роботу функцій Touch ID і Face ID (розблокування за відбитком пальця і розпізнавання особи). Цей чип зберігає токени для розшифровки пам'яті телефона і, відповідно, отримавши доступ до цього чипу, можна шляхом перебору встановити потрібний код.

Захистити переписку від потенційного злому можна, встановивши додаткові захисні коди в додатках. У мессенджері Telegram, скажімо, є можливість установити додатковий код на вході – в такому випадку всі чати шифруються всередині смартфона і отримати доступ до листування неможливо.

Нещодавно у Cellebrite з'явився конкурент: за інформацією Forbes, американський стартап Grayshift пропонує ліцензію на злом 300 смартфонів за 15 тисяч доларів (лишень 50 доларів за один смартфон проти 1500 у Cellebrite)[357].

Водночас у 2019 компанія Cellebrite випустила нове обладнання для злому мобільних пристроїв. За твердженням компанії, воно гарантує доступ до даних на всіх моделях iPhone та iPad і багатьох смартфонах на платформі Android. Зазначена UFED Premium технологія буде доступна представникам правоохоронних органів із 11 країн, зокрема США, Канади і Великобританії.

Вихід UFED Premium було вперше анонсовано на закритій конференції з мобільної криміналістики в американському Мертл-Біч в перших числах червня 2019 року. Офіційне повідомлення про вихід технології на ринок компанія опублікувала на своєму сайті 14 червня 2019 року.

Утім, експерти сумніваються, що ця технологія дійсно допоможе швидко зламувати останні моделі iPhone і iPad, які захищені шестизначним паролем. Вони вважають, що подібні

[357] URL: https://www.bbc.com/russian/features-45172681

UFED Premium технології ґрунтуються на використанні «експлойта» (уразливості), знайденого в програмному забезпеченні смартфонів. Уразливість, яка дозволяє підбирати паролі для мобільних пристроїв Apple, була вперше використана в пристрої GrayKey, випущеному американською компанією Grayshift у 2017 році.

У наш час компанії дізнаються про «слабкі місця» мобільних платформ із «чорного» ринку, де триває торгівля вразливостями, які уможливлюють отримання доступу до iPhone. Коли про вразливість стає відомо, виробники мобільних пристроїв оновлюють операційні системи. Зокрема, Apple віднедавна наймає чимало фахівців із кібербезпеки, які забезпечують закриття подібних вразливостей[358].

## 2.5. Технології розпізнання події злочину, пов'язані з наявністю в осіб, причетних до його вчинення, засобів мобільного зв'язку

Розпізнання події злочину, пов'язане з наявністю в осіб, причетних до його вчинення, засобів мобільного зв'язку, має певні особливості.

Станом на 1 січня 2019 року кількість абонентів мобільного зв'язку в Україні становила 53,934 млн осіб, кількість абонентів Інтернет – 26,067 млн осіб, кількість абонентів безпроводового доступу в Інтернет – 20,024 млн осіб[359].

Відповідно до ст. 8 Закону України «Про оперативно-розшукову діяльність», оперативним підрозділам для виконання завдань ОРД за наявності передбачених законом підстав надається право зняття інформації з транспортних телекому-

[358] URL: https://www.bbc.com/russian/news-48679883

[359] В Україні скоротилася кількість абонентів мобільного зв'язку. URL: https://www.rbc.ua/ukr/news/ukraine-sokratilos-kolichestvo-abonentov-1550582102.html

нікаційних мереж, електронних інформаційних мереж (п. 9), здійснювати установлення місцезнаходження радіоелектронного засобу (п. 12)[360].

Під *зняттям інформації з транспортних телекомунікаційних мереж* розуміється спостереження, відбір і фіксація змісту інформації уповноваженими оперативними підрозділами із використанням у встановленому законодавством порядку відповідних технічних засобів, а також одержання, перетворення і фіксація різних видів сигналів, що передаються каналами зв'язку.

Зняття інформації з транспортних телекомунікаційних мереж забезпечує контроль, конспіративне перехоплення та фіксацію з використанням технічних засобів телефонних розмов, що передаються засобами стаціонарного та рухомого (мобільного) зв'язку, а також інших даних, котрі передаються каналом зв'язку, що контролюється (SMS, MMS, факс, модемний зв'язок).

В ухвалі слідчого судді про дозвіл на втручання у приватне спілкування в цьому випадку додатково повинні бути зазначені ідентифікаційні ознаки, які дозволять унікально ідентифікувати абонента спостереження, транспортну телекомунікаційну мережу, кінцеве обладнання, на якому може здійснюватися втручання у приватне спілкування, а саме:

• номер абонента в телефонній мережі загального користування у форматі: код країни – код зони або оператора – номер абонента в мережі;

• міжнародний ідентифікаційний номер мобільного терміналу (IMEI);

• міжнародний ідентифікаційний номер мобільного абонента (IMSI)[361].

---

[360] Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. Відомості Верховної Ради України. 1992. № 22. Ст. 303.

[361] Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків: Право, 2012. С. 389.

Закон України «Про оперативно-розшукову діяльність», надаючи право оперативним підрозділам вживати заходів зі зняття інформації з каналів зв'язку, не містить норм, що розкривають сутність проваджуваних ними дій. Водночас у п. 3 постанови Пленуму Верховного Суду України № 2 від 28.03.2008 р. *«Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства»* зазначається, що зняття інформації з каналів зв'язку полягає у застосуванні технічного обладнання, яке дає змогу прослуховувати, фіксувати та відтворювати інформацію, що передавалася цим каналом зв'язку. Така інформація може містити дані як про взаємоз'єднання телекомунікаційних мереж, так і щодо змісту інформації, яка була передана каналом зв'язку. Іншими словами, відповідно до наданого роз'яснення отримання уповноваженими оперативними підрозділами інформації про з'єднання абонентів телекомунікацій навіть без розкриття змісту повідомлень, згідно зі змістом Закону України «Про оперативно-розшукову діяльність», може здійснюватись лише за рішенням суду[362].

Зняття інформації з транспортних телекомунікаційних мереж із метою контролю та фіксації інформації, що передається через Інтернет та іншими мережами передачі даних, може здійснюватись за ідентифікаційними ознаками, аналогічними тим, за якими проводиться контроль за телефонними розмовами. Зняття інформації з каналів зв'язку може здійснюватись за такими ознаками:

• за адресою електронної пошти у форматі «ім'я поштової скриньки @ домен.домен верхнього рівня» (як-от info@ssu.gov.ua);

[362] Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства: постанова Пленуму Верховного Суду України 28.03.2008 № 2. URL: http://www.yurincom.com/ua/legal_practice/?id=5096.

• адресою в мережі передачі даних із комутацією пакетів, зокрема IP-адреси для мережі Інтернет у форматі ххх.ххх.ххх.ххх (скажімо, 010.011.012.130);

• апаратною адресою (MAC-адреса) пристрою, приєднаного до мережного середовища[363].

За результатами зняття інформації з транспортних телекомунікаційних мереж може бути зафіксована інформація, що вказує на ознаки кримінального правопорушення в діях підозрюваного, обвинуваченого, а також відомості про протиправну діяльність окремих осіб, що контактували із цими особами через канали телекомунікаційної мережі у проміжок проведення ОТЗ.

За результатами проведення зняття інформації з транспортних телекомунікаційних мереж складається протокол, у якому зазначаються: місце і час проведення цього ОТЗ, правові підстави здійснення, описуються отримані результати або розшифровуються окремі епізоди звукозапису розмов, що містять інформацію, яка має значення для ОРД і кримінального провадження.

Зняття інформації з транспортних телекомунікаційних мереж покладається на уповноважені підрозділи органів Національної поліції, НАБУ, ДБР та органів безпеки. Керівники та працівники операторів телекомунікаційного зв'язку зобов'язані сприяти виконанню дій зі зняття інформації з транспортних телекомунікаційних мереж, уживати необхідних заходів щодо нерозголошення факту проведення таких дій та отриманої інформації, зберігати її в незмінному вигляді[364].

Частина 1 ст. 9 Закону України «Про телекомунікації» вказує, що охорона таємниці телефонних розмов, телеграфної чи іншої кореспонденції, що передаються технічними засобами

---

[363] Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків: Право, 2012. С. 389.

[364] Кримінальний процесуальний кодекс України. URL: https://zakonrada.gov.ua/laws/main/4651-17

телекомунікацій, та інформаційна безпека телекомунікаційних мереж гарантуються Конституцією та законами України[365]. Ураховуючи викладене, КПК покладає на керівників і працівників операторів телекомунікаційного зв'язку обов'язок сприяти виконанню дій зі зняття інформації з транспортних телекомунікаційних мереж, уживати необхідних заходів щодо нерозголошення факту проведення таких дій та змісту отриманої інформації, а також, із метою забезпечення подальшого використання у кримінальному судочинстві, зберігати отриману інформацію в незмінному вигляді.

Вищий спеціалізований суд України у своєму роз'ясненні від 29.01.2013 р. № 223-158/3/4-13[366] звертає увагу слідчих суддів на те, що у КПК передбачено декілька процесуальних дій, які мають певну схожість. Зокрема, статтями 263 та 268 КПК передбачено такі НСРД, як зняття інформації з транспортних телекомунікаційних мереж та установлення місцезнаходження радіоелектронного засобу відповідно, а ст. 159 та п. 7 ч. 1 ст. 162 КПК – такий захід забезпечення кримінального провадження, як тимчасовий доступ до документів, які знаходяться в операторів і провайдерів телекомунікацій та містять інформацію про зв'язок, абонента, надання телекомунікаційних послуг, зокрема отримання послуг, їх тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо).

Дозвіл на проведення НСРД, передбачених статтями 263 та 268 КПК, надає слідчий суддя суду апеляційної інстанції, дозвіл на вжиття дій, передбачених ст. 159 та п. 7 ч. 1 ст. 162 КПК, надає слідчий суддя суду першої інстанції.

Крім того, тимчасовий доступ надається до документів, які містять інформацію про зв'язок, абонента, надання телеко-

[365] Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

[366] Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні: рекомендаційні роз'яснення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ № 223-158/3/4-13 від 29.01.2013. Київ: ВВСУ, 2013. 12 с.

мунікаційних послуг (отримання послуг, їхню тривалість, зміст (вихідні чи вхідні з'єднання, SMS, MMS тощо), маршрути передавання тощо) і не дають змоги втрутитися у приватне спілкування (отримати доступ до змісту інформації, яка передається). Статтями 159, 162 КПК передбачено отримання інформації про зв'язок (зокрема про місцезнаходження радіоелектронного засобу), що відбувся в минулому (постфактум), на той час як установлення місцезнаходження радіоелектронного засобу передбачає локалізацію (моніторинг) місцезнаходження радіоелектронного засобу в режимі реального часу (тобто інформацію про те, де перебуває відповідний засіб на момент спостереження за ним)[367].

Для встановлення особи, яка користується терміналом мобільного зв'язку, що становить оперативний інтерес, визначається його точне місцезнаходження за допомогою пеленгування; використання комп'ютерів компанії, яка надає послуги мобільного зв'язку; з допомогою аналізу даних про сеанси зв'язку абонента з різними базовими станціями.

Метою зазначених заходів є встановлення орієнтовного місцезнаходження особи, яка користується терміналом, шляхів підходу та відходу з місця події причетних до злочину осіб, напрямок їх руху. У разі наявності вихідних дзвінків із викраденого чи власного терміналу після вчинення злочину встановлюються зв'язки особи.

За інформацією Scientific Reports, учені можуть ідентифікувати особу навіть за обмеженою інформацією щодо переміщення мобільного телефону. Аналіз даних дослідження про переміщення 1,5 млн мобільних телефонів упродовж 15 місяців засвідчив, що для унікального визначення одного користувача

[367] Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні: рекомендаційні роз'яснення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ № 223-158/3/4-13 від 29.01.2013. Київ: ВВСУ, 2013. 12 с.

мережі достатньо знати чотири місця, в яких він з'являється в конкретний час доби. Зазначений критерій дозволив дослідникам успішно впізнати 95 % осіб із загальної вибірки[368].

З метою автоматизації аналізу інформації, отриманої за наслідками моніторингу місця скоєння злочину, використовується спеціалізоване програмне забезпечення, зокрема програмні продукти, розроблені компаніями i2 Limited, Visual Analytics і Xanalys. Так, Analyst's Notebook – програмний продукт компанії i2 Limited, призначений для аналізу системи взаємопов'язаних об'єктів і динаміки послідовних подій. Об'єкти на діаграмі можуть бути подані не тільки як піктограми, але й у вигляді фотографій, файлів, аудіо-, відеозаписів тощо.

Водночас однією із актуальних проблем є те, що оператори мобільного зв'язку не вважають своїми обов'язками питання із налагодження тісного співробітництва з оперативними підрозділами Національної поліції, не завжди повною мірою розкривають усі наявні можливості технічного обладнання для розкриття злочинів.

Сучасні GPS-технології можуть допомогти виконати пошук телефону через супутник. Здійснює це супутникова система, що працює через спеціальну програму стеження (/gps/programma-slezhenija-za-telefonom) на телефонах фірми Nokia, iPhone, HTC і на різних операційних системах, як-от Android. Якщо система стеження використовується для спостереження за людьми, то у об'єкта спостереження з собою завжди має бути спеціальний пристрій – персональний GPS-трекер або мобільний телефон фірми Nokia, iPhone, HTC із підтримкою функції GPS або на системі Android. Отож, цей мобільний телефон перетвориться на своєрідний «маячок» зі встановленою на ньому спеціальною програмою спостереження. Якщо використ-

[368] Ученые идентифицировали людей по перемещению их телефонов. URL: http://lenta.ru/news/2013/03/27/mobility/.

товувати програму стеження для спостереження за людьми, то мобільний телефон легко можна покласти в портфель або кишеню об'єкта, а якщо необхідно GPS-стеження за автомобілем, мобільний телефон можна покласти в бардачок. Після визначення програмою стеження точних координат, місцезнаходження та швидкості інформація надсилається на сервер системи зі заздалегідь заданою періодичністю.

Професійний засіб для прослуховування, яким є програма ShadowGuard, дозволяє не тільки стежити за інформацією на іншому телефоні, але і управляти деякими функціями – приміром, блокувати вхідні і вихідні повідомлення та дзвінки[369].

Як повідомило турецьке видання Sabah, годинник Apple Watch, який був на руці саудівського журналіста Джамаля Хашкаджі, записав момент його вбивства 2 жовтня 2018 р. у консульстві Саудівської Аравії в Стамбулі[370].

Аудіозаписи, які Apple Watch здійснили за спілкування журналіста в консульстві, були автоматично передані на смартфон, який Хашкаджі залишив своїй нареченій Х. Дженгіз біля входу в консульство, а пізніше збережені в його акаунті в хмарному сховищі Apple iCloud.

Водночас повідомляється, що, виявивши після смерті Хашкаджі, що Apple Watch вели диктофонний запис, особи, які розмовляли з журналістом, спробували розблокувати годинник за допомогою пароля. Згодом їм це вдалося за допомогою відбитка пальця Хашкаджі. Саудівська розвідка нібито змогла видалити деякі файли, але не всі – частина з них уже була збережена на iCloud[371].

---

[369] Развитие технологий слежения за сотовыми абонентами. URL: https://www.spycry.com/Razvitie-tehnologij-slezheniya-za-sotovymi-abonentami.html

[370] Вбивство саудівського журналіста записав його годинник Apple Watch – ЗМІ. URL: https://www.pravda.com.ua/new/2018/10/14/7195128/

[371] Там само.

## 2.6. Здійснення оперативно-розшукових заходів і негласних слідчих (розшукових) дій у мережі Інтернет

Відкриті джерела інформації вважаються найбільш обсяжними і затребуваними інформаційними каналами[372].

За результатами експертних оцінок, розвідувальні служби з відкритих джерел добувають від 35 % до 95 % розвіданих. Ще в 1947 році відомий аналітик ЦРУ Шерман Кент, якого в США вважають засновником «аналітичної розвідки», стверджував, що в мирний час до 80 % інформації, необхідної для прийняття рішення, доступні саме з відкритих джерел. Щоб довести свою точку зору, Ш. Кент запропонував п'яти професорам Єльського університету підготувати звіт про стан збройних сил США, чисельність бойових частин і з'єднань не нижче рівня дивізії, потужності військово-морського флоту і бойової авіації (з описами кораблів і літаків), використовуючи лише відкриті джерела інформації. За результатами проведеної роботи науковці представили Ш. Кенту так званий «Єльський звіт» на 30 сторінках і кілька сотень сторінок додатків. При цьому, за оцінкою Ш. Кента, представлений звіт на 90 % відповідав дійсному стану військ[373].

Пізніше колишній керівник розвідувального управління Міністерства оборони США С. Уілсон зазначив, що до 90 % розвідувальних даних беруться з відкритих і порівняно відкритих

---

[372] Минин А. Я. Разведка и ее использование против организованной преступности и коррупции в США: учебное пособие / А. Я. Минин, В. И. Попов, В. И. Козлов, В. П. Кувалдин. Москва: МИ МВД России, 2000. 37 с.; Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского, В. С. Овчинского. Москва: ИНФА, 2000. 367 с.; Плэтт В. Стратегическая разведка. Основные принципы. Москва: Форум, 1997. 376 с.; Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учеб. пособие. Москва: Щит-М, 2009. 464 с.

[373] Doronin A. I. Business Intelligence. M.: Os-89, 2003. 384 p. URL: http://www.fb2book.com/ ?kniga=6313&strn=1&cht=1(in Russian).

джерел. І тільки 10 % – за рахунок роботи інших видів розвідки[374].

Останнім часом значного впливу на суспільне життя в нашій країні набули глобальні інформаційні мережі (найперше – мережа Інтернет), які отримали в науковій літературі назву «кіберпростір» (ciberspase)[375].

Окремі аспекти вжиття оперативно-розшукових заходів і негласних слідчих (розшукових) дій у кіберпросторі розглядалися в наукових працях В. В. Агеєва[376], О. Ю. Бусол[377], І. О. Воронова[378], В. О. Голубєва[379], Є. В. Дем'янчук[380],

---

[374] Нежданов И. Ю. Конкурентная разведка в России. Нежданов Игорь Юрьевич – частный взгляд на проблему. URL: http://analitirus.blogspot.com.

[375] Див.: Шеломенцев В. П. Особливості пошуку фактичних даних про злочини у кіберпросторі засобами оперативно-розшукової діяльності. Шляхи розвитку оперативно-розшукової діяльності в сучасних умовах: матеріали наук.-практ. конф. (м. Харків, 28 листоп. 2009 р.). Харків: ХНУВС, 2009. 272 с.; Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і безпека.* Харків, 2009. № 4(31). URL: http://www.nbuv.gov.ua/portal/Soc_ Gum/pib/2009_4/PB.../PB-4_48pdf.

[376] Агеев В. В., Агеева Е. В. К вопросу о поиске оперативно-розыскной информации в Интернете. Криминологический журнал ОГУЭП. Москва, 2011. № 1 (15). С. 65–70.

[377] Бусол О. Ю. Організація аналітичної розвідки як спеціальний суб'єкт оперативно-розшукового прогнозування: автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 21.07.04. Київ, 2009. 20 с.

[378] Воронов И. А. Теоретические основы использования информационных и поисковых систем глобальной сети Интернет в оперативно-розыскной деятельности. *Вісник ЛДУВС ім. Е. О. Дідоренка.* Луганськ, 2009. № 1. С. 194–203.

[379] Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями: монография. Запорожье: ГУ «ЗИГМУ», 2003. 336 с.

[380] Див.: Демянчук Е. В. Интернет как объект оперативно-розыскной деятельности. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (25–26 мая 2004 г., г. Москва). Москва: Акад. упр. МВД России, 2004. С. 214–216; Демянчук Е. В. Мониторинг сети Интернет как мероприятие, проводимое с целью получения оперативно значимой информации. Спеціальна техніка у правоохоронній діяльності: матер. ІІ міжнар. науково-прак. конф. (22 травня 2005 р., м. Київ). Київ: КНУВС, 2006. С. 171–178; Демян-

А. І. Дороніна[381], О. В. Манжая[382], І. Ю. Нежданова[383], А. С. Овчинського[384], В. С. Овчинського[385], С. С. Овчинського[386], Ю. Ю. Орлова[387], А. Л. Осипенка[388], М. М. Перепелиці[389],

чук Е. В. Оперативно-розыскные мероприятия и методы по выявлению и пресечению пропаганды идей терроризма и экстремизма в сети Интернет. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (25–26 мая 2004 г., г. Москва). Москва: Акад. упр. МВД России, 2004. С. 189–192.

[381] Доронин А. Аналитическая разведка средствами Интернет. URL: http://www.agentura.ru/dossier/russia/people/doronin/internet/.

[382] Здійснення оперативно-розшукових заходів шляхом використання кіберпростору: навч.-практ. посіб. / М. М. Перепелиця, О. В. Манжай, В. В. Шендрик. Київ: ДП «Друкарня МВС України», 2010. 146 с.

[383] Нежданов И. Ю. Конкурентная разведка в России. Нежданов Игорь Юрьевич – частный взгляд на проблему. URL: http://analitirus.blogspot.com.

[384] Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского, В. С. Овчинского. Москва: Инфра-М, 2000. 367 с.

[385] Див.: Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского, В. С. Овчинского. Москва: Инфра-М, 2000. 367 с.; Оперативно-розыскная деятельность: учеб. / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова, А. Ю. Шумилова. 2-е изд., доп. и перераб. Москва: ИНФРА-М, 2004. 848 с.

[386] Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского, В. С. Овчинского. Москва: Инфра-М, 2000. 367 с.

[387] Орлов Ю. Ю. Застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теорія і практика): монографія. Київ: Київський нац. ун-т внутрішніх справ, 2007. 559 с.

[388] Див.: Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Изд-воОмск. акад. МВД России, 2009. 480 с.; Осипенко А. Л. Борьба с преступностью в глобальних компьютерных сетях: международный опыт: монография. Москва: Норма, 2004. 432 с.; Осипенко А. Л. Осуществление оперативно-розыскных мероприятий при раскрытии сетевых компьютерных преступлений. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (25-26 мая 2004 г., г. Москва). Москва: Акад. упр. МВД России, 2009. С. 204–209.

[389] Перепелиця М. М. Здійснення оперативно-розшукових заходів шляхом використання кіберпростору: навч.-практ. посіб. / М. М. Перепелиця, О. В. Манжай, В. В. Шендрик. Київ: ДП «Друкарня МВС України», 2010. 146 с.

М. А. Погорецького[390], В. П. Шеломенцева[391], В. В. Шендрика[392], І. Ф. Хараберюша[393], Є. М. Яковця[394] та ін.

Інтернет (від англ. Internet) – це всесвітня система взаємоз'єднаних комп'ютерних мереж, що ґрунтується на комплекті Інтернет-протоколів. Інтернет становить фізичну основу для розміщення величезної кількості інформаційних ресурсів і послуг, таких як взаємопов'язані гіпертекстові документи Всесвітньої павутини (World Wide Web – www) та електронна пошта[395].

У Великому тлумачному словнику сучасної української мови термін «Інтернет» пояснюється як Усесвітня асоціація комп'ютерних мереж, інтегрована мережна павутина, яка скла-

---

[390] Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. Інформаційна безпека людини, суспільства, держави. Київ, 2009. № 2. С. 77–81.

[391] Див.: Шеломенцев В. П. Особливості пошуку фактичних даних про злочини у кіберпросторі засобами оперативно-розшукової діяльності. Шляхи розвитку оперативно-розшукової діяльності в сучасних умовах: матеріали наук.-практ. конф. (м. Харків, 28 листоп. 2009 р.). Харків: ХНУВС, 2009. 272 с.; Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття. Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю, 2009. № 21. URL: http://www.nbuv.gov.ua/portal/Soc_Gum/bozk/21text/g21_09.htm; Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави.* Київ, 2009. № 2. С. 77–81.

[392] Здійснення оперативно-розшукових заходів шляхом використання кіберпростору: навч.-практ. посіб. / М. М. Перепелиця, О. В. Манжай, В. В. Шендрик. Київ: ДП «Друкарня МВС України», 2010. 146 с.

[393] Див.: Хараберюш І. Ф. Використання спеціальної техніки щодо протидії злочинності в Україні: теоретичні, правові та організаційні аспекти: монографія. Донецьк, 2011. 234 с.; Хараберюш И. Компьютерная преступность – проблемы противодействия преступности в сфере нових информационных технологий, 2006. URL: http//crème-research.ru.

[394] Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учеб. пособие. Москва: Щит-М, 2009. 464 с.

[395] Інтернет. Матеріал з Вікіпедії – вільної енциклопедії. URL: http://uk.wikipedia.org/wiki/Інтернет.

дається з різних фізичних неоднорідних комунікаційних мереж, об'єднаних в єдину логічну архітектуру[396].

Відповідно до проєкту Закону про електронні комунікації (№ 2264 від 15.10.2019 р.), Інтернет – це глобальна комп'ютерна мережа, що надає різноманітні комунікаційні та інформаційні послуги і складається з менших комп'ютерних мереж, об'єднаних із допомогою стандартизованих комунікаційних протоколів, основним з яких є IP – інтернет-протокол[397].

З розвитком Інтернету пов'язують поширення терміна «кіберпростір» (cyberspace), під яким розуміють штучне електронне середовище існування інформаційних об'єктів у цифровій формі, утворене в результаті функціонування кібернетичних комп'ютерних систем управління та обробки інформації[398].

У Законі України «Про основні засади забезпечення кібербезпеки України» *кіберпростір* визначається як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних[399].

Термін «кіберпростір» є поєднанням слів «кібер» і «простір». Слово «кібер» (від грецького κυβερ) означає *над*. Під прос-

---

[396] Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В. Т. Бусел. Київ, Ірпінь: ВТФ: Перун, 2004. С. 402.

[397] Проєкт Закону про електронні комунікації (№ 2264 від 15.10.2019). URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=67082

[398] Див.: Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття. Боротьба з організованою злочинністю і корупцією (теорія і практика). Київ: Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю, 2009. № 21. С. 316; Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави.* Київ, 2009. № 2. С. 80.

[399] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

тором розуміють необмежену протяжність; вільний великий простір, просторінь[400]. Проте події у кіберпросторі відбуваються не на фізичних ділянках місцевості, а у певному специфічному середовищі. Дослідники вбачають, що кіберпростір доцільно розглядати саме як «кібернетичний простір», що створений на основі принципів і методів кібернетики[401].

Так, термін «кіберпростір» часто вживають як синонім слова «Інтернет»[402]. Утім, на думку М. А. Погорецького та М. П. Шеломенцева, з якою ми погоджуємося, кіберпростір у найбільш повному розумінні реалізується на основі регіональних і глобальних комп'ютерних мереж (насамперед, це Інтернет), на основі локальних інформаційних мереж можна говорити лише про реалізацію окремих сегментів кіберпростору, а в автономному комп'ютері відсутня така ознака кіберпростору, як інформаційна взаємодія між користувачами в режимі реального часу[403].

Дослідники розглядають кіберпростір як певне середовище: 1) організоване за допомогою принципів, методів і засобів кібернетики; 2) утворене в результаті функціонування кібернетичних комп'ютерних систем управління та обробки інформації[404].

Згідно зі звітом Організації Об'єднаних Націй, 4,1 млрд людей у світі підключені до Інтернету. За даними Міжнародного союзу електрозв'язку при ООН, кількість користувачів

---

[400] Великий тлумачний словник сучасної українськоїмови / упоряд. і голов. ред. В. Т. Бусел. Київ, Ірпінь: ВТФ: Перун, 2004. С. 989.

[401] Див.: Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В. Т. Бусел. Київ, Ірпінь: ВТФ: Перун, 2004. С. 427; Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. Інформаційна безпека людини, суспільства, держави. Київ, 2009. № 2. С. 78.

[402] Черняк Л. Internet и кибернетика. URL: http://www.icfcst.kiev.uamuseumEP/cibernetic_r.html.

[403] Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави.* Київ: Національна академія СБ України, 2009. № 2(2). С. 80.

[404] Там само. С. 78.

Інтернету зросла з 25,8 % населення Землі у 2009 році до 53,6 % у 2019-му. Найвищий відсоток користувачів світової павутини в Європі (82,5 %), а найнижчий – в Африці (28,2 %). Без Інтернету залишається близько 3,6 млрд людей. Більшість із них мешкають у найменш розвинутих країнах. Серед жінок Інтернетом користуються 48 %, серед чоловіків – 58 %[405].

Частка людей, які мають доступ до мережі Інтернет серед дорослого населення України, становить 58 %, а це більше 25,6 млн користувачів. Відповідно до даних реєстру Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, на території України працює понад 7 тис. інтернет-провайдерів[406].

Водночас слід зазначити, що користувачами Інтернету є не лише законослухняні громадяни, а й особи, що мають злочинні наміри. Кримінальні структури активно використовують Інтернет для спілкування між собою, поширення своїх злочинних ідей (зоерема терористичних і екстремістських) серед населення, для пошуку, збору і передавання кримінальної інформації[407].

У сучасних умовах кіберпростір також широко використовується злочинцями як місце вчинення протиправних діянь і містить сліди їхньої злочинної діяльності. Необхідність посилення боротьби зі злочинністю у кіберпросторі вимагає від правоохоронних органів розробки та впровадження в практичну діяльність нових оперативно-розшукових заходів

[405] ООН: 4,1 мільярда людей у світі підключені до інтернету. URL: https://www.radiosvoboda.org/a/news-oon-internet/30254946.html

[406] Реєстр операторів, провайдерів телекомунікацій станом на 27.08.2019. URL: https://nkrzi.gov.ua/index.php?r= site/index&pg=55&language=uk

[407] Див.: Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями: моногр. Запорожье: ГУ «ЗИГМУ», 2003. 336 с.; Компьютерная преступность и кибертерроризм: сборник научных статей / под ред. Голубева В. А., Рыжкова Э. В. Запорожье: Центр исследования компьютерной преступности, 2005. Вып. 3. 448 с.; Осипенко А. Л. Сетевая компьютернаяпреступность: теория и практика борьбы: моногр. Омск: Изд-воОмск. акад. МВД России, 2009. 480 с.

і методів, які б ураховували специфіку функціонування кіберпростору.

Кіберзлочинність в Україні сьогодні є однією з найбільших загроз національній безпеці в інформаційній сфері. Кіберпростір використовується для незаконної торгівлі людьми, наркотичними засобами, зброєю, розповсюдження дитячої порнографії, проведення різної екстремістської діяльності (зокрема пропаганди насильства, жорстокості, расової, національної, релігійної нетерпимості), порушення авторських прав тощо.

Кількість злочинів, що вчиняється у кіберпросторі, зростає пропорційно кількості користувачів комп'ютерних мереж. За оцінками Інтерполу, швидкість зростання злочинності в глобальній мережі Інтернет є найбільшою порівняно з іншими видами злочинів, зокрема торгівлею наркотиками та зброєю. У сучасних умовах кіберзлочинність уже ввійшла до переліку найбільш серйозних загроз із тих, з якими доводиться стикатися поліції[408].

У липні 2019 року Департамент кіберполіції Національної поліції України відзначив свій перший ювілей – 10 років боротьби з кіберзлочинністю. Упродовж цього часу кіберполіції вдалося провести більше 70 міжнародних спецоперацій та викрити більше 45 тисяч злочинів.

Утім, ці показники не відображають реальну кількість кіберзлочинів, що характеризуються високою латентністю, використанням новітніх технологій, сучасним апаратним і програмним забезпеченням; організованістю, міжрегіональними та міжнародними зв'язками; використаням інформаційних ресурсів, які територіально розташовані у різних країнах[409].

---

[408] Зима Л. М. Протидія кіберзлочинності у банківській сфері: стан, проблеми та шляхи їх вирішення. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж: тези доповідей Міжнарод. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.). Суми: ДВНЗ «УАБС НБУ», 2010. С. 74–75.

[409] Там само. С. 77.

З-поміж усіх спецоперацій кіберполіції слід відзначити найбільш резонансні: припинення діяльності піратських онлайн-ресурсів fs.to та ex.ua, викриття шахрайської фінансової біржі «trade12», закриття злочинної бот-мережі АВАЛАНШ, затримання злочинців за розбещення неповнолітніх і поширення ними відповідного контенту в закритій мережі Інтернет, ліквідація найбільшого у даркнеті майданчику з продажу персональних даних – xDedic тощо[410].

Подальшій криміналізації кіберпростору сприяє низка характерних особливостей «віртуального» середовища:

1) *транснаціональність Інтернету* (відсутність кордонів, митниць, територіальна роз'єднаність груп людей);

2) *уявна анонімність користувачів* (як імена у мережі Інтернет використовуються псевдоніми (ніки));

3) *наявність значної кількості користувачів*, до яких легко можна довести свої ідеї, організувати їх для проведення якої-небудь акції, формувати громадську думку, навмисно дезінформувати, збирати інформацію);

4) *законодавча неврегульованість* такого середовища[411].

Злочинні групи, що формуються у кіберпросторі, характеризуються особливими формами організації (мережна структура, наявність міжнародних зв'язків, відсутність прямих контактів між учасниками тощо) та управління з використанням закритих комунікаційних каналів. У таких групах, зазвичай, немає лідера, учасники особисто не знайомі, а координація діяльності здійснюється з використанням мережних технологій. Після досягнення злочинної мети такі групи можуть швидко розпадатися або помітно перебудовуватися[412].

---

[410] Кіберполіція відзначає свій перший ювілей: 10 років боротьби з кіберзлочинністю. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vidznachaje-svij-pershij-yuvilej-10-rokiv-borotbi-z-kiberzlochinnis/

[411] Демянчук Е. В. Борьба с преступлениями экстремистской и террористической направленности, совершаемые с использованием сети «Интернет». Научный портал МВД России. Москва, 2009. № 1. С. 99–100.

[412] Осипенко А. Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы. *Научный вестник Омской академии МВД России.* Омск, 2010. № 2 (37). С. 39.

У сучасних умовах глобальної інформатизації суспільства надзвичайно актуальною стає проблема ідентифікації особи в мережі Інтернет. Чимало інтернет-сайтів для зручності користувачів застосовують систему ідентифікації з допомогою процедур «реєстрація/авторизація». Проблема використання подібного механізму ідентифікації користувача полягає в тому, що інформація про користувача надається лише ним, без процедури верифікації. У більшості випадків користувачі в мережі Інтернет використовують псевдоніми (ніки).

Попри те, потреба суспільства в підвищенні достовірності інформації вимагає розробки механізмів ідентифікації користувачів у мережі. У реальному житті ми легко можемо отримати інформацію про особу, з якою маємо справу: за особистого спілкування ми можемо сформувати уявлення про людину за зовнішнім виглядом, за необхідності ми можемо вимагати чи попросити надати необхідні документи, які містять перевірену інформацію. У мережі Інтернет таких можливостей у більшості випадків немає.

Для здійснення платіжних операцій за допомогою мережі Інтернет можуть використовуватися системи на основі банківських карток, смарт-карток, інтернет-банкінгу або «електронних» грошей. Найбільш популярними платіжними системами, які використовуються в мережі Інтернет, є: Western Union, Money Gram, Hawala, WebMoney, Qiwi, PayPal, Q-Cash тощо.

Є 4 групи відомостей, які найбільш часто зазнають нападів із використанням шкідливих програм:

1) доступ до різних фінансових операцій (онлайн-банкінг, платіжні картки, електронні гроші), інтернет-аукціонів тощо;

2) доступ до поштових скриньок, які є частиною ICQ-аккаунтів, як і всі знайдені на комп'ютері адреси електронної пошти;

3) паролі, коди доступу до інтернет-пейджерів, сайтів тощо;

4) паролі, коди до онлайн-ігр[413].

[413] Яппаров Р. М. Информационные технологии и компьютерные преступления в сети Интернет. Информационные технологии, связь и защита информации МВД России. Москва: ВНИИ МВД России, 2012.

Віднедавна спостерігається тенденція до збільшення шахрайських дій у мережі Інтернет, зокрема отримання персональної інформації (паролів, банківських рахунків або дампів із інформацією про власників кредитних карт тощо), шляхом розсилки електронних листів від імені банку, які містять посилання на підроблені сайти, що імітують роботу справжніх, – так званого «фішингу». Цьому сприяло стрімке поширення інтернет-аукціонів, «фінансових пірамід», використання небанківських електронно-платіжних систем.

Причому ці сайти схожі на справжні. Зазвичай такий сайт пропонує зареєструватися для здійснення покупок. За реєстрації необхідно ввести свої дані, а саме – номер та інші реквізити банківської картки (крім коду), з якої в майбутньому планується здійснювати покупки.

Але під сайтом такої інтернет-крамниці маскуються шахраї, тому покупки на ньому не буде. Натомість надійде повідомлення, що транзакція неможлива за певних причин (їх шахраї придумають безліч). Іноді пропонують спробувати використати іншу картку, дані якої теж потрапляють до шахраїв. Після цього у зловмисників є вся інформація щодо картки, зокрема секретний код, і шахраї зразу ж за рахунок жертви купують реальний товар, який потім можна реалізувати.

Крім того, фішингові сайти використовують для того, щоби заволодіти акаунтами жертви, оскільки чимало людей за реєстрації на різних сайтах використовують одні і ті ж логіни та паролі. У подальшому шахраї входять у систему під іменем жертви.

Фішингом є також випадки, коли користувачу від імені банку, де він обслуговується, надходить повідомлення про зміну певних правил і необхідність увійти в свої банківські налаштування для внесення змін. Після цього дається посилання на нібито банківський, а насправді фішинговий сайт. Шахраї сподіваються на те, що користувач зазвичай перейде за цим посиланням і на фальшивому сайті банку вводить свій пароль і логін. Подібний вид шахрайства наразі часто застосовується щодо власників смартфонів для отримання їх ID і доступу потім до

інформації на цьому телефоні (акаунти, документи, база номерів тощо). Знову йдеться про внесення певних змін у налаштування, для чого надсилається посилання, де це необхідно здійснити[414].

Нова система боротьби з комп'ютерним шахрайством на основі обсяжних даних була розроблена в компанії Visa. На відміну від попередніх систем вона враховувала до 500 особливостей кожної транзакції і аналізувала те, що відбувається з точністю до окремих банкоматів. За рік система зупиняє шахрайські платежі на суму близько 2 млрд доларів США[415].

Один із великих американських банків підключив до боротьби з шахраями суперкомп'ютер Watson, розроблений в IBM. Система IBM, яка використовує елементи Watson, аналізує потік транзакцій в реальному часі, оцінюючи підозрілість кожної з них. На оцінку, крім іншого, впливає історія відносин банку з торговою точкою, яка ініціювала угоду. Чим більше шахрайських транзакцій в її послужному списку, тим менше до неї довіри. У IBM стверджують, що система на 15 % збільшила кількість виявлених шахрайських звернень до банку і на 50 % зменшила кількість помилкових спрацьовувань. А сума, яку вдалося захистити від шахраїв, зросла на 60 %[416].

У 2017 році американські правоохоронці, зокрема ФБР і поліція, запропонували нову класифікацію інтернет-злочинності, а саме:

1) платіжне шахрайство. Це поширений в США вид злочинності, коли злочинні групи (головно африканські й азіатські) розсилають листи, в яких пропонують кореспондентам значні суми грошей. Як умова виплати цих грошей передбачається здійснення попередніх платежів, пов'язаних із оплатою юридичних та інших послуг для здійснення платежу;

---

[414] Реформа полиции в Америке времён Трампа. URL: http://zavtra.ru/blogs/reforma_politcii_v_amerike_vremyon_trampa

[415] «Большие данные» против мошенников. URL: https://www.compu terra.ru/183255/fraud-bigdata/

[416] Там само.

2) попередній внесок. Дедалі частіше злочинці посилають електронні листи, в яких указують, що одержувач кваліфікований фінансовою компанією на отримання пільгового великого кредиту або виграв значну фінансову премію;

3) соціальна інженерія як підкріплення електронного шахрайства. Цей тип шахрайства використовується проти юридичних осіб, які мають широке коло контрагентів;

4) благодійність як злочин. Злочинці дедалі частіше створюють фіктивні благодійні організації. Зазвичай після серйозних стихійних катаклізмів;

5) шахрайство на довірі. Нещодавно в США різко поширилося шахрайство на довірі. Якщо раніше це відбувалося тільки через електронну пошту, то з середини «нульових» років дедалі активніше використовуються соціальні мережі;

6) витік корпоративних даних. У більшості випадків хакери добувають корпоративні дані за допомогою методів соціального інжинірингу;

7) карткове шахрайство. Серед усіх видів інтернет-злочинності, спрямованих проти населення, найбільшої шкоди в 2016-2017 рр. заподіяло карткове інтернет-шахрайство. Загальні втрати населення США від цього виду шахрайства за два роки становили понад 1,1 млрд доларів;

8) інтернет-злочинність проти дітей, до якого входять будь-які види кіберзлочинності, об'єктом яких є діти[417].

У сучасних умовах використання мережі Інтернет оперативними та слідчими підрозділами правоохоронних органів є необхідною умовою успіху у сфері боротьби зі злочинністю. Також слід відрізняти організацію боротьби з кіберзлочинами та організацію здійснення ОРЗ та НСРД шляхом використання кіберпростору, адже останні можуть проводитись як у справах про кіберзлочини, так і у справах про злочини, вчинені у звичайному середовищі.

Так, слід зазначити, що роль оперативних і слідчих підрозділів у попередженні та розкритті злочинів шляхом викори-

[417] Реформа полиции в Америке времён Трампа. URL: http://zavtra.ru/blogs/reforma_politcii_v_amerike_vremyon_trampa

стання кіберпростору сьогодні не можна назвати достатньою. Здебільшого це пояснюється браком відповідних спеціалістів в оперативних і слідчих підрозділах Національної поліції, які б одночасно мали професійні знання комп'ютерних технологій та навички оперативної роботи.

Зважаючи на викладене, можна окреслити *основні напрями використання мережі Інтернет:*

1) виявлення осіб, які становлять оперативний інтерес;

2) пошук конкретних осіб, установлення їх фізичного місцезнаходження;

3) налагодження негласних зв'язків із подальшим уходженням у безпосередній контакт;

4) пошук викрадених речей та встановлення причетних до цього осіб;

5) здійснення психологічного впливу на учасників кримінальних структур шляхом ведення активної роботи на форумах і чатах[418].

Попри це, є низка проблем, пов'язаних із використанням інформації в мережі Інтернет:

– зареєстровані непоодинокі випадки, коли соціальні мережі сприяють учиненню злочинів (наприклад, особа повідомляє в мережі, що поїхала у відпустку, і в цей час її житло грабують)[419];

– соціальні мережі несуть певну загрозу ще й тому, що злочинці також спілкуються через них, створюють закриті групи;

– у мережі міститься багато недостовірної інформації. У зв'язку з цим дані, отримані з Інтернету, необхідно зіставляти та перевіряти з використанням оперативних обліків та інших джерел інформації.

---

[418] Воронов И. А. Теоретические основы использования информационных и поисковых систем глобальной сети Интернет в оперативно-розыскной деятельности. *Вісник ЛДУВС ім. Е. О. Дідоренка.* Луганськ, 2009. № 1. С. 200.

[419] МВС радить українцям обережніше користуватися соцмережами. *Тиждень*. 12.05.2011. URL: http://tyzhden.ua/News/23957

Викриття злочинця, який активно використовує комп'ютерні засоби в повсякденному житті, зокрема для досягнення злочинних цілей, потребує системного аналізу інформації в інформаційно-телекомунікаційних мережах. Для ефективного пошуку такої інформації залучаються такі ресурси:

• *сервери служби Whois*, які містять інформацію про належність певної IP-адреси до конкретного провайдера[420];

• *електронну пошту (E-mail)*, що забезпечує обмін поштовими повідомленнями з будь-яким абонентом цієї мережі[421];

• *соціальні мережі*, які надають можливість спілкування користувачам зі спорідненими інтересами. Серед соціальних мереж лідером за кількістю користувачів залишається Facebook – 2,2 млрд активних користувачів у місяць, Twitter – 335 млн активних користувачів у місяць[422];

• *блоги* (англ. blog, від «weblog», «мережний журнал або щоденник подій») – веб-сайти, основний зміст яких становлять записи, що є регулярно доповнюваними, зображення або мультимедіа[423];

• *сайти знайомств* – інтернет-сервери, що надають користувачам Інтернету послуги з віртуального спілкування з іншими користувачами[424];

• *веб-форуми* – клас веб-додатків для організації спілкування відвідувачів веб-сайту[425];

•*чати* (англ. chat – розмова) – засіб спілкування користувачів мережі в режимі реального часу[426];

• *сервіси IP-телефонії*, що надають послуги з передавання телефонних розмов абонентів за протоколом IP шляхом засто-

---

420 Whois. URL: http://uk.wikipedia.org/wiki/Whois

421 Електро́нна по́шта. URL: https://uk.wikipedia.org/wiki/

422 Кількість інтернет-користувачів перевищила 2 мільярди: ТСН – Останні новини, 20.01.2012. URL: http://www.unian.net/ukr/print/480748

423 Блог. URL: http://uk.wikipedia.org/wiki/блог

424 Он-лайн_служба_знайомств. URL: http://uk.wikipedia.org/wiki/Он-лайн_служба_знайомств

425 Веб-форум. URL: http://uk.wikipedia.org/wiki/веб-форум.

426 Чат. URL: http://uk.wikipedia.org/wiki/чат

сування інформаційно-телекомунікаційних мереж (одним із найпоширеніших сервісів таких послуг є Skype)[427];

• *сервіс YouTube*, який надає послуги відеохостингу користувачам, які можуть додавати, переглядати і коментувати ті чи інші відеозаписи (аудиторія користувачів YouTube – більше 1 млрд)[428];

• *файло́вий се́рвер* (англ. *file server*) – це виділений сервер, призначений для виконання файлових операцій введення-виведення, який зберігає файли будь-якого типу. Загалом має великий обсяг дискового простору, реалізованого у формі RAID-масиву для забезпечення безперебійної роботи та підвищеної швидкості запису та читання даних. Зараз більшість інформації зберігається не тільки на фізичних серверах, але і на віртуальному сервері[429].

У 2019 році найпопулярнішим браузером для комп'ютерів став Google Chrome. Його частка на ринку становить 59,59 відсотків. Другу сходинку посів Internet Explorer, який отримав частку в 16,84 %. Частка Mozilla Firefox становила 12,2 %, що дозволяє браузеру утримувати третю сходинку підсумкового рейтингу[430].

Моніторинг соціальних сайтів у мережі Інтернет також дає змогу перевірити наявні або зібрати нові відомості про конкретну особу, отримати фотографії різних років її життя, виявити зв'язки (родинні, дружні, комерційні, злочинні) та контакти, встановити місце перебування та роботи. Принцип функціонування таких мереж допускає здійснення безпосереднього контакту з конкретною особою або виявлення її зв'язків з іншими особами. Ця діяльність є новим напрямом здійснення

---

[427] Скайп. URL: http://uk.wikipedia.org/wiki/Скайп

[428] YouTube. URL: http://uk.wikipedia.org/wiki/YouTube

[429] Файловий сервер. URL: https://uk.wikipedia.org/wiki/

[430] Який інтернет-браузер краще. Який вибрати браузер для слабкого комп'ютера. Основні переваги Опера. URL: https://beasthackerz.ru/uk/kompyuter/kakoi-internet-brauzer-luchshe-kakoi-vybrat-brauzer-dlya-slabogo.html

ОРЗ, що потребує розроблення та впровадження відповідної тактики їх проведення.

Залежно від виду ресурсу і його призначення, реквізитами пошуку можуть бути індивідуальний номер абонента, вік, стать, ім'я, прізвище, псевдонім, номер електронної пошти, місто або країна проживання. Доволі часто встановлення навіть факту використання певного ресурсу особою може значно підвищити поінформованість оперативних працівників про обставини злочину, а також сприяти отриманню додаткових відомостей, які сприяють розкриттю злочину, висуненню додаткових версій або створенню легенди в процесі оперативної розробки. Перевірка доменного імені з використанням різних інтернет-сайтів дозволяє встановити, на чиє ім'я і в якій країні зареєстрований сайт[431].

Візитною карткою комерційної організації в Інтернеті є її корпоративний сайт, на якому, зазвичай, розміщена інформація про місцезнаходження посадових осіб і банківські реквізити організації.

Роботу з інформаційними системами, які зберігають значний обсяг інформації, полегшують вбудовані програмні функції пошуку конкретної особи, відбору всіх контактів, груп друзів, установлення періодичності відвідування ресурсів Інтернету. Втім, основний недолік цих програм полягає в тому, що вони втрачають певну кількість корисної інформації, відтак формують неповну картину того, що відбувається. Крім того, ці програми головно призначені для потреб комерційних організацій, а до специфіки завдань, що стоять перед правоохоронними органами, не адаптовані.

На вибір тактики здійснення пошукових заходів у мережі Інтернет впливає:

– необхідність залучення спеціальних познань у галузі інформаційних технологій за проведення ОРЗ;

[431] Агеев В. В., Агеева Е. В. К вопросу о поиске оперативно-розыскной информации в Интернете. *Криминологический журнал ОГУЭП.* Москва, 2011. № 1 (15). С. 65–70.

– існування «інтелектуальної» протидії розкриттю злочинів із боку осіб, які їх учинили;

– значний обсяг даних (в електронній формі), які необхідно опрацювати під час розкриття злочину;

– дефіцит часу і динамічність обстановки[432].

Окремо слід зазначити, що правоохоронним органам, зокрема органам Національної поліції, у сучасних умовах не слід використовувати Інтернет лише як додаткове джерело інформації.

На наш погляд, його можна залучати як спеціальний засіб здійснення психологічного впливу на учасників кримінальних структур шляхом ведення активної роботи на форумах і чатах.

Інноваційною технологією пошуку викрадених речей та встановлення причетних до цього осіб є вивчення пропозицій інтернет-крамниць та аукціонів. Пошук доцільно починати з виявлення регіонального об'єкта збуту. Ще одним етапом є аналіз товарів за категоріями, і, врешті-решт, пошук конкретної марки приладу або речі. У багатьох випадках на відповідних ресурсах розміщуються зображення товару, наводяться його характеристики, за наявності вказуються дефекти, що, по суті, і є пошуковими ознаками. Останній етап передбачає безпосередній контакт із особою, яка розмістила таку інформацію. Деякі інтернет-крамниці обов'язково вимагають вводити паспортні дані та ідентифікаційний код особи, яка пропонує товар на продаж[433].

За допомогою популярних пошукових систем при введенні ключових слів «продаю», «антикваріат», «автотранспорт» є можливість отримати достатню кількість ресурсів, які слід

---

[432] Осипенко А. Л. О некоторых особенностях раскрытия сетевых компьютерных преступлений. Москва: Научный портал МВД России, 2010. № 2. С. 43.

[433] Здійснення оперативно-розшукових заходів шляхом використання кіберпростору: навч.-практ. посіб. / М. М. Перепелиця, О. В. Манжай, В. В. Шендрик. Київ: ДП «Друкарня МВС України», 2010. С. 46.

вивчити з метою виявлення предметів, схожих за описом із викраденими і виставленими на продаж[434].

У випадку, якщо такий ОРЗ обмежує конституційні права громадян, він проводиться тільки на підставі ухвали слідчого судді. У разі підтвердження, наприклад, інформації про те, що на продаж виставлені викрадені культурні цінності, можна здійснювати контроль залишеної продавцем поштової скриньки (за наявності судового рішення)[435].

Слід зазначити, що більшість ОРЗ здійснюється як у звичайному середовищі, так і в кіберпросторі. У сучасних умовах правоохоронні органи використовують Інтернет не лише як додаткове джерело інформації, а також як спеціальний засіб здійснення ОРЗ шляхом використання кіберпростору.

Боротьба зі злочинністю у кіберпросторі неефективна без комплексного застосування оперативно-розшукових сил, засобів, заходів і методів, які мають, насамперед, розвідувально-пошуковий характер, тобто спрямовані на отримання раніше невідомої і ретельно приховуваної від правоохоронних органів інформації про кримінальні події і причетних до них осіб[436].

На наш погляд, найбільш ефективним є спостереження з використанням спеціального обладнання, встановленого на боці провайдера телекомунікацій.

Підсумовуючи викладене, зазначимо:

1) мережа Інтернет є об'єктом ОРД як система суспільних відносин інформаційного суспільства в інформаційному просторі, що містить відомості про злочини та осіб, які їх учинили,

---

[434] Оперативно-розыскная деятельность: учеб. / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова, А. Ю. Шумилова. 2-е изд., доп. и перераб. Москва: ИНФРА-М, 2004. С. 401.

[435] Там само. С. 402.

[436] Осипенко А. Л. Осуществление оперативно-розыскных мероприятий при раскрытии сетевых компьютерных преступлений. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (25–26 мая 2004 г., г. Москва). Москва: Акад. упр. МВД России, 2009. С. 204.

й виявлення яких вимагає здійснення оперативними та слідчими підрозділами оперативно-розшукових заходів і негласних слідчих (розшукових) дій безпосередньо в кіберпросторі;

2) оперативні та слідчі підрозділи використовують мережу Інтернет не лише для пошуку оперативно-розшукової інформації, а й як спеціальний засіб здійснення ОРЗ і НСРД у кіберпросторі;

3) під оперативно-розшуковими заходами та негласними слідчими (розшуковими) діями в мережі Інтернет розуміється комплекс дій, які здійснюються оперативними підрозділами у кіберпросторі з метою пошуку доказів (предметів, обставин тощо), що свідчать про факти вчинення злочинів і вказують на причетних до них осіб.

## 2.7. Особливості викриття фактів збуту наркотиків із використанням мережі Інтернет

Нещодавно набув поширення безконтактний збут наркотичних засобів і психотропних речовин, зокрема, з використанням мережі Інтернет. Найчастіше інтернет-крамниці з продажу наркотиків пропонують свої послуги у Києві, Харкові, Одесі, Дніпрі, Миколаєві, Херсоні[437].

Зокрема, у липні 2019 року працівники Департаменту протидії наркозлочинності Національної поліції викрили злочинну організацію зі збуту синтетичних «дизайнерських» наркотиків через спеціальний інтернет-ресурс. Установлено, що лідером злочинної організації був 37-річний житель Києва, який налагодив прямі поставки в Україну висококонцентрова-

[437] Підрозділи протидії наркозлочинності та кіберполіція співпрацюватимуть для припинення розповсюдження наркотиків через Інтернет. URL: https://www.npu.gov.ua/news/ narkozlochini/kiberpolicziya-ta-pidrozdili-protidiji-narkozlochinnosti-spivpraczyu vatimut-dlya-pripinennya-rozpovsyudzhennya-narkotikiv-cherez-internet/

них нових психоактивних речовин із Китайської Народної Республіки та залучив до співпраці свого родича – фахівця з ІТ-технологій. Останній створив спеціальний сайт для реалізації нових психоактивних речовин і канал у популярному месенджері та забезпечував їхню постійну роботу й адміністрування.

Усі фігуранти дотримувалися жорсткої конспірації, постійно змінювали місця дислокації та зберігання психоактивних речовин. Для спілкування між членами організації використовувалися канали зв'язку з високим ступенем шифрування.

Під час завершального етапу спецоперації затримано 8 членів злочинної організації, проведено 26 обшуків і вилучено майже 100 тис. доз наркотиків і психотропів, кілограм концентрату нових психоактивних речовин, із якого можна виготовити 30 кг психотропних речовин вартістю майже 9 млн гривень. Також вилучено понад 150 тис. доларів США, 12 тис. євро і 350 тис. гривень готівки, здобутої від реалізації наркозасобів, 47 банківських карток, оргтехніку, 2 одиниці зброї, 8 автомобілів[438].

У Миколаєві у вересні 2019 року працівники Управління протидії наркозлочинності ліквідували канал постачання наркотиків і психотропів вартістю понад мільйон гривень. Фігуранти угруповання постачали клієнтам замовлення шляхом закладок, ховаючи їх у горіхах. Самі ж отримували поставки, замасковані під поштову доставку товарів з інтернет-крамниці. За низки обшуків за місцем проживання, в автомобілі та на квартирі-складі правоохоронці вилучили у зловмисників понад кілограм амфетаміну, 150 підготовлених закладок, півтори сотні пігулок екстазі, 77 марок ЛСД, канабіс, солі, біля одного

[438] Поліція викрила злочинну організацію у збуті синтетичних «дизайнерських» наркотиків через спеціальний Інтернет-ресурс. URL: https://www.npu.gov.ua/news/ narkozlochini/policziya-vikrila-zlochinnu-organizacziyu-u-zbuti-sintetichnix-dizajnerskix-narkotikiv-cherez-speczialnij-Internet-resurs/

кілограму прекурсорів, інші наркотичні речовини, а також банківські картки та грошові кошти[439].

У листопаді 2019 року правоохоронці провели масштабну спецоперацію для ліквідації діяльності наркосиндикату, у результаті якої було затримано двох організаторів і 17 учасників злочинної групи. Раніше у цій справі правоохоронці з Республіки Білорусь затримали ще двох учасників злочинної організації.

Для збуту виготовленої продукції, прийому та оплати замовлень зловмисники використовували інтернет-крамницю. Оплата замовлення здійснювалася через цифрову платіжну платформу, електронні гаманці або за допомогою криптовалюти. З метою конспірації гаманці через кілька діб видалялися та створювалися нові.

Для належного контролю, функціонування та безпеки діяльності злочинної організації існувала чітка ієрархія та розподіл ролей: контроль за функціонуванням лабораторій, їх охорона, «хіміки», «фінансисти», обслуговування інтернет-крамниці, доставка продукції до складів зберігання, «кур'єри», «закладчики» тощо. За попередніми підрахунками, лише через інтернет-крамницю було реалізовано наркотичних засобів і психотропних речовин майже на 21 млн гривень.

За результатами проведення майже 100 одночасних санкціонованих обшуків поліцейські вилучили понад 46 кг наркотичних засобів і психотропних речовин, а також 170 літрів прекурсорів вартістю 25 млн гривень. Окрім цього, вилучено 24 тис. доларів США, 1100 євро та 38,6 тис. гривень, більше двох десятків банківських карток і мобільних телефонів, зброю та набої різного калібру, боєприпаси, «чорнові» записи з дани-

[439] У Миколаєві у результаті масштабної реалізації поліцейські ліквідували канал постачання наркотиків та психотропів вартістю понад мільйон гривень. URL: https://www.npu.gov.ua/news/narkozlochini/u-mikolajevi-u-rezultati-masshtabnoji-realizacziji-policzejski-likviduvali-kanal-postachannya-narkotikiv-ta-psixotropiv-vartistyu-ponad-miljon-griven/

ми про «рух» наркотиків, дилерів, «клієнтуру» та боржників, а також 6 автомобілів преміум-класу[440].

Для залучення потенційних покупців для онлайн-продажу наркотиків збувачі використовують спеціалізовані сайти, форуми (чати), сайти оголошень, соціальні мережі, вірусну спам-рекламу, на яких розміщують відомості про реалізацію наркотичних засобів чи психотропних речовин, а також адреси електронної пошти, шифри, умовні терміни, за допомогою яких можна зв'язатись зі збувальником майбутньому покупцю. При цьому відомості про рекламу або пропозицію придбати наркотичні засоби чи психотропні речовини можуть розміщатись як у відкритому, так і в завуальованому виглядах.

Крім того, доволі популярне розміщення на різних об'єктах міської інфраструктури кустарних чи трафаретних надписів із пропозиціями продажу наркотиків (так зване вуличне графіті). Найчастіше можна спостерігати написи «мет», «фен», «амф», «спайси», «бошкі», «солі», «спіди», «бистрий», «скорость», «закладки», «клад», «JWH», «МДМА», адреси інтернет-сайтів, номери популярних месенджерів (Viber, WhatsApp, Telegram, Skype, Jabber) тощо[441].

Приховуючи сліди своєї протиправної діяльності, злочинці використовують спеціальні прийоми, які підміняють інформацію про фактичні адреси їх мережевої активності, а мережеві ресурси створюють на серверах, розташованих в інших країнах. Так, зокрема, використовується TOR-браузер – систему проксі-серверів, що дає змогу встановлювати анонімне мере-

[440] У результаті масштабної спецоперації Нацполіція викрила синдикат наркоторговців: вартість вилучених наркотиків становить 25 мільйонів гривень. URL: https://www.npu.gov.ua/news/narkozlochini/u-rezultati-masshtabnoji-speczoperacziji-naczpolicziya-vikrila-sindikat-narkotorgovcziv-vartist-viluchenix-narkotikiv-stanovit-25-miljoniv-griven/

[441] Національний звіт за 2017 рік щодо наркотичної ситуації в Україні (за даними 2016 року). Поглиблений огляд наркоситуації в Україні для Європейського моніторингового центру з наркотиків та наркотичної залежності / Державна установа «Український моніторинговий та медичний центр з наркотиків та алкоголю Міністерства охорони здоров'я України». 2017. С. 161-164 с.

жеве з'єднання, захищене від прослідковування, а також технологія VPN підключення, яка забезпечує створення в Інтернеті зашифрованої додаткової «чорної» сітки для передачі даних. У випадках використання номерів операторів мобільного зв'язку збувачі систематично змінюють свої контакти з метою уникнення можливої ідентифікації.

Особа, яка хоче придбати наркозасоби за допомогою мережі Інтернет або мобільних месенджерів, зв'язується зі збувачем і здійснює необхідне замовлення. У відповідь отримує від збувача повідомлення з номером банківського рахунку або номер електронного гаманця для онлайн-розрахунку (WebMoney, Qiwi, PayPal, Q-Cash, EasyPay та інші) та проводить оплату. Таке спілкування може здійснюватись різними способами: в режимі онлайн через програми типу ICQ, Skype, Viber, WhatsApp, шляхом інтернет-переписки у форумах (чатах) чи з використанням електронної пошти, соціальних мереж (Facebook, Twitter, Instagram) тощо.

Після підтвердження переведення коштів покупець отримує від збувача повідомлення з адресою розміщення «закладки» та конкретним місцем, де вона прихована (зазвичай повідомлення підтверджується фото).

Інколи для отримання онлайн-замовлення наркотиків злочинці використовують можливості Укрпошти та приватних служб кур'єрської доставки товарів (Нова Пошта, Інтайм, Автолюкс). Після відправлення таких посилок збувач повідомляє покупцю номер декларації.

Віднедавна для повної конспірації та анонімності онлайн-збувачі почали використовувати «ЧАТ-боти», або, іншими словами, віртуальні автоматичні співрозмовники через мобільні інтернет-месенджери, які розповсюджують рекламу наркотиків через повідомлення та мають змогу підтримувати переписку, приймати замовлення та відповідати на запитання.

Під час документування злочинів цієї категорії виникає низка проблемних питань. Основною проблемою є те, що в Україні законодавчо не врегульовано механізм блокування чи

обмеження доступу до інтернет-ресурсів, через які вчиняються кримінальні правопорушення чи де є заборонений контент.

Відповідно до п. 9 ст. 38 Закону України «Про телекомунікації», оператори та провайдери телекомунікацій мають право відключати на підставі рішення суду кінцеве обладнання, якщо воно використовується абонентом для вчинення протиправних або дій, що загрожують інтересам державної безпеки. Однак такий алгоритм дій не є достатньо ефективним, оскільки відсутній єдиний орган, наділений повноваженнями з виконання судових рішень із блокування чи обмеження доступу до протиправних сайтів.

Після встановлення сайту, на якому ймовірно здійснюється реклама щодо розповсюдження наркотичних засобів або через який здійснюється реалізація наркотиків, потрібно з'ясувати, де технічно знаходиться цей сайт і яка компанія надає його власникам послуги хостингу. Зважаючи на те, що, відповідно до даних реєстру Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, на території України працює понад 7 тис. інтернет-провайдерів, можуть виникнути певні проблеми у винесенні судового рішення із вимогою блокування протиправного інтернет-ресурсу[442].

Якщо інтернет-ресурс, із якого здійснювалася реалізація наркотичних засобів, знаходиться за межами України, до компетентних правоохоронних органів іноземних держав, крім ухвали суду, також направляється запит про надання міжнародно-правової допомоги. Ця процедура також не має чіткого механізму і може бути тривалою.

Крім того, в Україні після отримання ухвали суду провайдери телекомунікацій можуть повідомити про відсутність у них технічної можливості із блокування чи обмеження доступу до інтернет-ресурсів. Водночас законодавством не встановлено вимоги щодо обов'язкової наявності такого обладнання у про-

[442] Реєстр операторів, провайдерів телекомунікацій станом на 27.08.2019. URL: https://nkrzi.gov.ua/index.php?r= site/index&pg=55&language=uk

вайдерів. Оператори телекомунікацій зобов'язані лише за власні кошти встановлювати на своїх телекомунікаційних мережах технічні засоби, необхідні для здійснення уповноваженими органами оперативно-розшукових заходів, і забезпечувати функціонування цих технічних засобів, а також у межах своїх повноважень сприяти вжиттю оперативно-розшукових заходів і недопущенню розголошення організаційних і тактичних прийомів їх проведення[443].

Також відсутній механізм притягнення до відповідальності провайдерів телекомунікацій за невиконання рішень суду щодо блокування інтернет-сайтів чи обмеження доступу до забороненого контенту.

Важливе значення для посилення ефективності протидії наркозлочинності у мережі Інтернет має налагодження повної співпраці підрозділів протидії наркозлочинності та кіберполіції і напрацювання чітких механізмів, які дозволять виявляти такі злочини.

Зокрема, кіберполіцейські мають надавати підрозділам протидії наркозлочинності на місцях всю необхідну підтримку, що дасть змогу ідентифікувати як продавця, так і споживача. Сьогодні злочинці вже припиняють користуватися аналоговими каналами зв'язку та класичними місцями для збереження інформації. Дедалі частіше вони використовують хмарні сервіси збереження інформації та абузостійкі хостинги, які не контролюються державними органами. Отже, для підрозділів Національної поліції важливо використовувати сучасні високотехнологічні інструменти для отримання доказової бази[444].

Окрім того, працівники Департаменту протидії наркозлочинності повинні швидко, ефективно та комплексно реагу-

---

[443] Про телекомунікації: Закон України від 18.11.2003№ 1280-IV. *Відомості Верховної Ради України*. 2004. № 12. Ст. 155.

[444] Сергій Демедюк: Для протидії сучасній злочинності правоохоронці потребують якісних інструментів реверсної інженерії. URL: https://cyberpolice.gov.ua/news/sergij-demedyuk-dlya-protydiyi-suchasnij-zlochynnosti-pravooxoronczi-potrebuyut-yakisnyx-instrumentiv-reversnoyi-inzheneriyi-1575/

вати на виклики сьогодення й якісно документувати факти розповсюдження наркотиків із використанням сучасних інформаційних і телекомунікаційних технологій, оперативно перевіряти інформацію від громадян щодо діяльності інтернет-крамниць із продажу наркотиків.

## 2.8. Використання безпілотних літальних апаратів у правоохоронній діяльності

Одними з перших почали використовувати безпілотні літальні апарати (БпЛА, дрони) для охорони правопорядку поліцейські США. Зокрема, Федеральне управління цивільної авіації (FAA) авторизувало вже 74 урядові агентства з використання БпЛА у повітряному просторі країни, 17 із яких – правоохоронні. Найбільш відомі серед них – Montgomery County в Техасі, Mesa County Sheriff's Department в Колорадо і Grand Forks у Північній Дакоті. Дозвіл FAA надав можливість правоохоронцям легально задіяти БпЛА для детального обстеження місць злочину і пошуку постраждалих людей[445].

Поліцейські США намагаються використовувати дрони і в більш складних операціях, таких як спостереження за потенційно небезпечними злочинцями. Зокрема, у червні 2018 року компанія Axon оголосила, що разом із DJI поставлятиме поліції США патрульних дронів за програмою Axon Air. Усі дрони з'єднані з Evidence.com – «хмарною» системою управління даними, куди надходитиме вся інформація з камер дронів.

Axon Air пропонує підрозділам поліції функції, які можуть виконувати дрони: шукати і рятувати людей, здійснювати реконструкцію автомобільних аварій, спостерігати за великими скупченнями людей, здійснювати переслідування правопору-

[445] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

шників і моніторинг будівель, реагувати на природні катастрофи, аналізувати місця злочинів[446].

Компанія Amazon оформила патент на мініатюрні дрони для патрульних поліцейських, які отримали назву UAVA (Unmanned Aerial Vehicle Assistant – безпілотний літальний апарат-асистент). Судячи з опису, дрон-коп сидітиме на плечі патрульного поліцейського, за командою «злетіти» літальний апарат підніматиметься в повітря для виконання команд поліцейського. Оснащений відеокамерою дрон зможе зазирнути туди, куди працівнику поліції заходити небезпечно, і, відтак, позбавить його від невиправданого ризику. Крім того, дрон зможе брати участь у переслідуванні злочинців. Маючи підтримку з повітря, наздогнати правопорушника буде набагато легше, а він, перебуваючи в полі зору безпілотника, має менше шансів утекти[447].

В окремих країнах БпЛА уже протидіють браконьєрам і контрабандистам. Зокрема, у 2013-2014 роках на 80 відсотків скоротився браконьєрський відстріл слонів і носорогів в Африці. Американський уряд і корпорація Google в межах гуманітарної допомоги африканським країнам, які особливо потерпають від браконьєрства, надали підрозділ патрульних і бойових дронів і навчили місцевий обслуговувальний персонал правилам поводження з цією грізною зброєю. На дронах, що використовуються проти браконьєрів, були зняті бойові установки, а замість них установлені липучі сітки і вражаючі дротики зі снодійним[448].

Британські поліцейські почали використовувати практично безшумні мультикоптери Black Hawk (рис. 8), що дозволяє вести відеозапис зі звуком. Також стало відомо про плани

---

[446] DJI и Axon начнут выпускать дронов-полицейских. URL: https://hightech.fm/2018/06/07/axon

[447] Полиция будущего: расследование и предотвращение преступлений. URL: https://naked-science.ru/article/nakedscience/policiya-budushchego

[448] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

британської поліції використовувати БпЛА в операціях із переслідування злочинців. За різними оцінками, це обійдеться поліцейським набагато дешевше і безпечніше, ніж застосування мотоциклів, автомобілів і вертольотів. Придбання дрона і його тривала експлуатація обійдуться поліції в суму меншу, ніж одна погоня з використанням вертольота (що можливо далеко не завжди) і двох поліцейських автомобілів. Окрім того, застосування БпЛА не загрожує життю поліцейських[449].

*Рис. 8. Мультикоптер Black Hawk.*
*Фото: washingtontimes.com*

Про перше успішне застосування квадрокоптера британською поліцією стало відомо ще в лютому 2010 року, коли за допомогою апарату AirRobot AR100B, оснащеного системою відеоспостереження і тепловізійною камерою, поліцейські

[449] Беспилотный летательный апарат БПЛА (дрон). URL: http://www.tadviser.ru/index.php/

графства Мерсісайд на заході Англії змогли розшукати в густому тумані автомобільного злодія[450].

У квітні 2016 року мерія міста Дубай запустила в небо дрона-поліцейського, основним завданням якого стало стеження за екологічним порядком у місцях відпочинку і пустелі (рис. 9). Подібні дрони зможуть швидко з'являтися в різних місцях, знімаючи на камеру порушників. Водночас особливо наголошується, що, якщо дрони добре себе зарекомендують, поліція ОАЕ всерйоз задумається про використання цих апаратів для більш складних завдань[451].


*Рис. 9. Дрон-поліцейський міста Дубай.*
*Фото: twitter.com*

[450] Наша служба и опасна и трудна. Дроны на службе правоохранительных органов. URL: https://iot.ru/gadzhety/nasha-sluzhba-i-opasna-i-trudna-drony-na-sluzhbe-pravookhranitelnykh-organov

[451] Там само.

Ізраїльська компанія Laser Detect Systems (LDS) представила на виставці HLS&Cyber Expo в Тель-Авіві перший в світі безпілотник SpectroDrone, оснащений датчиками для пошуку вибухівки і саморобних вибухових пристроїв із безпечної відстані. Безпілотник використовує лазерну систему виявлення вибухівки та інших небезпечних матеріалів у газах, рідинах, порошках із відстані в кілька кілометрів. SpectroDrone здатний виконувати ці завдання, маючи оперативний радіус дії в 3 кілометри. Передбачається, що новий апарат можна застосовувати для розшуку баз і складів терористів, а також для виявлення мін і фугасів у зонах локальних конфліктів. Нині для цих цілей використовують системи виявлення вибухівки, що розміщуються на автомобільній техніці, а також переносні комплекти і службових собак[452].

Водночас неправомірне застосування дронів зловмисниками може призвести до тяжких наслідків. Приміром, дрони над злітно-посадковою смугою лондонського аеропорту Гатвік стали причиною скасування сотень авіарейсів і призвели до хаосу. Літакам довелося змінювати маршрут і прямувати до інших аеропортів Великобританії. Ситуація була настільки серйозною, що для допомоги поліції вирішили залучити армію.

Влада багатьох країн розуміє, що цілком безпечні на вигляд безпілотні літальні апарати можуть становити загрозу – скажімо, для авіації, і розробляють методи боротьби з ними.

Зокрема, дронів-порушників виявляють або визначають їхнє місце розташування за допомогою камер, радарів і датчиків частот. Подібні технологічні рішення можна інтегрувати в наявну інфраструктуру аеропортів. Потім пристрої створюють радіоперешкоди, через що дрон, втративши зв'язок із базою, автоматично повертається до власника. Такий метод, зокрема, розробила компанія Quantum Aviation. Під час Олімпійських ігор у Лондоні у 2012 році їй було доручено створити систему

[452] Наша служба и опасна и трудна. Дроны на службе правоохранительных органов. URL: https://iot.ru/gadzhety/nasha-sluzhba-i-opasna-i-trudna-drony-na-sluzhbe-pravookhranitelnykh-organov

захисту від можливих терористичних нападів із використанням дронів[453].

У Китаї розробили спеціальний пістолет, який створює перешкоди, і, як повідомляється, може вивести з ладу безпілотники на відстані майже в кілометр. Альтернативою вогнепальній зброї стали ручні або наплічні пристрої, за допомогою яких можна вистрілювати в дрона сіткою, яка його перехоплює і не дає крутитися пропелерам, тоді безпілотник падає.

Британська інженерна компанія OpenWorks розробила величеньку базуку SkyWall100, яка стріляє по цілі сіткою з парашутом. Для точності пристрій обладнаний оптичним прицілом[454].

Існують також дрони-перехоплювачі, які наближаються до дрона-порушника, скидають на нього сітку, і таким чином знешкоджують його в повітрі (рис. 10). Подібні пристрої працювали на зимовій Олімпіаді в Південній Кореї, а поліція Токіо використовує їх уже три роки.

*Рис. 10. Перехоплення дрона-порушника.*
*Фото: 3dnews.ru*

[453] Лазери, орли і радари: як у світі борються з дронами. URL: https://www.bbc.com/ukrainian/features-46652017

[454] Там само.

Принцип роботи тут гранично простий: на великий квадрокоптер знизу прикріплюється сітка розміром приблизно 2 на 3 метри. Далі такий апарат наздоганяє дрібних дронів-порушників і, зловивши їх сіткою, виносить із забороненої зони. Вперше на практиці подібний метод відлову дронів-порушників був випробуваний ще в лютому 2016 року. Також цю технологію взяли на озброєння у Франції[455].

Ще одним варіантом боротьби з дронами-порушниками є лазерні пристрої, які здатні збивати безпілотники через кілька секунд після виявлення. Над цією технологією працюють США і Китай. Зокрема, компанія Boeing розробила апарат, який за допомогою високоенергетичного променя виявляє і виводить із ладу невеликі дрони. Радіус дії – кілька кілометрів. Як повідомляється, вони здатні функціонувати навіть за низької видимості, як-от у тумані[456].

Нещодавно на виставці зброї в Казахстані Китай продемонстрував лазерну гармату «Тихий мисливець». Як повідомляється, її використовує поліція для перехоплення дронів і інших невеликих повітряних цілей, маючи при цьому високу точність[457].

У Нідерландах придумали нетехнологічний спосіб боротьби з високотехнологічною проблемою. Поліція там займається дресируванням орлів для знешкодження дронів-порушників. Вони захоплюють пропелери своїми кігтями й таким чином відразу ж виводять їх із ладу. За словами дресирувальників, орли сприймають дронів за здобич і не нападатимуть на якісь інші цілі, коли їх випускають[458].

Американський виробник нелетальної зброї Taser International заявив, що готовий надати поліції США безпілотники, оснащені електрошокерами. Компанія провела переговори з представниками поліції на конференції в Сан-Дієго, пише The Wall Street Journal. Улітку 2015 року поліція Далласа впер-

[455] Наша служба и опасна и трудна. Дроны на службе правоохранительных органов. URL: https://iot.ru/gadzhety/nasha-sluzhba-i-opasna-i-trudna-drony-na-sluzhbe-pravookhranitelnykh-organov

[456] Лазери, орли і радари: як у світі борються з дронами. URL: https://www.bbc.com/ukrainian/features-46652017

[457] Там само.

[458] Там само.

ше в історії за допомогою робота Remotec F-5, озброєного вибухівкою, нейтралізувала Міку Ксавьера Джонсона, який до цього застрелив п'ятьох поліцейських під час вуличної акції.

У поліції США вважають, що застосування озброєних електрошокером дронів може зберегти життя працівникам поліції під час небезпечних операцій. Taser – це електрошокова зброя несмертельної дії з радіусом дії до 10 м, що дозволяє проводити затримання правопорушників із нелетальними наслідками.

Водночас неприйняття суспільством ідеї, що безпілотні літальні апарати можуть бути обладнані якимось видом зброї, є перешкодою, яку треба подолати, – вважають представники департаменту поліції Портленда[459].

Правоохоронним і законодавчим органам різних країн ще потрібно вирішити юридичні питання, пов'язані з використанням дронів. Однак уже зараз очевидно, що можливості силовиків із залученням БпЛА зростуть багаторазово.

Нині можна вирізнити такі можливості використання дронів правоохоронними структурами:

- запобігання терористичним актам;
- операції з боротьби з організованою злочинністю;
- операції із затримання злочинців і розшуку зниклих людей;
- вивчення місця злочину;
- профілактичне відеоспостереження;
- контроль масових заходів і акцій протесту;
- забезпечення VIP-зустрічей, зокрема на найвищому рівні;
- підтримка оперативного зв'язку;
- запобігання нелегальній імміграції і контрабанді;
- спостереження за наземними і морськими лініями регулярних перевезень і транспортними потоками, аналіз причин ДТП;
- відстеження викрадених автомобілів;
- боротьба з морськими піратами;
- запобігання браконьєрству, незаконній розробці надр і незаконній вирубці лісів тощо[460].

---

[459] Полиция США может вооружить дроны электрошокерами. URL: https://apparat.cc/news/police-drones-armed-with-stun-guns/

[460] Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

## *Розділ 3*

# ОСОБЛИВОСТІ ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ

## 3.1. Організаційно-правові основи інформаційно-аналітичного забезпечення розслідування злочинів

Результативність діяльності правоохоронних органів у боротьбі зі злочинністю безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності.

У нормативно-правових актах і науковій літературі поряд із терміном «інформаційно-аналітичне забезпечення» часто вживаються терміни «інформаційне забезпечення», «інформаційно-аналітична діяльність», «інформаційно-аналітична робота», «аналітична робота», «кримінальний аналіз», «модель поліцейської діяльності, керованої аналітикою» тощо[461].

---

[461] Див.: Юрченко О. М., Стрельбицька Л. М., Вертузаєв О. М. Застосування новітніх інформаційних технологій в інформаційно-аналітичному забезпеченні оперативно-службової діяльності правоохоронних органів. *Науковий вісник Київського національного університету внутрішніх справ.* Київ, 2006. № 3. С. 40–49; Задорожний Ю. А. Проблемы информационно-аналитического обеспечения ОРД в современных условиях. Виявлення, фіксація та використання доказів у процесі досудового слідства. *Вісник ЛАВД імені 10-річчя незалежності України. Спеціальний випуск.* Луганськ, 2005. С. 89–99; Юридическое, техническое и информаци-

онно-аналитическое обеспечение оперативно-розыскной деятельности: учебное пособие / А. Н. Халиков, Е. Н. Яковец, Н. И. Журавленко; под редакцией А. Н. Халикова. Москва: Юрлитинформ, 2010. 472 с.; Хахановський В. Г. Інформаційно-аналітичне забезпечення ОРД: основні поняття та нормативно-правова база. Шляхи вдосконалення оперативно-розшукової діяльності ОВС. *Вісник ЛІВС.* Львів, 2002. № 2(1). С. 191–195; Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учеб. пособие. Москва: Щит-М, 2009. 464 с.; Берназ П. В. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. Південноукраїнський правничий часопис. 2015. № 4. С. 49; Белов О. А. Информационное обеспечение раскрытия и расследования преступлений: монография. Москва: Юрлитинформ, 2009. 136 с.; Захаров В. П., Рудешко В. І. Проблеми інформаційного забезпечення правоохоронних структур: навчально-практичний посібник. Львів: ЛьвДУВС, 2007. 372 с.; Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / под ред. В. И. Попова. Москва: ИНФРА-М, 2002. 97 с.; Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. Москва: ИНФРА-М, 2000. 367 с.; Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/98-ВР. *Відомості Верховної Ради України.* 1998. № 27–28. Ст. 181; Автоматизовані системи. Терміни та визначення: ДСТУ 2226–93. Чинний від 1994-07-01. Київ: Держстандарт України, 1993. 91 с. (Національні стандарти України); Овчинский А. С., Каретников М. К. Проблемы подготовки специалистов в области применения современных информационных технологий. *Вестник МВД России*. 2000. № 4–5. С. 130–131; Основи кримінального аналізу: посіб. з елементами тренінгу / О. Є. Користін, С. В. Албул, А. В. Холостенко та ін. Одеса: ОДУВС, 2016. 112 с.; Власюк О. В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України. *Матеріали постійно діючого науково-практичного семінару.* Харків: Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого, 2011. Вип. 3. Ч. 1. С. 82–85; Заєць О. М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні. Сучасний стан і перспективи розвитку. *Вісник кримінального судочинства.* 2016. № 4. С. 17–25; Махнюк А. В. Теоретичні основи провадження кримінального аналізу у сфері правоохоронної діяльності. *Науковий вісник Державної прикордонної служби*. 2011. № 94. С. 3–7; Некрасов В. А. Сучасне розуміння кримінальної розвідки як напряму діяльності правоохоронних органів. *Кримінальна розвідка: методологія, законодавство, зарубіжний досвід:* матер. Міжнар. наук.-практ. конф. (м. Одеса, 29 квіт. 2016 р.). Одеса: ОДУВС, 2016. С. 19–20; Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования. Д. Ю. Узлов, В. М. Струков, О. Б. Григорович та ін. *Право і безпека*.

Термін «аналітичний» означає «стосується аналізу», заснований на застосуванні аналізу, тому можна використовувати словосполучення «аналітична робота» і «аналітична діяльність» як тотожні слову «аналіз»[462].

У науковій літературі *інформаційне забезпечення розслідування злочинів* визначається як комплекс заходів, що здійснюються різними підрозділами правоохоронних органів, спрямованих на отримання з гласних і негласних джерел криміналістичної, оперативної та процесуальної інформації, її фіксацію, зберігання, обробку, аналіз, а також використання первинних і збагачених даних із метою виконання слідчими та оперативними підрозділами покладених на них функцій[463].

Інформаційне забезпечення складається з трьох взаємопов'язаних компонентів:

1) *інформаційних систем*, у межах яких здійснюється збір, накопичення, системна обробка, зберігання й видача споживачу необхідної криміналістичної, оперативної, процесуальної та іншої інформації;

2) *аналітичної роботи*, що полягає у здійсненні комплексу організаційних заходів і методичних прийомів з обробки та синтезу наявної криміналістичної, оперативної, процесуальної та іншої інформації;

3) *управлінської діяльності*, яка забезпечує прийняття необхідних рішень щодо стратегії й тактики протидії злочинності[464].

---

2015. № 2 (57). С. 132–139; J. G. Carter, S. W. Phillips, S. M. Gayadeen. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. *Journal of Criminal Justice*. 2014. № 42. P. 433-442; Яніцкі М. Оперативний кримінальний аналіз. *Міжнародна організація з міграції*. Київ, 2009. 86 с.

[462] Великий тлумачний словник сучасної української мови / упоряд. і голов. ред. В. Т. Бусел. Київ, Ірпінь: ВТФ: Перун, 2001. С. 17.

[463] Міжнародна поліцейська енциклопедія: у 10 т. / відп. редактори В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. Київ: Атіка, 2010. Т. VI. Оперативно-розшукова діяльність поліції (міліції). С. 349.

[464] Галючек А., Журавльов В. Інформаційне та аналітичне забезпечення оперативно-розшукової діяльності спеціальних підрозділів по боротьбі з організованою злочинністю ОВС: метод. рек. Запоріжжя: Запорізький юридичний інститут ДДУВС, 2008. С. 7–8.

*Інформаційні системи* – це організаційно-технічні системи, в яких реалізуються технології обробки інформації з використанням технічних і програмних засобів[465]. До складу інформаційних систем можуть уходити інформаційні підсистеми, які містять банки даних, поєднані технологією обміну інформацією.

Неабияке значення в аналітичній роботі мають аналітичні схеми. Формуються вони у складних багатоепізодних справах, пов'язаних із діяльністю організованих злочинних груп, за розслідування яких доводиться встановлювати способи вчинення злочинів, визначати складні зв'язки, які взаємно пересікаються між окремими учасниками злочину[466].

У науковій літературі *управлінську діяльність* у системі Національної поліції поділяють на *внутрішньосистемну*, яка спрямована на упорядкування управлінських відносин, що виникають із питань організації системи та структури органів Національної поліції, та *зовнішньосистемну* управлінську діяльність, зміст якої зводиться до забезпечення поліцейськими функцій з охорони правовідносин[467].

Поряд із терміном «інформаційне забезпечення» вживається дефініція «інформаційно-аналітичне забезпечення», під яким В. Г. Хахановський розуміє кількісне (консолідація масивів інформації у вигляді баз і банків даних, упорядкування, систематизація), а також якісно-змістовне перетворення криміналістичної, оперативної та процесуальної інформації (продуку-

[465] Міжнародна поліцейська енциклопедія: у 10 т. / відп. редактори В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. Київ: Атіка, 2010. Т. VI. Оперативно-розшукова діяльність поліції (міліції). С. 352.

[466] Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів: монографія. Київ: Нац. акад. внутр. справ України, 2005. С. 9.

[467] Голосніченко І. П. Адміністративне право України (основні категорії і поняття). Київ: ГАН, 2005. С. 40–45.

вання нових знань, прийняття управлінських рішень) на базі інформаційної аналітики[468].

Головним завданням *інформаційно-аналітичного забезпечення розслідування злочинів* є систематичне і своєчасне надходження в підрозділи досудового розслідування достовірної криміналістичної, оперативної та процесуальної інформації.

У теорії та практиці правоохоронної діяльності вживається також термін «моніторинг» (від англ. *monitoring*, із лат. *monitor* – той, що наглядає і нагадує) – комплекс досліджень (спостереження, аналіз та інші методи пізнання) і контролю за станом чи процесами певного середовища прикладної системи, метою якого є попередження про появу шкідливих, небезпечних чи бажаних факторів (явищ) для існування цієї системи[469].

На теренах вітчизняної науки дедалі частіше поряд з інформаційно-аналітичним забезпеченням говорять про кримінальний аналіз. *Кримінальний аналіз* є специфічним видом інформаційно-аналітичної діяльності правоохоронних органів, який полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі виявлення, припинення та розслідування злочинів і мають значення для ОРД й досудового розслідування, з метою їх використання правоохоронними органами і судом, подальшого проведення оперативного, тактичного і стратегічного аналізу.

Розглянемо тепер поняття «*інформаційно-аналітична робота*», яку у науковій літературі розглядають, по-перше, як елемент організації розслідування злочинів, тобто пошук, збирання, оцінка, аналіз, узагальнення даних, необхідних для прийняття управлінського чи оперативного рішення;

---

[468] Хахановський В. Г. Інформаційно-аналітичне забезпечення ОРД: основні поняття та нормативно-правова база. Шляхи вдосконалення оперативно-розшукової діяльності ОВС. *Вісник ЛІВС.* Львів, 2002. № 2 (1). С. 191.

[469] Міжнародна поліцейська енциклопедія: у 10 т.; відп. редактори В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. Київ: Атіка, 2010. Т. VI. Оперативно-розшукова діяльність поліції (міліції). С. 353.

по-друге, як засіб отримання інформації під час розслідування злочинів[470].

*Інформаційно-аналітична робота у розслідуванні злочинів* – це передбачена законодавством України й урегульована відомчими нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, зокрема обмеженого доступу, що має значення для вирішення завдань ОРД і досудового розслідування, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави[471].

Вирізняються такі складові елементи поняття інформаційно-аналітичної роботи при розслідуванні злочинів та їх особливості:

1. *Інформаційно-аналітична робота при розслідуванні злочинів* – це система заходів (процесуальних, криміналістичних, оперативно-розшукових, пошукових, розвідувальних, контррозвідувальних, організаційно-управлінських, технічних, аналітичних тощо), що передбачені законами України та врегульовані відомчими нормативними актами органів, уповноважених на здійснення досудового розслідування та ОРД, які визначають її порядок і умови.

2. *Суб'єктами* інформаційно-аналітичної роботи у розслідуванні злочинів є слідчі, експертно-криміналістичні, оперативні й інформаційно-аналітичні підрозділи та їх посадові особи і певною мірою інші працівники правоохоронних органів і негласні працівники.

3. *Об'єктами* інформаційно-аналітичної роботи за розслідування злочинів є фізичні та юридичні особи, корпоративні об'єкти, предмети, документи, речовини, тварини, трупи, приміщення, споруди, ділянки місцевості, мережа Інтернет, інформаційні ресурси, явища, процеси, події, навички, зовнішні дії

---

[470] Шумилов А. Ю. Оперативно-розыскная энциклопедия. Москва: Издатель Шумилова И. И., 2004. 364 с.

[471] Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: ЛьвДУВС, 2017. 244 с.

людини, радіоефір, трафіки зв'язків абонентів мобільного зв'язку тощо.

4. *Механізм* інформаційно-аналітичної роботи охоплює низку дій суб'єктів її здійснення (пошук, фіксацію, отримання, обробку, систематизацію, узагальнення, аналіз, прогнозування, зберігання та використання інформації).

5. *Предметом* інформаційно-аналітичної роботи у розслідуванні злочинів є характерні особливості чи ознаки об'єктів інформаційно-аналітичної роботи, зафіксовані на відповідних носіях або в пам'яті людей, або їх відображення.

6. *Основними засобами* інформаційно-аналітичної роботи при розслідуванні злочинів є:

– оперативна та криміналістична техніка і спеціальні технічні засоби, призначені для гласного та негласного отримання інформації;

– відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи тощо) і різні технічні пристрої, за допомогою яких здійснюється обробка, систематизація та аналіз оперативно-розшукових та інших відомостей фактографічного та криміналістичного характеру.

Важливу роль у цьому виконують принципи інформаційно-аналітичної роботи.

До *загальних принципів* інформаційно-аналітичної роботи у розслідуванні злочинів уходять принципи верховенства права, законності, гуманізму; дотримання прав і свобод людини; поєднання гласних і негласних методів і засобів; високої оперативності (наступальності); всебічності, повноти та об'єктивності; науковості; застосування досвіду і теоретичних знань інших суміжних наук.

*Спеціальні принципи* інформаційно-аналітичної роботи під час розслідування злочинів пов'язані з закономірностями, що виникли із сутності її процесу. До них належать: безперервність накопичення інформації, системність, узгодженість, варіантність, верифікованість, ефективність тощо.

Основними *інформаційними ресурсами*, що використовуються в процесі інформаційно-аналітичної роботи у розслідуванні злочинів, є:

– *оперативні обліки*, які складаються із оперативно-розшукових, оперативно-профілактичних та оперативно-довідкових обліків;

– *криміналістичні обліки*, які складаються з оперативно-пошукових та інформаційно-довідкових колекцій;

– *банки даних* кримінологічної, адміністративної, статистичної інформації;

– *банки даних* інших міністерств, відомств, підприємств, установ та організацій, які не стосуються безпосередньо боротьби зі злочинністю;

– *банки даних* міських і обласних органів влади;

– *об'єкти* надання та отримання охоронних послуг;

– *оператори* мобільного зв'язку;

– *звернення та заяви* громадян, депутатські запити;

– *засоби* масової інформації, зокрема Інтернет.

Заслуговує на увагу розроблення та використання у розслідуванні злочинів автоматизованих робочих місць слідчого (*АРМ слідчого «Інсайт»*), що містить 12 модулів *(«Законодавство», «Документ», «Слідчі дії», «Слідча практика», «Науково-технічні засоби», «Судові експертизи», «Криміналістичні методики», «Словник термінів», «Правоохоронні органи та експертні установи», «Навчання», «Бібліографія», «Довідкова корисна інформація»*), які можуть використовуватись окремо або комплексно, а також АРМ судових експертів різних експертних спеціальностей (*АРМ трасолога, АРМ баліста, АРМ економіста, АРМ фоноскопіста, АРМ дослідження об'єктів інтелектуальної власності тощо), АРМ судді, АРМ обробки та надсилання документів, АРМ секретаря судді, АРМ працівника підрозділу боротьби з наркозлочинністю, АРМ юриста, АРМ юриста-кримінолога, АРМ прокурора*[472].

[472] Юсупов В. В. Криміналістика в Україні у XX–XXI століттях: монографія. Київ: ФОП Маслаков, 2018. С. 455–456.

Професор В. Г. Хахановський зазначає, що в експертно-криміналістичних підрозділах функціонують програмно-апаратний комплекс *«Баліст»*, інформаційно-довідкові системи *«Паспорт»*, *«Автодокументи»,* АІС *«ATLAS», «Автодок», «Відеооблік», «Відеоряд»* тощо[473].

Кримінальний процесуальний кодекс України регламентує проведення допиту, впізнання у режимі відеоконференції під час досудового розслідування (ст. 232 КПК України) та проведення процесуальних дій у режимі відеоконференції під час судового провадження (ст. 336 КПК України).

*Основними завданнями інформатизації досудового розслідування* на сучасному етапі є:

– збирання, обробка й накопичення якісної та вірогідної інформації в базах даних за всіма напрямами діяльності слідчих, експертно-криміналістичних та оперативних підрозділів;

– забезпечення оперативного доступу користувачів (слідчих та оперативних працівників) до баз даних безпосередньо з робочих місць;

– використання сучасних аналітичних методів обробки криміналістичної, процесуальної та оперативно-розшукової інформації;

– використання ресурсів невідомчих інформаційних систем з метою забезпечення правоохоронної діяльності багатовидовою інформацією;

– визначення перспективних напрямів та тенденцій розвитку сучасної злочинності;

– адаптація наявних положень тактики і методики криміналістики, ОРД та досудового розслідування до умов сучасного інформаційного суспільства;

– розроблення, упровадження та використання спеціального програмного забезпечення.

---

[473] Хахановський В. Г. Теорія і практика криміналістичної інформатики: автореф. дис. … докт. юрид. наук: 12.00.09. Київ, 2011. С. 14.

## 3.2. Характеристика Єдиної інформаційної системи МВС України

Відповідно до Закону України «Про Національну поліцію», поліція виконує інформаційно-аналітичну діяльність винятково для реалізації своїх повноважень, визначених цим Законом.

Національна поліція в межах інформаційно-аналітичної діяльності:

1) формує бази (банки) даних, що входять до єдиної інформаційної системи Міністерства внутрішніх справ України;

2) користується базами (банками) даних Міністерства внутрішніх справ України та інших органів державної влади;

3) здійснює інформаційно-пошукову та інформаційно-аналітичну роботу;

4) здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями[474].

Національна поліція може створювати власні бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу, а також міжвідомчі інформаційно-аналітичні системи, необхідні для виконання покладених на неї повноважень.

Для забезпечення публічної безпеки і порядку поліція може закріплювати на форменому одязі, службових транспортних засобах, монтувати по зовнішньому периметру доріг і будівель автоматичну фото- і відеотехніку, а також використовувати інформацію, отриману із автоматичної фото- і відеотехніки, що знаходиться в чужому володінні, з метою: попередження, виявлення або фіксування правопорушення, охорони громад-

[474] Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40–41. Ст. 379.

ської безпеки та власності, забезпечення безпеки осіб; забезпечення дотримання правил дорожнього руху. Інформація про розміщену автоматичну фототехніку і відеотехніку повинна бути розміщена на видному місці[475].

Діяльність Національної поліції, яка пов'язана із захистом і обробкою персональних даних, здійснюється на підставах, визначених Конституцією України, Законом України «Про захист персональних даних», іншими законами України.

У МВС створена і функціонує ***Єдина цифрова відомча телекомунікаційна мережа МВС (ЄЦВТМ)***. ЄЦВТМ є логічно цілісною мультисервісною багаторівневою телекомунікаційною мережею МВС, що взаємодіє з Національною телекомунікаційною мережею, Національною системою конфіденційного зв'язку, телекомунікаційною мережею загального користування та містить сукупність технічних засобів телекомунікацій і транспортної телекомунікаційної мережі для забезпечення передавання інформації, яка належить до державних інформаційних ресурсів, з метою задоволення потреб споживачів у сервісних послугах ЄЦВТМ як у звичайних умовах, так і під час особливого періоду, а також в умовах надзвичайних ситуацій чи запровадження надзвичайного стану[476].

Національна поліція наповнює та підтримує в актуальному стані бази (банки) даних, що входять до єдиної інформаційної системи МВС України.

Інформація про доступ до бази (банку) даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, разом з інформацією про поліцейського, який отримав доступ, і про обсяг даних, доступ до яких було отримано. Кожна дія поліцейського щодо отримання інформації з інформаційних ресурсів фіксується в спеціальному електронному архіві, ве-

[475] Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40–41. Ст. 379.

[476] Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС: наказ МВС від 04.07.2016 № 596, зареєстровано в Міністерстві юстиції України 28 липня 2016 р. за № 1055/29185.

дення якого покладається на службу інформаційних технологій МВС України[477].

В електронному архіві фіксуються прізвище, ім'я, по батькові та номер спеціального жетона поліцейського, вид отриманої інформації, реєстр, із якого отримувалася інформація, час отримання інформації та інші дані, необхідні для ідентифікації поліцейського, який отримував інформацію з реєстрів.

Національна поліція вживає заходів щодо недопущення будь-яких порушень прав і свобод людини, пов'язаних із обробкою інформації. Поліцейські несуть персональну дисциплінарну, адміністративну та кримінальну відповідальність за вчинені ними діяння, що призвели до порушень прав і свобод людини, пов'язаних із обробкою інформації[478].

У Національній поліції створена і функціонує ***Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (система ІПНП)*** – як сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються в процесі діяльності Національної поліції та її інформаційно-аналітичного забезпечення. Система ІПНП є частиною єдиної інформаційної системи МВС (ЄІС МВС)[479].

Основними завданнями системи ІПНП є: інформаційно-аналітичне забезпечення діяльності НПУ; забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС; забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу; забезпечення електронної взаємодії з МВС та іншими органами державної влади.

---

[477] Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40–41. Ст. 379.

[478] Там само.

[479] Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України»: наказ МВС від 03.08.2017 № 676.

Складовими системи ІПНП є: центральний програмно-технічний комплекс; автоматизовані робочі місця користувачів; телекомунікаційна мережа доступу; комплексна система захисту інформації.

Складові центрального програмно-технічного комплексу ІПНП повинні забезпечити генерацію інтерфейсів, оброблення тимчасових наборів і формування інформаційних ресурсів ЄІС МВС для таких підсистем:

– *ІП «Єдиний облік»* (автоматизований облік заяв і повідомлень про вчинені кримінальні правопорушення та інші події, зареєстрованих органами НПУ);

– *ІП «Кримінальна статистика»* (автоматизований облік відомостей про кримінальні правопорушення, осіб, які їх учинили або підозрюються в їх учиненні);

– *ІП «Адміністративна практика»* (автоматизований облік відомостей щодо зареєстрованих в органах поліції адміністративних правопорушень, осіб, які їх учинили, результатів розгляду цих правопорушень та виконання накладених стягнень у вигляді штрафів);

– *ІП «Корупція»* (автоматизований облік даних стосовно всіх зареєстрованих кримінальних та адміністративних корупційних правопорушень, осіб, які їх учинили);

– *ІП «Особа» («Правопорушник» і «Підсудний»)* (автоматизований облік інформації про осіб, щодо яких поліцейські здійснюють профілактичну роботу, а також про обвинувачених осіб, обвинувальний акт щодо яких направлено до суду);

– *ІП «Особа» (трафік)* (автоматизований облік відомостей щодо осіб, причетних до торгівлі людьми, та осіб, причетних до нелегальної міграції);

– *ІП «Розшук»* (автоматизований облік відомостей щодо розшуку підозрюваних, обвинувачених (підсудних) осіб, які ухиляються від відбування покарання, безвісти зниклих та інших категорій осіб, які розшукуються);

– *ІП «Пізнання»* (автоматизований облік інформації, зокрема біометричних даних щодо осіб, які переховуються від

органів влади, безвісти зниклих осіб, невпізнаних трупів і людей, які не можуть надати про себе будь-яку інформацію);

– *ІП «Гарпун»* (автоматизований облік даних про транспортні засоби, які пересуваються шляхами загального користування та номерні знаки, які розшукуються з будь-яких підстав у межах кримінального або виконавчого провадження);

– *ІП «Номерні речі»* (автоматизований облік відомостей щодо речей, викрадених, вилучених із ознаками підробки, заборонених або обмежених в обігу у фізичних осіб, безгосподарних, знайдених або вилучених із камер схову вокзалів, аеропортів, зданих до органів поліції, які мають індивідуальні заводські (фабричні) номери);

– *ІП «Культурні цінності»* (автоматизований облік даних щодо викрадених, вилучених культурних цінностей, що належать до об'єктів матеріальної і духовної культури);

– *ІП «Кримінальна зброя»* (автоматизований облік відомостей про викрадену, втрачену, вилучену, знайдену зброю, а також добровільно здану зброю із тієї, що незаконно зберігалася, незалежно від її технічного стану, що має індивідуальні заводські (фабричні) номери або номери деталей);

– *ІП «Зареєстрована зброя»* (автоматизований облік відомостей стосовно зброї, що має індивідуальні заводські (фабричні) номери, перебуває в користуванні громадян, підприємств, установ, організацій, господарських об'єднань, яким надано, відповідно до законодавства, дозвіл на її придбання, зберігання, носіння, перевезення, та яка обліковується органами поліції);

– *ІП «Домашній арешт»* (автоматизований облік даних стосовно підозрюваних, обвинувачених, щодо яких застосовано запобіжний захід у вигляді домашнього арешту);

– *ІП «Втрачені документи»* (автоматизований облік викрадених, втрачених, вилучених документів (бланків документів), зокрема ті, що визнано недійсними, документів осіб, які знаходяться в розшуку, а також документів (бланків документів), що мають індивідуальні заводські (фабричні) номери);

– *ІП «ТЗ, що розшукуються»* (автоматизований облік відомостей про транспортні засоби (автомобілі, мотоцикли, мопеди, плавзасоби), які розшукуються органами поліції, про виявлені безгосподарні транспортні засоби (викрадені та втрачені державні номерні знаки транспортних засобів));

– *ІП «Атріум»* (автоматизований облік даних стосовно осіб, звільнених із місць позбавлення волі, засуджених та тих, які притягаються до кримінальної відповідальності);

– *ІП «Мігрант»* (автоматизований облік даних стосовно осіб, затриманих за порушення законодавства України про державний кордон, про правовий статус іноземців та осіб без громадянства);

– *ІП «Слідство: доручення»* (автоматизований облік відомостей про надання та виконання доручень слідчих щодо проведення слідчих (розшукових) дій за розпочатими кримінальними провадженнями);

– *ІП «Дактилоскопічний облік»* (автоматизований облік відомостей про дактилоскопічні карти, складені щодо осіб, затриманих за підозрою у вчиненні правопорушень, а також невпізнаних трупів і людей, які не можуть надати про себе будь-яку інформацію);

– *ІП «Аналітика»* (програмний комплекс аналітичних засобів забезпечує роботу генератора запитів і генератора звітів);

– *ІП підтримки ЕЦП* (програмні засоби, що розміщуються та функціонують на програмнотехнічних потужностях ІПНП і забезпечують можливості накладання ЕЦП на документи, утворені в процесі оперативно-службової діяльності поліції в електронному вигляді та внесені до ІПНП);

– *ІП «Кримінальна аналітика»* (забезпечує доступ (інформаційну взаємодію) до інформаційних ресурсів окремим програмним засобам або формує необхідні інтерфейси, що використовуються для функціонування моделі поліцейської діяльності, керованої аналітикою «Intelligence Led Policing»)[480].

[480] Див.: Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковсь-

Крім того, за розкриття та розслідування злочинів використовуються такі бази даних Національної поліції:

– *ІП «HotLine» – Call-центр Національної поліції* (автоматизована система прийому повідомлень на «гарячу» телефонну лінію 0800-500202);

– *ІП «102»* (автоматизована підсистема прийому повідомлень «102» за допомогою телекомунікаційних мереж);

– *ІП «Цунамі»* (автоматизована підсистема централізованого управління нарядами поліції);

– *Програмний модуль інтеграційної платформи ІПНП* (для взаємодії інформаційних підсистем НПУ з регіональними сегментами систем забезпечення публічної безпеки і порядку (в рамках реалізації проектів «Безпечне місто»), інформаційними підсистемами та реєстрами інших ЦОВВ);

– *ІП картографічної інформації* (програмні компоненти геоінформаційних підсистем, що необхідні для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта);

– *ІП «ДТП»* (автоматизований облік відомостей про дорожньо-транспортні пригоди, зокрема фотовідеозображення з місця події, фіксування координат події на карті регіону (країни));

– *ІП «Кіберзлочин»* (автоматизований облік відомостей щодо правопорушень та осіб, які причетні до скоєння злочинів у сфері інформаційних технологій);

– *ІП «Дозвіл БДР»* (автоматизований облік відомостей щодо дозволів на рух окремих категорій транспортних засобів, зокрема небезпечних і негабаритних вантажів);

– *ІП «ITT-Custody records»* (автоматизована підсистема, що забезпечує відстеження порядку тримання осіб в ізоляторах тимчасового тримання головних управлінь НПУ);

---

кий. Київ, 2017. 36 с.; Оперативно-розшукова діяльність: посібник для вищих навчальних закладів. Київ: «Видавництво Людмила», 2019. 240 с.; Методичні рекомендації МВС України щодо алгоритму дій користувачів з організації формування Інтегрованої інформаційно-пошукової системи ОВС України: службовий лист МВС від 16.01.2014 за 727/3р.

– *Сегмент порталу взаємодії з ресурсами в мережі Інтернет* (програмний комплекс, що забезпечує підтримку мобільних додатків, призначених для інформування підрозділів поліції про правопорушення та події)[481].

Розвиток програмного комплексу здійснюється на основі експериментального проекту *мобільного додатку «Моя поліція»*, що здійснює опрацювання повідомлень і звернень громадян, які надійшли із застосуванням технологій для мобільних телефонних пристроїв (смартфонів).

За допомогою мобільного додатку передбачено опрацювання таких основних функціональних можливостей:

– *кнопка «SOS»* (для екстреного виклику на спецлінію «102»);

– *повідомлення про правопорушення* (зокрема з фото-, відео та аудіофайлами);

– *push-сповіщення* (отримання користувачами важливої інформації від поліції (зокрема про надзвичайні новини, орієнтування, перекриття руху під час проведення масових заходів тощо));

– *«активний свідок»* (дозволяє швидко знаходити свідків правопорушення, використовуючи потенціал мобільних платформ);

– *карта відділень поліції та медичних закладів* (дає змогу відшукати найближче відділення, куди можна звернутися по допомогу);

– *інструкція спілкування з поліцейськими* (як правильно діяти у тій чи іншій ситуації, а також як мають поводитися поліцейські);

---

[481] Див.: Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковський. Київ, 2017. 36 с.; Оперативно-розшукова діяльність: посібник для вищих навчальних закладів. Київ: «Видавництво Людмила», 2019. 240 с.; Методичні рекомендації МВС України щодо алгоритму дій користувачів з організації формування Інтегрованої інформаційно-пошукової системи ОВС України: службовий лист МВС від 16.01.2014 за 727/3р.

– *моніторинг роботи поліцейських* (користувачі програми мають змогу оцінити роботу поліцейського за п'ятибальною шкалою, а також залишити анонімний відгук);

– *актуальні новини поліції* (можливість користувачів ознайомитися з новинами поліції)[482].

Відповідно до напряму функціонування галузевих служб Національної поліції, розрізняють оперативні, кримінологічні, криміналістичні, адміністративні обліки.

Важливою умовою протидії злочинності є ефективне використання системи оперативних обліків. ***Оперативні обліки*** – це система реєстрації, накопичення, класифікації, зберігання та використання даних про осіб, предмети, події за їх прикметами та ознаками, призначена для ефективного забезпечення оперативно-розшукової діяльності оперативних підрозділів правоохоронних органів, яка складається із автоматизованих інформаційних систем, картотек, оперативно-розшукових справ, справ контрольно-наглядового провадження та інших документів оперативно-розшукового та довідкового призначення.

Зокрема, для систематизації та аналізу матеріалів, одержаних у результаті ОРД, у Департаменті інформаційно-аналітичної підтримки та управліннях інформаційно-аналітичної підтримки територіальних органів Національної поліції функціонує ***автоматизована інформаційна система оперативного призначення (АІС ОП).***

АІС ОП уведена в дію наказом МВС України від 20 жовтня 2017 р. № 870 «Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної

[482] Див.: Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковський. Київ, 2017. 36 с.; Оперативно-розшукова діяльність: посібник для вищих навчальних закладів. Київ: «Видавництво Людмила», 2019. 240 с.; Методичні рекомендації МВС України щодо алгоритму дій користувачів з організації формування Інтегрованої інформаційно-пошукової системи ОВС України: службовий лист МВС від 16.01.2014 за 727/3р.

інформаційної системи МВС»[483] і призначена для накопичення й обробки відомостей, що утворюються в процесі оперативно-розшукової діяльності НПУ.

Функції АІС ОП полягають у такому: автоматизація процесів обліку отриманої в процесі ОРД НПУ інформації; збір, зберігання, пошук та узагальнення інформації; відображення повнотекстової, графічної, табличної та статистичної інформації, а також фото- і відеозображень; утворення електронного досьє; формалізація технологічних процесів обробки інформації, визначення типових маршрутних технологічних схем для їх виконання; забезпечення надійного зберігання інформаційних обліків та їх систематизація; забезпечення комплексного захисту інформації та розмежування доступу до інформації, що зберігається в АІС ОП.

Обліку в АІС ОП підлягають відомості про осіб, щодо яких заведено оперативно-розшукові справи, які отримані:

1) від осіб, які конфіденційно співробітничають із оперативними підрозділами НПУ;

2) за вжиття оперативно-розшукових заходів у межах оперативно-розшукових справ.

Поряд із обліками спеціального призначення, які формують і використовують оперативні підрозділи Національної поліції, створені обліки загального користування, які ведуть слідчі, криміналістичні підрозділи, сервісні центри, поліція охорони тощо.

Підрозділи інформаційно-аналітичної підтримки НПУ здійснюють формування, супроводження та використання у службовій діяльності інформаційних ресурсів (обліків), держателем (власником) яких є МВС України, зокрема:

***Інформаційна підсистема «Оперативно-довідкова картотека» («ОДК») єдиної інформаційної системи МВС***

[483] Про затвердження Положення про автоматизовану інформаційну систему оперативного призначення єдиної інформаційної системи МВС: наказ МВС України від 20 жовтня 2017 р. № 870.

***України***[484]. ІП «ОДК» містить відомості про осіб: які засуджені судами до будь-якого покарання за вчинене кримінальне правопорушення; які підозрюються в учиненні кримінального правопорушення; інформація стосовно яких знаходиться в архівних кримінальних справах, що зберігаються в Центральному державному архіві, обласних державних архівах України, галузевих державних архівах МВС України, СБУ, а також громадян України, засуджених судами інших держав.

***Автоматизована дактилоскопічна ідентифікаційна система «Дакто-2000»*** – автоматизований облік дактилоскопічних карт осіб, затриманих за підозрою в учиненні правопорушень, людей, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе та невпізнаних трупів.

***ІП «Пізнання»*** – автоматизований облік інформації, зокрема біометричних даних щодо осіб, які переховуються від органів влади, безвісти зниклих осіб, невпізнаних трупів і людей, які не можуть надати про себе будь-яку інформацію.

***ІП «Затримані і доставлені»*** – автоматизований облік осіб, затриманих і доставлених до територіальних органів (підрозділів) поліції за підозрою в учиненні правопорушень і надання таким особам безоплатної вторинної правової допомоги (затримані на підставі ст. 208 КПК України; ухвали слідчого судді, суду; у зв'язку з розшуком; на підставі ст. 260 КУпАП (адміністративне затримання); постанови суду «адмінарешт»)[485].

***Єдиний реєстр досудових розслідувань*** – це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних, які використовуються для формування звітності, а також надання інформації про відомо-

---

[484] Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковський. Київ, 2017. 36 с.

[485] Оперативно-розшукова діяльність: посібник для вищих навчальних закладів. Київ: «Видавництво Людмила», 2019. 240 с.

сті, внесені до Реєстру, з дотриманням вимог кримінального процесуального законодавства та законодавства, яким урегульовано питання із захисту персональних даних і доступу до інформації з обмеженим доступом.

Реєстр утворений та ведеться відповідно до вимог КПК України з метою забезпечення: реєстрації кримінальних правопорушень (проваджень) та обліку прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження; оперативного контролю за додержанням законів під час проведення досудового розслідування; аналізу стану та структури кримінальних правопорушень, учинених у державі; інформаційно-аналітичного забезпечення правоохоронних органів[486].

***Національна автоматизована інформаційна система Єдиного державного реєстру Міністерства внутрішніх справ стосовно зареєстрованих транспортних засобів та їх власників («НАІС ЄДР МВС»)***[487]. НАІС ЄДР МВС призначена для отримання інформації про зареєстровані транспортні засоби та їх власників.

Органи та підрозділи Національної поліції здійснюють пошук у Реєстрі відомостей про зареєстровані транспортні засоби та їх власників відповідно до Порядку ведення Реєстру, щонайменше за одним із таких критеріїв:

– прізвище, ім'я, по батькові (за наявності) власника та дата його народження;

– реєстраційний номер облікової картки платника податків або серія та номер паспорта власника (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника

[486] Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань: наказ ГПУ від 06.04.2016 № 139, зареєстрований в Міністерстві юстиції України 05 травня 2016 р. за № 680/28810.

[487] Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковський. Київ, 2017. 36 с.

податків і повідомили про це відповідному контролюючому органу і мають позначку в паспорті про право здійснювати платежі за серією та номером паспорта);

– повне найменування юридичної особи;

– ідентифікаційний код юридичної особи в Єдиному державному реєстрі підприємств та організацій України (код згідно з ЄДРПОУ);

– номерний знак запитуваного транспортного засобу.

Крім зазначених, також можуть застосовуватися інші критерії пошуку, відповідно до повноважень користувача, визначених законом.

***Криміналістичні обліки МВС України.*** Обліки складаються з оперативно-пошукових та інформаційно-довідкових колекцій. В експертно-криміналістичних підрозділах ведуться ручні або автоматизовані картотеки: фотознімків (колекцій) відбитків пальців рук, слідів взуття, транспортних засобів, знарядь учинення злочинів, мікрочасток, вилучених із місць подій; гільз, куль, набоїв, підроблених грошових знаків, документів, медичних рецептів на наркотичні та сильнодіючі лікарські препарати тощо.

*Оперативно-пошукові колекції* призначені для отримання інформації про особу, яка причетна до вчинення злочину; ідентифікації особи, знаряддя злочину (транспортного засобу, зброї, обладнання тощо, які використовувалися під час учинення злочину); установлення спільної родової (групової) належності матеріалів і речовин; інших фактичних даних, які свідчать про вчинення злочинів конкретною особою; отримання іншої інформації щодо вчинених злочинів та запобігання їм.

*Інформаційно-довідкові колекції* призначені для використання об’єктів, уміщених до них, під час проведення експертних досліджень, створення науково-дослідних і дослідно-конструкторських розробок, оновлення методичної та нормативної бази судової експертизи, підготовки орієнтовної інформації, узагальнення відомостей про причини й умови вчинення злочинів та інших правопорушень з метою запобігання їм.

*Криміналістичні обліки* охоплюють такі їх види: трасологічний; дактилоскопічний; балістичний; холодної зброї; грошових знаків, бланків документів, цінних паперів і пластикових платіжних карток; осіб за ознаками зовнішності; вибухотехнічний; пожежно-технічний; наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів; генетичних ознак людини; записів голосів і мовлення осіб; ідентифікаційних позначень транспортних засобів і реквізитів документів (підписів, печаток, штампів); матеріалів, речовин і виробів[488].

Національна поліція має безпосередній оперативний доступ до інформації та інформаційних ресурсів інших органів державної влади за обов'язковим дотриманням Закону України «Про захист персональних даних», зокрема:

*1) Державної прикордонної служби* (***Інтегрована міжвідомча автоматизована система обміну інформацією з питань контролю осіб, транспортних засобів і вантажів, які перетинають державний кордон «Аркан»***) щодо:

– громадян України, іноземців та осіб без громадянства, зареєстрованих у пунктах пропуску через державний кордон;

– осіб, затриманих за порушення вимог законодавства про державний кордон;

– осіб, яким заборонено в'їзд в Україну;

– іноземців та осіб без громадянства, зокрема тих, яким оформлено посвідку на постійне проживання в Україні;

– транспортних засобів, що перетнули державний кордон;

– документів, що дають право на в'їзд до та виїзд із України;

*2) Державної міграційної служби* щодо:

– реєстрації місця проживання або місця перебування особи;

[488] Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковський. Київ, 2017. 36 с.

– документів, що посвідчують особу, підтверджують громадянство України або спеціальний статус особи;

– імміграції в Україну;

– осіб, які отримали або претендували на отримання статусу біженця чи особи, яка потребує додаткового захисту, осіб, які набули (припинили) громадянство України, та осіб, яким надано (скасовано) дозвіл на імміграцію в Україну.

Організація доступу до інформаційних ресурсів МВС, ДМС та Держприкордонслужби визначається Порядком організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України, затвердженим наказом МВС від 26 вересня 2013 р. № 920, зареєстрованим у Міністерстві юстиції України 16 жовтня 2013 р. за № 1771/24303[489].

Органи Національної поліції, відповідно до покладених на них завдань і повноважень, передбачених законом, в обсягах і порядку, встановлених законодавством і підзаконними міжвідомчими нормативно-правовими актами МВС України та держателів відповідних реєстрів, можуть використовувати інформацію:

– Державного реєстру фізичних осіб-платників податків;

– Єдиного державного реєстру нормативно-правових актів;

– Єдиного реєстру громадських формувань;

– Єдиного державного демографічного реєстру;

– Державного реєстру актів цивільного стану громадян;

– Єдиного реєстру нотаріусів;

– Єдиного реєстру довіреностей;

– Єдиного реєстру спеціальних бланків нотаріальних документів;

---

[489] Порядок організації доступу до інформаційних ресурсів під час інформаційної взаємодії між Міністерством внутрішніх справ України, Державною міграційною службою України та Державною прикордонною службою України: наказ МВС від 26 вересня 2013 р. № 920, зареєстрований у Міністерстві юстиції України 16 жовтня 2013 р. за № 1771/24303.

– Державного реєстру атестованих судових експертів;

– Державного реєстру обтяжень рухомого майна;

– Єдиного державного реєстру юридичних осіб і фізичних осіб-підприємців;

– Єдиного державного реєстру осіб, які вчинили корупційні правопорушення;

– Єдиного державного реєстру осіб, щодо яких застосовано положення Закону України «Про очищення влади»;

– Єдиного реєстру підприємств, щодо яких порушено провадження у справі про банкрутство;

– Єдиного державного реєстру виконавчих проваджень;

– Державного реєстру речових прав на нерухоме майно;

– Державного реєстру друкованих засобів масової інформації та інформаційних агентств як суб'єктів інформаційної діяльності;

– Єдиного державного реєстру судових рішень;

– Єдиного реєстру досудових розслідувань;

– Єдиного державного реєстру підприємств та організацій України;

– Державного реєстру виборців;

– Реєстру позичальників;

– Реєстру документів дозвільного характеру;

– Реєстру громадських об'єднань;

– Реєстру методик проведення судових експертиз;

– Спадкового реєстру;

– Електронного реєстру апостилів;

– Єдиного ліцензійного реєстру;

– Єдиного державного реєстру декларацій осіб, уповноважених на виконання функцій держави або місцевого самоврядування[490].

[490] Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: методичні рекомендації / В. Г. Хахановський, Д. В. Дабіжа, В. В. Пясковський. Київ, 2017. 36 с.

## 3.3. Використання інформаційних ресурсів Інтерполу та Європолу у розслідуванні злочинів

***Банки даних Інтерполу***

Використання банків даних Інтерполу є однією із форм міжнародного поліцейського співробітництва. Банки даних Генерального секретаріату Інтерполу створені з метою забезпечення всебічної взаємодії правоохоронних органів держав-членів Інтерполу. Формування банків даних Інтерполу здійснюється за рахунок інформації, яку надають правоохоронні органи держав-членів Інтерполу на добровільних засадах. Право власності на цю інформацію належить винятково тим державам, які її надали.

У Генеральному секретаріаті Інтерполу створені та функціонують такі банки даних:

1. *Банк даних «Особи»* (ASF Nominal database) – містить інформацію про осіб, які розшукуються за вчинення злочинів, безвісти зниклих, осіб, які підлягають ідентифікації, зокрема невпізнані трупи та ін.

Крім того, Генеральний секретаріат за допомогою системи I-24/7 надає доступ до банку даних циркулярних повідомлень Інтерполу.

Циркулярні повідомлення Інтерполу (картки Інтерполу) запроваджені у 1946 році з метою організації міжнародного розшуку злочинців, осіб зниклих безвісти, ідентифікації невпізнаних трупів тощо.

Картки (циркулярні повідомлення) поділяються на такі категорії:

– *«розшукується»* («червоні картки» або «повідомлення з червоним кутом») – виставляються на злочинців, які підлягають арешту з подальшою видачею країні-ініціатору розшуку. Ці повідомлення містять повний текст ордеру (санкції) на арешт і детальний опис учиненого злочину;

– *«встановлення місцезнаходження»* («блакитні картки») – виставляються для збору інформації про зазначену в них особу, а саме – про її місцеперебування тощо;

– *«попередження»* («зелені картки») – інформують про «професійних» злочинців, які діють на території кількох країн;

– *«невпізнаний труп»* («чорні картки») – містять детальний опис знайдених трупів, а також, у разі їх наявності, відбитки пальців;

– *«зниклий безвісти»* («жовті картки») – містять інформацію про осіб, зниклих безвісти.

У зазначеному банку даних міститься інформація про усі зазначені циркулярні повідомлення в електронному вигляді.

Крім того, система I-24/7 надає змогу безпосередньо в режимі реального часу формувати та надсилати запит про поширення циркулярних повідомлень.

2. *Банк даних викрадених транспортних засобів* (ASF Stolen vehicles database) – містить інформацію про транспортні засоби, викрадені на території держав-членів Інтерполу.

3. *Банк даних викрадених/втрачених документів* (ASF Stolen/Lost Travel Documents and Stolen Administrative Blank Documents Database) – містить інформацію про викрадені/втрачені ідентифікаційні документи, а також викрадені/втрачені бланки адміністративних документів.

У разі викрадення або втрати значної кількості бланків документів суворої звітності може також указуватись діапазон їх номерів.

4. *Банк даних викрадених творів мистецтва* (ASF Stolen Works of Art) – містить інформацію про твори мистецтва, предмети антикваріату, інші культурні цінності, викрадені на території держав-членів Інтерполу.

Щодо предметів антикваріату також указується матеріал, із якого виготовлений предмет.

5. *Банк даних ДНК-профілів* (DNA Profiles Database) – містить інформацію про ДНК, вилучені з місць учинення злочинів на території держав-членів Інтерполу та від злочинців.

6. *Банк даних відбитків пальців рук* (Fingerprints Database) – містить відбитки пальців рук, вилучені з місць учинення злочинів на території держав-членів Інтерполу та від злочинців.

7. *Банк даних порнографічних зображень, створених із залученням неповнолітніх* (INTERPOL Child Abuse Image Database), дає змогу ідентифікувати зображення порнографічного характеру за «авторством» і місцем розміщення в мережі Інтернет.

8. *Банк даних підроблених платіжних карток* (Counterfeit Payment Cards Database) – містить зображення підроблених платіжних карток та їх елементів (лицьової та зворотної сторін, емблем, голограм, підписів власників тощо) та іншу релевантну інформацію стосовно підроблення платіжних карток.

Отримання інформації або перевірка тих чи інших відомостей за банками даних Інтерполу здійснюється:

– *безпосередньо*, в режимі on-line – через телекомунікаційну систему Інтерполу I-24/7 (банки даних щодо осіб, транспортних засобів, документів, творів мистецтва);

– *шляхом надсилання запиту* до Генерального секретаріату Інтерполу (банки даних ДНК, порнографічних зображень, відбитків пальців).

Для забезпечення цільового використання правоохоронними органами держав-членів банків даних Інтерполу, їх функціонування організовано так, що країна-власник інформації щодо об'єкта, розміщеного в банку даних Інтерполу, автоматично отримує повідомлення про факт перевірки цього об'єкта іншою державою (відповідно національним центральним бюро Інтерполу, певним правоохоронним органом тощо). Отримання такого повідомлення для країни-власника інформації є підставою звернутись до країни, що перевіряла об'єкт у банку даних, для з'ясування підстав проведення відповідної перевірки, запитування відомостей про місцезнаходження об'єкта тощо.

Використання можливостей Укрбюро Інтерполу для отримання інформації з банків даних Генерального секретаріату Інтерполу здійснюється згідно з Інструкцією про

порядок використання правоохоронними органами можливостей Укрбюро Інтерполу в Україні у попередженні, розкритті та розслідування злочинів, затвердженою наказом МВС, ГПУ, СБУ, Держкомітету у справах охорони державного кордону, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2[491].

Підставою для направлення такого запиту можуть бути матеріали кримінального провадження, оперативно-розшукова справа, матеріали перевірки тощо.

У більшості випадків перевірки здійснюються за банками даних розшукуваних осіб і викрадених транспортних засобів.

Переважна кількість перевірок за банком даних розшукуваних осіб здійснюється згідно з Порядком провадження за заявами про надання дозволу на імміграцію і поданнями про його скасування та виконання прийнятих рішень, затвердженим постановою Кабінету Міністрів України від 26 грудня 2002 р. № 1983[492].

Інформація банку даних Генерального секретаріату Інтерполу викрадених транспортних засобів міститься у відповідних автоматизованих інформаційно-пошукових системах МВС України.

Перевірки за вказаним банком даних через Укрбюро Інтерполу здійснюються в основному територіальними органами поліції під час проведення перевірок за фактами виявлення розшукуваних автомобілів у порядку, передбаченому Інструкцією про порядок здійснення підрозділами Державтоінспекції МВС державної реєстрації, перереєстрації та обліку транспортних засобів, оформлення і видачі реєстраційних до-

[491] Інструкція про порядок використання правоохоронними органами можливостей Укрбюро Інтерполу в Україні у попередженні, розкритті та розслідування злочинів, затверджена наказом МВС, ГПУ, СБУ, Держкомітету у справах охорони державного кордону, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2.

[492] Порядок провадження за заявами про надання дозволу на імміграцію і поданнями про його скасування та виконання прийнятих рішень, затверджений постановою Кабінету Міністрів України від 26 грудня 2002 р. № 1983.

ументів, номерних знаків на них, затвердженою наказом МВС від 11 серпня 2010 р. № 379 (зі змінами)[493].

***Банки даних Європолу***

14 грудня 2016 року Міністр внутрішніх справ України А. Аваков і директор Європолу Р. Вайнрайт підписали оперативну та стратегічну угоду щодо розширення співробітництва у боротьбі з транскордонною злочинною діяльністю, яка була ратифікована Верховною Радою України 12 липня 2017 року.

Україна створила національний контактний пункт, який слугує центральним пунктом обміну інформацією між Європолом і правоохоронними органами України. Крім того, в МВС установлено спеціальний захищений канал зв'язку «SIENA» для обміну інформацією з Європолом[494].

Безпечна мережева програма обміну інформації *SIENA (Secure Information Exchange Network Application)* дозволяє швидко та зручно обмінюватися оперативною та стратегічною інформацією, пов'язаною зі злочинністю, між:

– офіцерами зв'язку Європолу, аналітиками, експертами;

– країнами-учасницями ЄС;

– третіми країнами, які мають відповідні угоди з Європолом[495].

Взаємодія має покривати всі види злочинності, що охоплюються мандатом Європолу та які зазначені в Додатку № 1 (Chapter I – Scope; Article 3).

Компетенція Європолу поширюється на боротьбу з організованою злочинністю, тероризмом та іншими видами тяжких злочинів.

---

[493] Інструкція про порядок здійснення підрозділами Державтоінспекції МВС державної реєстрації, перереєстрації та обліку транспортних засобів, оформлення і видачі реєстраційних документів, номерних знаків на них: наказ МВС від 11 серпня 2010 р. № 379 (із змінами).

[494] Пояснювальна записка до проекту Закону України «Про ратифікацію Меморандуму про взаєморозуміння між Україною та Європейським поліцейським офісом щодо встановлення захищеної лінії зв'язку». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=55374&pf3540

[495] Там само.

Напрями співробітництва між Європолом та учасниками Угоди передбачені ст. 4 Угоди, зокрема:

1) *обмін інформацією* (спеціальними знаннями; загальними зведеннями; результатами стратегічного аналізу; інформацією щодо процедур кримінальних розслідувань; інформацією про методи запобігання злочинності);

2) *участь у навчальних заходах*;

3) *надання консультацій та підтримки* в окремих кримінальних розслідуваннях.

***FIU.net*** – це спеціалізована комп'ютерна мережа, що підтримує підрозділи фінансової розвідки в ЄС у боротьбі з відмиванням коштів і фінансування тероризму. У січні 2016 року FIU.net була об'єднана з Європолом. Посилення взаємодії між фінансовою та кримінальною оперативною інформацією FIU.net в підсумку сприяє боротьбі з організованою злочинністю та тероризмом в ЄС.

Україна має статус спостерігача в CARIN. ***Мережа «КАРІН» (CARIN)*** – це Кемденська міжвідомча мережа з повернення активів (Європол):

• 53 юрисдикції і 9 міжнародних організацій;

• неофіційна мережа правоохоронних і судових органів;

• Центр експертизи з питань урегулювання проблем злочинності;

• надання допомоги у виявленні та заморожуванні злочинних активів;

• обмін інформацією й ефективними практиками.

CARIN може надавати допомогу правоохоронним органам і прокуратурі щодо: відстежування активів; заморожування та конфіскації активів; управління активами; розподілу активів; інформації про процедури в інших країнах[496].

[496] Презентація КМЄС: незаконне збагачення Маартен Гроотхайзен. URL: http://assetconf.antac.org.ua/wp-content/uploads/2016/12/Workshop_15_1_Mathias_ Illegal-Enrichment_UA.pptx

## 3.4. Використання кримінального аналізу в діяльності правоохоронних органів

У країнах Європейського Союзу, США та інших розвинених країнах світу використання можливостей кримінального аналізу є обов'язковим для всіх правоохоронних органів. Його зміст, правила та процедури чітко визначено й урегульовано в нормативно-правових актах. Це, зокрема, стосується ведення оперативно-розшукової діяльності, досудового розслідування та розгляду кримінальних проваджень у суді.

Стратегією розвитку органів системи Міністерства внутрішніх справ на період до 2020 року, схваленої розпорядженням Кабінету Міністрів України від 15 листопада 2017 року № 1023-р, передбачається, що одним із пріоритетів державної політики у сфері протидії злочинності є комплексне впровадження сучасних систем кримінального аналізу, зокрема методології Європолу з оцінки загроз тяжких злочинів та організованої злочинності (SOCTA)[497].

Консультативна місія Європейського Союзу в Україні (КМЄС) підтримує впровадження в Національній поліції України моделі поліцейської діяльності, керованої аналітикою (Intelligence-Led Policing / ILP). ILP є моделлю поліцейської діяльності, згідно з якою оперативно-аналітична інформація/intelligence слугує підставою для проведення операцій/розслідувань, а не навпаки. Ця модель дає змогу зменшити матеріальні витрати, знизити рівень злочинності, забезпечити більш високий рівень безпеки особового складу[498].

Окремі аспекти використання кримінального аналізу в діяльності правоохоронних органів розглядали у своїх

[497] Стратегія розвитку органів системи Міністерства внутрішніх справ на період до 2020 року: розпорядження Кабінету Міністрів України від 15 листопада 2017 року № 1023-р.

[498] J. G. Carter, S. W. Phillips, S. M. Gayadeen. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. *Journal of Criminal Justice*. 2014. № 42. P. 435.

наукових працях С. В. Албул, О. В. Власюк, І. М. Горбаньов, М. В. Гребенюк, О. М. Заєць, К. Ю. Ісмайлов, О. Є. Користін, А. В. Махнюк, В. В. Мельник, В. А. Некрасов, Г. К. Тетерятник, В. К. Швець, А. В. Холостенко, Д. Ю. Узлов, Дж. Картер, С. Філіпс, М. Гайадин, М. Яніцкі та інші автори[499].

***Кримінальний аналіз*** – це дії, спрямовані на ідентифікацію і точне визначення взаємозв'язків між відомостями, які стосуються подій злочинного характеру, осіб, пов'язаних із ними, та даними, що походять із різних джерел, і їх використання правоохоронними органами і судами.

[499] Основи кримінального аналізу: посіб. з елементами тренінгу / О. Є. Користін, С. В. Албул, А. В. Холостенко та ін. Одеса: ОДУВС, 2016. 112 с.; Власюк О. В. Роль і місце кримінального аналізу у розкритті та розслідуванні злочинів на державному кордоні України. *Матеріали постійно діючого науково-практичного семінару.* Харків: Інститут підготовки юрид. кадрів для СБУ Нац. юрид. акад. України ім. Я. Мудрого, 2011. Вип. 3. Ч. 1. С. 82–85.; Заєць О. М. Інститут аналітичного супроводження досудового розслідування кримінального провадження в Україні. Сучасний стан і перспективи розвитку. *Вісник кримінального судочинства.* 2016. № 4. С. 17–25; Гребенюк М. В., Швець В. К. Проблеми використання кримінального аналізу оперативними підрозділами правоохоронних органів у протидії організованій злочинності. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності*: тези III Всеукр. науково-практ. конф. (Хмельницький, 1 березня 2019 року). Хмельницький: Вид-во НАДПСУ, 2019. С. 616-619; Махнюк А. В. Теоретичні основи провадження кримінального аналізу у сфері правоохоронної діяльності. *Науковий вісник Державної прикордонної служби*. 2011. № 94. С. 3–7; Некрасов В. А. Сучасне розуміння кримінальної розвідки як напряму діяльності правоохоронних органів. *Кримінальна розвідка: методологія, законодавство, зарубіжний досвід:* матер. Міжнар. наук.-практ. конф. (м. Одеса, 29 квіт. 2016 р.). Одеса: ОДУВС, 2016. С. 19–20; Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования. Д. Ю. Узлов, В. М. Струков, О. Б. Григорович та ін. *Право і безпека*. 2015. № 2 (57). С. 132–139; J. G. Carter, S. W. Phillips, S. M. Gayadeen. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. *Journal of Criminal Justice*. 2014. № 42. P. 433–442; Яніцкі М. Оперативний кримінальний аналіз. *Міжнародна організація з міграції*. Київ, 2009. 86 с.

*До головних завдань кримінального аналізу слід віднести:*

1) якісне планування окремої слідчої (розшукової) дії, допомога у прийнятті управлінського рішення (ILP);

2) аналітичне супроводження ОРД і досудового розслідування;

3) аналіз стану та ефективності досудового розслідування, оперативно-розшукової та превентивної діяльності (тактичний аналіз);

4) оброблення великого обсягу інформації (bigDATA) з метою досягнення можливості відстеження та пов'язування фактів (застосування спеціальних аналітичних методів);

5) аналіз складної і розгалуженої структури зв'язків між об'єктами оперативно-розшукової справи або матеріалами кримінального провадження;

6) виявлення ризиків, тенденцій майбутнього розвитку злочинності та її запобігання з урахуванням аналітичних рекомендацій;

7) вирішення масштабних, довгострокових проблем і постановка цілей, для виявлення тенденцій у злочинному світі;

8) напрацювання нових напрямів у досудовому розслідуванні, а також отримання повноцінного аналітичного продукту щодо об'єктів кримінального аналізу;

9) прогнозування розвитку видів злочинної діяльності і встановлення пріоритетів діяльності НПУ та інших суб'єктів правоохоронної діяльності;

10) аналіз інформації, з метою виявлення тенденцій, закономірностей, а також прогнозування розвитку ситуації на тривалий період часу (стратегічний аналіз).

Систему кримінального аналізу в правоохоронних органах можна розділити на два основні напрями:

– *аналіз злочинності*, її причин і умов, особистості тих, хто скоює злочини, а також методів контролю за злочинністю та протидії їй;

– *аналіз злочинів*, механізм їх відображення в джерелах інформації, діяльність із розкриття, розслідування та попередження всіх видів злочинів і розроблення на цій основі найбільш ефективних методів і засобів розкриття злочинів.

Слід зазначити, що Міжнародна асоціація працівників кримінального аналізу розмежовує аналіз злочинів і кримінальний аналіз. «Якщо ми аналізуємо злочинця, це звужує коло діяльності», – підкреслює старший радник з питань загальної правоохоронної діяльності представництва КМЄС в Україні Георгіос Покас[500].

Під час кримінального аналізу забезпечується цілеспрямований пошук, виявлення, фіксація, вилучення, упорядкування, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація.

Зокрема, в аналітичній роботі використовується:

• *оперативний аналіз* (аналіз даних телефонних дзвінків, аналіз злочинних угруповань, аналіз справ, порівняльний аналіз);

• *тактичний аналіз* (кримінальний аналіз, аналіз кримінальних тенденцій, геопросторовий аналіз, аналіз місць концентрації злочинності, часовий аналіз, МО-аналіз, кримінальні моделі, профілі підозрюваних/жертв);

• *стратегічний аналіз* (SWOT-аналіз, PEST-аналіз, аналіз моделей/форм злочинності та профілювання, аналіз тенденцій, аналіз із використанням географічного профілювання).

За джерелами даних аналіз розподіляється на:

– *аналіз даних із відкритих джерел* (OSINT);

– *аналіз даних із агентурних джерел* (HUMINT);

– *аналіз даних радіотехнічної розвідки* (SIGINT);

– *аналіз даних із багатьох джерел* (Multi-Source Analysis) тощо.

Система кримінального аналізу в правоохоронних органах вирізняє кілька рівнів, для кожного з яких характерна мета, відповідні види і обсяги вихідної інформації, що підлягають збору, вивченню та оцінці, зокрема:

1) *національний* (загальнодержавний);

[500] В ОДУВС обговорили сучасний стан та перспективи розвитку кримінального аналізу. URL: http://oduvs.edu.ua/news/v-oduvs-obgovorili-suchasnij-stan-ta-perspektivi-rozvitku-kriminalnogo-analizu/?fbclid=IwAR2t1maJ Kq2WkztWEU-Wb_qnxjF2etHx4nd75HF3MJsVP9YVuQYvfPWleMA

2) *регіональний* (районний);

3) *місцевий.*

*Кримінальний аналіз на національному рівні* передбачає спостереження і прогнозування на тривалі терміни еволюції кримінальної ситуації на державному рівні (географічні зони, види і типи дій) і розроблення на цій основі перспективних заходів щодо їх можливої нейтралізації, зміцнення правопорядку та вдосконалення діяльності правоохоронних органів на тривалий термін.

Період, що аналізується на національному рівні, становить не менше одного року, а рекомендації аналітиків розраховані на термін до 3–5 років.

*Кримінальний аналіз на регіональному рівні* є комплексним аналізом оперативної обстановки за короткі, середні і тривалі терміни (квартал, півріччя, дев'ять місяців, рік) у певних географічних районах.

Метою аналізу інформації на оперативному рівні є виявлення змін у стані правопорядку і спрямування діяльності керівництва за всіма рівнями ухвалення рішень (місцевий, регіональний і національний) щодо ефективного розподілу організаційних ресурсів, розстановки сил і засобів, розробки комплексних заходів і прийняття рішення щодо посилення боротьби з найбільш поширеними і небезпечними правопорушеннями.

Зазвичай час для аналізу на регіональному рівні визначається на основі оцінки добової, декадної і місячної інформації, не перевищуючи одного року.

*На місцевому рівні кримінальний аналіз* здійснюється відразу після отримання даних/інформації про настання події або про ті події, які можуть відбутися найближчим часом, і у складних кримінальних провадженнях.

Роль такого аналізу полягає в направленні і підтриманні інформаційних знань із метою виявлення кримінальних об'єктів (осіб, груп, організацій), відносин між ними, злочинних діянь, тактики дій, а також їх становища.

Результати аналізу на тактичному рівні (залежно від їх масштабу і можливості реалізації) використовуються

в прийнятті оперативних рішень, розстановці сил і засобів, за проведення різних комплексних, типових і разових операцій.

В. Мельник і В. Некрасов уважають, що для сфери кримінального аналізу економічної злочинності більш притаманним є аналіз джерел інформації, що містяться у великих масивах даних, зокрема:

– у зазначених масивах здійснюється пошук певних незначних відхилень у господарському процесі, а також закономірностей, притаманних злочинним схемам і технологіям;

– інформація, що характеризує процеси в легальному секторі економіки, розпорошена різними масивами інформації, сформована на різних платформах та має різну інституційну належність;

– фінансові та господарські операції, що відображені в облікових і звітних документах, містять сліди інтелектуальних підробок. Саме тому необхідно проводити дослідження відповідності відомостей, що містяться у звітних документах із фактичною діяльністю;

– правоохоронні органи сьогодні не володіють методологією кримінального аналізу та аналізу ризиків щодо підозрілих фінансових і господарських операцій[501].

Слід зазначити, що, надаючи аналітикам змогу опрацьовувати дані про злочини, оперативні працівники та слідчі отримують можливість використовувати готовий оперативно-аналітичний продукт, а не первинну інформацію.

У цьому вони отримують такі переваги:

*по-перше*, окреслюються конкретно тенденції злочинності не лише за географічною ознакою, а й у часових рамках;

*по-друге*, продукт надає можливість мати більше інформації щодо місць ймовірного вчинення злочинів. Це допомагає покращити попередження правопорушень;

[501] Мельник В., Некрасов В. Як подолати ворога, багатшого за транснаціональні корпорації? URL: http://n-v.com.ua/yak-podolaty-vorogabagatshogo-za-korporatsyi/

*по-третє*, працівники поліції мають більше можливостей у разі потреби надати допомогу колегам у розкритті та розслідуванні злочинів.

Водночас підхід до поліцейської діяльності, керованої аналітикою, наражається на низку проблем на різних рівнях аналізу, зокрема:

– для оперативного аналізу дані часто недоступні ззовні підрозділу або робочої групи і прив'язані до оперативного працівника;

– для тактичного аналізу наявні інструменти дають широкі можливості для візуалізації, але інколи відчувається слабкість математичного апарату;

– для стратегічного аналізу дані часто відсутні через те, що їх ніхто не узагальнює для аналізу або аналіз проводиться лише з точки зору покращення звітності правоохоронного органу, при тому, що, скажімо, PEST-аналіз і SWOT-аналіз можна застосовувати для передбачення очікуваних змін у діяльності злочинних угруповань[502].

У системі НПУ є чимало джерел розрізненої інформації, яка аналізується співробітниками різних служб автономно. Приміром, у Департаменті карного розшуку аналізується інформація щодо загальнокримінальної злочинності, у Департаменті протидії наркозлочинності – інформація, пов'язана з наркозлочинами, у Департаменті стратегічних розслідувань – дані щодо організованої злочинності тощо.

Крім того, кожний оперативний працівник накопичує і зберігає власну оперативну інформацію, яка після його звільнення або переміщення по службі стає практично недоступною для інших оперативних працівників. Відтак немає можливості якісно оцінити інформацію в глобальному масштабі.

Держава витрачає кошти на отримання інформації, а в результаті ці дані втрачаються. Отож, порушується європейсь-

[502] A. V. Movchan and V. Yu. Taranukha. Constructing an Automation System to Implement Intelligence-Led Policing Into the National Police of Ukraine. *Cybernetics and Systems Analysis*, Vol. 54, No. 4, July, 2018. P. 643-649.

кий принцип про те, що інформація не належить конкретному поліцейському, інформація належить державі як один із продуктів діяльності поліції. Тому постає завдання із консолідації всієї оперативної інформації, її подальшого аналізу, що має сприяти розкриттю насамперед тяжких та особливо тяжких злочинів[503].

Більшість департаментів Національної поліції України в оперативно-службовій діяльності використовує такі джерела інформації, як *Інтегровану інформаційно-пошукову систему Національної поліції* (АРМОР) та *статистичну інформацію*, надану Департаментом інформаційно-аналітичної підтримки.

Можливості здійснення аналізу інформації з відкритих джерел (OSINT) у кожному підрозділі є різними, хоча мережа Інтернет є одним із найповніших джерел даних.

Найбільш поширеним аналітичним інструментом, що використовується у повсякденній роботі органів Національної поліції, є Microsoft Office (Word і Excel), хоча в деяких департаментах застосовується аналітичне програмне забезпечення (зокрема, i2 Analyst's Notebook, E-Gismaps, ArcGIS тощо)[504].

У 2017 році в структурі центрального апарату Національної поліції України створено *Управління кримінального аналізу*, яке має виконувати функцію координації діяльності у сфері аналізу і впровадження та розвитку моделі поліцейської діяльності, керованої аналітикою. У 2019 році Управління реорганізовано в Департамент кримінального аналізу.

Відповідно до наказу Національної поліції України від 29.12.2019 № 1354 «Про затвердження Положення про Департамент кримінального аналізу Національної поліції України», Департамент кримінального аналізу (ДКА) розробляє, впроваджує та застосовує нові методи та напрями здійснення кримі-

[503] Єрофєєв В. Кримінальний аналіз – це ефективна робота поліції та безпека громадян. URL: http://mvs.gov.ua/ua/news/10309_Kriminalniy_analiz_ce_efektivna_robota_policii_ta_bezpeka_gromadyan_FOTO.htm

[504] Intelligence-Led Policing: the cutting edge of modern law enforcement. URL: http://euam.php7.postbox.kiev.ua/ua/news/ opinion/intelligence-led-policing-the-cutting-edge-of-modern-law-enforcement/ (in Ukrainian).

нального аналізу, спрямовані на підвищення ефективності протидії злочинності[505].

ДКА є уповноваженим структурним підрозділом НПУ з проведення, організації та координації інформаційно-пошукової та аналітичної роботи, спрямованої на збір, оцінку та реалізацію інформації, зокрема інформації з обмеженим доступом, шляхом надання її уповноваженим органам (підрозділам) для вжиття заходів відповідно до їх компетенції, оцінювання ризиків, а також використання її для забезпечення виконання функцій, покладених на поліцію.

Основними завданнями ДКА є:

1) організація та здійснення інформаційно-аналітичної діяльності для реалізації повноважень поліції;

2) визначення стратегічних напрямів роботи, шляхів розвитку кримінального аналізу в діяльності органів та підрозділів поліції;

3) забезпечення взаємодії та координації діяльності органів (підрозділів) поліції у сфері кримінального аналізу, а також збір, обробка, узагальнення та аналіз інформації з метою протидії злочинності;

4) забезпечення формування та підтримка функціонування автоматизованих інформаційних систем, що утворюються в процесі здійснення оперативно-розшукової та аналітичної діяльності;

5) у межах компетенції, відповідно до вимог міжнародного та вітчизняного законодавства, участь у здійсненні інформаційної взаємодії з правоохоронними органами іноземних держав і міжнародними організаціями.

Суттєвим аспектом кримінального аналізу є аналіз географічних даних. У нинішніх умовах географічні дані є джерелом цінної інформації на кожному рівні роботи правоохоронних органів. Розвиток цього напрямку аналізу передбачає наяв-

[505] Про затвердження Положення про Департамент кримінального аналізу Національної поліції України: наказ Національної поліції України від 29.12.2019 № 1354.

ність спеціалістів-аналітиків, які зможуть здійснити оцінку даних на базі *географічних інформаційних систем* (GIS) для оперативних підрозділів.

Зокрема, з метою профілактики й оперативного реагування на злочини аналітики Департаменту кримінального аналізу запроваджують географічну прив'язку до кожного житлового будинку, з можливістю нанесення інформації на карту. Це уможливлює виконання якісного аналізу скоєних правопорушень, визначення зони вчинення злочинів, скеровування в такі місця додаткових нарядів патрульної поліції та надання завдання дільничному офіцеру поліції щодо повторного відпрацювання місць проживання осіб, які перебувають під адміністративним наглядом[506].

Серед методик аналізу оперативної інформації, які застосовують правоохоронні органи більшості розвинених країн світу, найбільш часто використовуються програмні продукти i2 і ANACAPA. Такі програмні рішення візуального аналізу даних і отримання нових знань призначені для оперативних підрозділів і слідчих, чия діяльність пов'язана з необхідністю аналітичної обробки інформаційних потоків і даних, представлених у різних форматах.

Зокрема, *програмний продукт i2* становить комп'ютерне програмне забезпечення на базі SQL-server, покликане узагальнювати, аналізувати, висувати ймовірнісні зв'язки, а також візуалізувати в реальному часі обмін інформацією. Це програмне забезпечення є сукупністю сумісних між собою різних програм, що виконують відповідні специфічні функції на всіх етапах розкриття і розслідування злочинів.

Аналітична лінія продуктів i2 представлена елементами, які здатні вирішувати більшість аналітичних завдань як окремо, так і в різній комбінації (зокрема, Analyst's Notebook, Analyst's Notebook-Esri® Edition, Analyst's Workstation, iBase, iBase IntelliShare, iXv Visualizer, iBridge, iXa, TextChart,

[506] Єрофєєв В. Кримінальний аналіз – це ефективна робота поліції та безпека громадян. URL: http://mvs.gov.ua/ua/news/10309_Kriminalniy_analiz_ce_efektivna_robota_policii_ta_bezpeka_gromadyan_FOTO.htm

ChartReader, PatternTracer). У сфері кримінального аналізу i2 зазвичай застосовується із програмними продуктами iBase, iBridge, iGlass, Analyst's Workstation.

Серед користувачів цієї операційної аналітичної системи можна вирізнити правоохоронні органи США та Канади (ФБР, ЦРУ, DEA, NSA, RCMP), правоохоронні органи країн Євросоюзу, Інтерпол та Європол[507].

Недоліками цієї лінійки продуктів є значна слабкість підсистем, орієнтованих на обробку текстової інформації мовами, що не належать до романо-германської групи, та слабкість математичного апарату.

Так, i2 TextChart підтримує ефективне виділення та об'єднання сутностей лише для англійської мови, а низка функцій доступні лише для англійської, французької, німецької, іспанської та італійської мов, а засоби обробки кириличних текстів вельми примітивні[508].

Продукт i2 PatternTracer орієнтований найперше на обробку телефонних дзвінків, задля віднаходження кластерів, що відповідають специфічній активності та для виділення ключових учасників. Аналіз інших, зокрема різнорідних, часових послідовностей не підтримується.

Програмний продукт компанії «Anacapa Sciences Inc.» утворює передову методику розслідування злочинів й аналізу оперативної інформації. ANACAPA опинилася біля витоків розробки спеціальних аналітичних методик для сфери безпеки і ще 1971 року розпочала проведення навчальних курсів із підготовки фахівців-аналітиків.

Нині ANACAPA пропонує такі 4 базові курси:

1) аналіз інформації під час проведення розслідувань Criminal Intelligence Analysis (CIA);

2) аналітичні методи розслідування Analytical Investigation Methods (AIM);

---

[507] Возможности использования аналитических программ в борьбе с организованной преступностью. URL: https://articlekz.com/article/11838

[508] i2 TextChart. URL: http://www-01.ibm.com/support/docview.wss?uid=swg27027043(in English).

3) аналіз фінансових махінацій Financial Manipulation Analysis (FMA);

4) поглиблений аналіз із використанням комп'ютерних технологій Computer-Aided Analysis (CAA)[509].

Як і продукти лінійки i2, продукти ANACAPA надають зручні інструменти для багатьох важливих завдань, але нерозглянуті ті ж проблеми, а саме: підтримка лінгвістичних засобів аналізу документів для української та російської мов (включаючи, але не обмежуючись автоматичним здобуттям із них даних для аналізу та ключових фактів) і підтримка математичних засобів для аналізу взаємозв'язків того чи іншого виду між сутностями[510].

Крім того, потребують нагального вирішення такі проблеми:

1) забезпечення аналітиків доступом до спеціального аналітичного програмного забезпечення;

2) створення захищеної мережі для організації обміну інформацією в електронній формі;

3) створення ІТ-системи збирання та обробки оперативно-аналітичної інформації.

Цінним інструментом для виявлення підозрілої фінансової активності є аналітичне програмне забезпечення для судових бухгалтерів (Link Analysis Software for Forensic Accountants), яке поєднує спостереження за незвичайними цифровими фінансовими операціями, профілювання клієнтів та аналіз статистичних даних для визначення ймовірності протиправної поведінки[511].

Слід зазначити, що в Україні вже є приклади успішного використання сучасних інформаційно-аналітичних систем.

---

[509] About the company Anacapa Sciences Inc. URL: http://www.spi2.ru/about/partners/anacapa/

[510] A. V. Movchan and V. Yu. Taranukha. Constructing an Automation System to Implement Intelligence-Led Policing Into the National Police of Ukraine. *Cybernetics and Systems Analysis*, Vol. 54, No. 4, July, 2018. P. 643-649.

[511] Albrech C. C. Fraud and Forensic Accounting In a Digital Environment: White Paper for The Institute for Fraud Prevention. URL: http://www.theifp.org/research-grants/IFP-Whitepaper-4.pdf

Зокрема, в ГУНП у Харківській області розроблена та використовується «Інтелектуальна система кримінального аналізу у режимі реального часу» (Real-time Intelligence Crime Analytics System, RICAS).

Система RICAS забезпечує доступ до таких інформаційних ресурсів:

– інформація кримінального характеру та реєстрації подій;

– GPS-даних;

– даних про безвісти зниклих та осіб, що перебувають у розшуку;

– даних про осіб, які відбули покарання;

– державні реєстри тощо.

Крім того, система забезпечена доступом до камер відеоспостереження, встановлених у місті, в режимі реального часу[512].

Водночас, на думку експертів, невідомо, як аналітичні звіти, підготовлені з використанням системи RICAS, відповідатимуть стандартам і процедурам, передбаченим моделлю ILP. Ще однією проблемою може виявитись сумісність цієї системи з іншими системами.

Використання аналітичних програм в аналізі даних забезпечує чимало переваг, які допомагають підвищити ефективність і результативність роботи суб'єктів доказування. У процесі інтеграції інформації здійснюється її каталогізація та введення в систему контролю і пошуку інформації, яка дозволяє легко знаходити необхідні відомості та отримувати до них доступ. Програмні продукти – доволі гнучкі, пристосовані для зберігання вже зібраної інформації. Вони також можуть бути адаптовані до інтеграції додаткової інформації, яка надійде в майбутньому. Під час розслідування злочинів й аналізу інформації

[512] Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования / Д. Ю. Узлов, В. М. Струков, О. Б. Григорович та ін. *Право і безпека*. 2015. № 2 (57). С. 132-139.

в інформаційну систему можуть уводитися нові розділи та підрозділи. Ці програмні продукти здатні сприймати величезні обсяги інформації, забезпечені засобами безпеки для обмеження доступу до інформації, отриманої в процесі розслідування. Збір відомостей з декількох джерел підвищує ймовірність отримання ключової доказової інформації і забезпечує можливість підтвердження і перевірки достовірності відомостей. Інформація, отримана з різних каналів, допомагає співробітникам правоохоронних органів приймати відповідне рішення[513].

Доповнювати аналітичну діяльність має *кримінальна розвідка*, що надасть можливість отримати доступ до джерел інформації та слідів злочину, до яких немає вільного доступу або відсутня можливість отримати такий доступ у гласний спосіб.

Попри це, *шляхом кримінального аналізу* здійснюється:

– *визначення учасників* кримінальних схем, зв'язків, кількості та характеру контактів;

– *визначення джерел і напрямів* фінансових потоків, інших матеріальних об'єктів;

– *визначення механізму організації* злочинної діяльності, підґрунтя функціонування кримінального явища;

– *оцінка ризиків, загроз*, можливих збитків, уразливостей для ухвалення управлінських рішень.

Водночас *кримінальна розвідка* сприяє:

– *визначенню джерел* інформації та слідів злочину, до яких немає вільного доступу або відсутня можливість отримати такий доступ у гласний спосіб;

– *отриманню ґрунтовної інформації* про: об'єкт, стосовно якого є обґрунтовані підозри у причетності до злочину; ієрархічну побудову організованих злочинних угруповань, специфіку та характер їхньої діяльності, розгалужену кримінальну інфраструктуру;

---

[513] Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк: Управление Организации Объединенных Наций по наркотикам и преступности. Вена, 2010. С. 25. URL: https://www.unodc.org/pdf/ criminal_justice/10-52547_1_Policing_4_ebook.pdf.

– *нейтралізації діяльності* окремих організованих злочинних угруповань, руйнуванню кримінальних технологій[514].

Зважаючи на викладене, зазначимо, що *головною метою кримінального аналізу є зміцнення механізмів попередження, виявлення, документування та розслідування кримінальних правопорушень, а також налагодження механізмів моніторингу криміногенної ситуації, обміну інформацією на державному, регіональному і міжнародному рівнях стосовно тенденцій та ризиків у цій сфері.*

НПУ з урахуванням досвіду поліції інших країн планово запроваджує міжнародні стандарти управління інформацією у сфері запобігання правопорушенням і розслідування злочинів. Заходи з упровадження кримінального аналізу вживаються в межах реалізації відомчої програми одночасно зі створенням системи аналізу ризиків.

Для підготовки поліцейських аналітиків використовується досвід іноземних колег. Зокрема, підрозділ кримінального аналізу доволі успішно діє в поліції Румунії, працівники цього підрозділу сприяли впровадженню кримінального аналізу в поліції Польщі і Молдови. В Україні за підтримки КМЄС ними також проведено низку тренінгів.

Однак, найсучасніша техніка та новітні технології не в змозі розкривати злочини, якщо працівники поліції не будуть готові працювати з ними. Про це, зокрема, наголошувалось під час наради з керівниками закладів вищої освіти МВС, які здійснюють підготовку поліцейських: «У навчанні майбутніх поліцейських ми повинні рухатися до нової моделі підготовки працівників кримінального блоку. У вишах потрібно викладати дисципліну за фахом «кримінальний аналіз». Якщо електронними додатками користується увесь світ, то в Україні початкова інформація збирається старими способами. Це забирає час,

[514] Мельник В., Некрасов В. Як подолати ворога, багатшого за транснаціональні корпорації? URL: http://n-v.com.ua/yak-podolaty-vorogabagatshogo-za-korporatsyi/

тоді як іноземним правоохоронцям на збір необхідної інформації може знадобитися лише кілька діб»[515].

«Кримінальний аналіз – це не техніка, не програмне забезпечення – це люди, тому без кваліфікованих кадрів, кримінального аналітика, який розуміє, що робити і як інтерпретувати інформацію, неможливо досягти позитивних результатів», – зазначає Д. Пефтієв[516].

Підсумовуючи, зазначимо, що успішна реалізація та впровадження нових методів кримінального аналізу дасть змогу у майбутньому поширити їх на всю систему Національної поліції та активно використовувати сучасні аналітичні методи і прийоми, завдяки яким мона створити передумови для більш ефективного виконання оперативними і слідчими підрозділами своїх завдань, що, своєю чергою, сприятиме підвищенню ефективності протидії злочинності загалом.

Отже, впровадження інформаційно-аналітичних програм у діяльність правоохоронних органів доводить свою ефективність і тепер вони можуть бути успішно використані в роботі оперативних і слідчих підрозділів Національної поліції.

[515] Князєв С. У навчанні майбутніх поліцейських ми повинні рухатися до нової моделі підготовки. URL: https://www.npu.gov.ua/uk/publish/article/2168283

[516] В ОДУВС обговорили сучасний стан та перспективи розвитку кримінального аналізу. URL: http://oduvs.edu.ua/news/v-oduvs-obgovorili-suchasnij-stan-ta-perspektivi-rozvitku-kriminalnogo-analizu/?fbclid=IwAR2t1maJKq2WkztWEU-Wb_qnxjF2etHx4nd75HF3MJsVP9YVuQYvfPWleMA

# ВИСНОВКИ

Вирішення проблем щодо підвищення ефективності розкриття та розслідування злочинів у сучасних умовах безпосередньо залежить від розроблення та впровадження новітніх технологій та інновацій у правоохоронну діяльність, на що й спрямована наша монографія. Під час її написання нам удалося сформулювати низку нових наукових положень, рекомендацій та висновків, які мають теоретичне й практичне значення. Основні з них такі:

1. *Новітні технології у розслідуванні злочинів* – це сучасні, найновіші інноваційні методи, прийоми, технологічні процеси, програмні і технічні засоби, інструменти, які інтегровані з метою збирання, отримання, обробки, систематизації, аналізу, зберігання та використання криміналістичної, оперативної та процесуальної інформації, для алгоритмізації й оптимізації процесу розкриття і розслідування злочинів та їх судового розгляду, підвищення якості правозастосовної діяльності.

2. Вивчення наукового рівня криміналістичного забезпечення діяльності з розслідування злочинів, використання інноваційних досягнень сучасної науки і техніки свідчать про певне їх відставання від кримінальної практики застосування новітніх засобів, методів і технологій у злочинній діяльності. Особливо це проявляється у застосуванні злочинцями сучасних інформаційних технологій для вчинення злочинів на національному та міжнародному рівнях.

3. Упровадження інновацій в практику боротьби зі злочинністю сприяє оптимізуванню розслідування та уникненню слідчих помилок. Зокрема, заслуговує на увагу розроблення та використання у розслідуванні злочинів автоматизованих робочих місць слідчого (АРМ слідчого «Інсайт»), АРМ судових експертів різних експертних спеціальностей (АРМ трасолога, АРМ

баліста, АРМ економіста, АРМ фоноскопіста, АРМ дослідження об'єктів інтелектуальної власності тощо), АРМ судді, АРМ обробки та надсилання документів, АРМ секретаря судді, АРМ працівника підрозділу боротьби з наркозлочинністю, АРМ юриста, АРМ юриста-криміналога, АРМ прокурора.

4. *Інформаційні технології у розслідуванні злочинів* – це сукупність методів, технологічних процесів і програмно-технічних засобів, інтегрованих із метою збирання, обробки, систематизації, узагальнення, аналізу, зберігання та використання криміналістичної, оперативної та процесуальної інформації, а також обмеженого доступу, що має значення для вирішення завдань ОРД і досудового розслідування, забезпечення безпеки громадян, суспільства і держави.

5. Сьогодні новітні інформаційні технології ефективно використовуються для розслідування злочинів. Зокрема, вони дозволяють здійснювати фіксацію доказової інформації за допомогою цифрових засобів аудіозапису, відео- та фотозйомки, дистанційно (за допомогою дальномірів) вимірювати відстані між предметами під час огляду місця події та будувати плани і схеми місця події із залученням програмних засобів тощо.

6. Особливу роль у криміналістиці виконують спеціалізовані комп'ютерні системи ідентифікації людини – вони дають змогу отримувати й аналізувати за декількома взаємопов'язаними параметрами інформацію, що прямо чи опосередковано спроможна призвести до розкриття злочину. Зокрема, нещодавно значного поширення в діяльності правоохоронних органів набули інформаційно-пошукові системи біометричної ідентифікації особи.

7. Сучасний світ неможливо уявити без щохвилинного застосування користувачами пристроїв електронно-обчислювальної техніки, смартфонів, розумних годинників тощо. Саме тому працівники Національної поліції мають володіти актуальними знаннями щодо видів ЕОТ, особливостями її використання, наявністю можливостей зняття інформації з електронних інформаційних систем.

8. У нинішніх умовах злочинці активно використовують кіберпростір як місце вчинення протиправних діянь. У ньому, отже, й містяться сліди їхньої злочинної діяльності. Необхідність посилення боротьби зі злочинністю у кіберпросторі вимагає від правоохоронних органів розроблення та впровадження в практичну діяльність нових оперативно-розшукових заходів і методів, які б ураховували специфіку його функціонування.

9. Так, можна вирізнити такі можливості використання БпЛА правоохоронними структурами: запобігання терористичним актам; операції боротьби з організованою злочинністю; операції із затримання злочинців і розшуку зниклих людей; вивчення місця злочину; профілактичне відеоспостереження; контроль масових заходів і акцій протесту; забезпечення VIP-зустрічей, зокрема на найвищому рівні; підтримка оперативного зв'язку; запобігання нелегальній імміграції та контрабанді; спостереження за наземними і морськими лініями регулярних перевезень і транспортними потоками; аналіз причин ДТП; відстеження викрадених автомобілів; боротьба з морськими піратами; запобігання браконьєрству, незаконній розробці надр і незаконній вирубці лісів тощо.

10. *Інформаційно-аналітична робота у розслідуванні злочинів* – це передбачена законодавством України й урегульована відомчими нормативними актами система заходів, спрямованих на збір, обробку, узагальнення, аналіз, зберігання та використання інформації, зокрема обмеженого доступу, що має значення для вирішення завдань ОРД і досудового розслідування, в інтересах кримінального судочинства, безпеки громадян, суспільства і держави.

11. *Основними засобами* інформаційно-аналітичної роботи у розслідуванні злочинів є: оперативна та криміналістична техніка і спеціальні технічні засоби, призначені для гласного та негласного отримання інформації; відповідні апаратно-програмні комплекси (автоматизовані інформаційно-пошукові, експертні та логіко-аналітичні системи тощо) і різні технічні пристрої, за допомогою яких здійснюється обробка, системати-

зація та аналіз оперативно-розшукових та інших відомостей фактографічного та криміналістичного характеру.

12. Кримінальний аналіз є специфічним видом інформаційно-аналітичної діяльності правоохоронних органів, який полягає у перевірці та оцінці інформації, її інтерпретації, встановленні зв'язків між даними, що отримуються у процесі виявлення, припинення та розслідування злочинів і мають значення для ОРД й досудового розслідування, з метою їх використання правоохоронними органами і судом, подальшого проведення оперативного, тактичного та стратегічного аналізу. Успішна реалізація та впровадження нових методів кримінального аналізу дасть змогу у майбутньому активно використовувати сучасні аналітичні методи і прийоми, завдяки яким можна створити передумови для більш ефективного виконання оперативними і слідчими підрозділами своїх завдань. Це, своєю чергою, сприятиме підвищенню ефективності протидії злочинності загалом.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Автоматизовані системи. Терміни та визначення: ДСТУ 2226-93. Чинний від 1994-07-01. Київ: Держстандарт України, 1993. 91 с. (Національні стандарти України).
2. Агеев В. В., Агеева Е. В. К вопросу о поиске оперативно-розыскной информации в Интернете. *Криминологический журнал ОГУЭП.* Москва, 2011. № 1 (15). С. 65–70.
3. Аленін Ю. П. Теоретичні та практичні основи розкриття і розслідування осередків злочинів: автореф. дис. на здобуття наук. ступеня д-ра юрид. наук: 12.00.09. Харків, 1997. 48 с.
4. Анталогія сиску: в 14 т. / відп. ред. Ю. І. Римаренко, В. І. Кушерець; упоряд. Ю. І. Римаренко та ін. Київ: Знання України, 2005. Т. 1: Документи та матеріали з кримінального сиску (1397–1918 рр.), 2005. 596 с.
5. Бауэр Ф., Гооз Г. Информатика. Вводный курс: в 2-х ч. Москва: Мир, 1990. С. 18–19.
6. Бахин В. П. Криминалистика: проблемы и мнения (1962–2002 гг.). Киев: [б. и.], 2002. 266 с.
7. Белкин Р. С. История отечественной криминалистики. Москва: Норма, 1999. 496 с.
8. Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики. Москва: Инфра-М-НОРМА, 2001. 240 с.
9. Белкин Р. С. Криминалистическая энциклопедия: справ. пособие. Москва: БЕК, 1997. 334 с.
10. Белов О. А. Информационное обеспечение раскрытия и расследования преступлений: монография. Москва: Юрлитинформ, 2009. 136 с.
11. Берназ В. Д. Інновації – основа криміналістичного забезпечення діяльності з розслідування злочинів. *Південноукраїнський правничий часопис.* 2015. Вип. № 4. С. 49–53.
12. Берназ В. Д. Інтеграція досягнень сучасної науки в слідчу діяльність. *Південноукраїнський правничий часопис.* 2008. Вип. № 4. С. 189–191.
13. Бірюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: монографія. Луганськ: ЛДУВС, 2009. 664 с.
14. Благута Р. І. Заходи забезпечення кримінального провадження – інститут не новий, нові проблеми застосування. *Юридичний Вісник України.* 2013. № 27. С. 14–15.
15. Благута Р. І. Організація та підготовка до проведення негласних слідчих (розшукових) дій: проблеми та шляхи вирішення. *Науковий вісник Львівського державного університету внутрішніх справ.* 2013. № 1. С. 333–340.

16. Боер В. М., Павельева О. Г. Информационное право: учеб. пособие. Ч. 1: ГУАП. Санкт-Петербург, 2006. 116 с.

17. Бочковий О. В., Звонок Є. О. Віртуальні соціальні мережі як джерела оперативно значимої інформації для підрозділів карного розшуку МВС. URL: http://itcrime.at.ua/publ/pitannja_ord_ta_kriminalistiki/zbirnik_materialiv_konferenciji_u_khmelnicku_ 2010_roku/3-1-0-3

18. Брусиловский А. Е., Строгович М. С. Свидетельские показания в качестве судебных доказательств. Методика и техника следственной работы / под ред. Г. К. Рогатинского и А. В. Викторова. Киев: Советское строительство и право, 1934. 128 с.

19. Василинчук В. І. Оперативно-розшукова профілактика злочинів у бюджетній сфері: монографія. Київ: ДП «Розвиток», 2011. 520 с.

20. Великий тлумачний словник сучасної українськоїмови / упоряд. і голов. ред. В. Т. Бусел. Київ; Ірпінь: ВТФ Перун, 2005. 1728 с.

21. Винер Н. Мое отношение к кибернетике, ее прошлое и будущее. Москва: Советское радио, 1969. 24 с.

22. Воронов И. А. Теоретические основы использования информационных и поисковых систем глобальной сети Интернет в оперативно-розыскной деятельности. *Вісник ЛДУВС ім. Е. О. Дідоренка.* 2009. № 1. С. 194–203.

23. Галаган В. І., Саліхов І. Ю. Встановлення події кримінального правопорушення як обставини, яка підлягає доказуванню у кримінальному провадженні: монографія. Київ: УкрДГРІ, 2017. 198 с.

24. Галахов С. С., Комарова Е. В. Этапы становления информационно-аналитического обеспечения оперативно-розыскной деятельности органов внутренних дел. *Научный портал МВД России.* 2008. № 1. С. 59–62.

25. Голосніченко І. П. Адміністративне право України (основні категорії і поняття). Київ: ГАН, 2005. 232 с.

26. Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями: монография. Запорожье: ГУ «ЗИГМУ», 2003. 336 с.

27. Голубовский В. Ю. Теоретические и правовые аспекты информационного обеспечения ОРД. Санкт-Петербург: Санкт-Петербургский ун-т МВД РФ, 2000. 152 с.

28. Голунский С. А., Шавер Б. М. Криминалистика. Методика расследования отдельных видов преступлений. Москва: Юрид. изд-во НКЮ СССР, 1939. 372 с.

29. Господарський процесуальний кодекс України; Кодекс від 06.11.1991 № 1798-XI. URL: https://zakon.rada.gov.ua/laws/show/1798-12

30. Гребельский Д. В. Теоретические основы и организационно-правовые проблемы оперативно-розыскной деятельности органов внутренних дел. Москва: РИО Акад. МВД СССР, 1977. 170 с.

31. Грицанов А. А. Новейший философский словарь. Минск: В. М. Скакун, 1999. 877 с.

32. Грібов М. Л. Зміст та основні напрями криміналістичного забезпечення негласних слідчих (розшукових) дій. *Вісник кримінального судочинства.* 2017. № 1. С. 35–41.

33. Громов В. И. Методика расследования преступлений: руководство для органов милиции и уголовного розыска. Москва: Изд-во НКВД РСФСР, 1930. 136 с.

34. Даньшин М. В. Криміналістика XXI століття: місце у системі наукового знання: монографія. Харків, 2013. 480 с.

35. Демянчук Е. В. Мониторинг сети Интернет как мероприятие, проводимое с целью получения оперативно значимой информации. Спеціальна техніка у правоохоронній діяльності: матер. II Міжнар. науково-прак. конф. (м. Київ, 22 травня 2005 р.). Київ: КНУВС, 2006. С. 171–178.

36. Демянчук Е. В. Борьба с преступлениями экстремистской и террористической направленности, совершаемые с использованием сети «Интернет». *Научный портал МВД России.* Москва, 2009. № 1. С. 99–106.

37. Демянчук Е. В. Интернет как объект оперативно-розыскной деятельности. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (г. Москва, 25–26 мая 2004 г.). Москва: Акад. упр. МВД России, 2004. С. 214–216.

38. Демянчук Е. В. Оперативно-розыскные мероприятия и методы по выявлению и пресечению пропаганды идей терроризма и экстремизма в сети Интернет. Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (г. Москва, 25–26 мая 2004 г.). Москва: Акад. упр. МВД России, 2004. С. 189–192.

39. Докази та доказування у кримінальному провадженні: навч. посібник / Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін. Львів: ЛьвДУВС, 2018. 272 с.

40. Дубовий О. П., Лукашенко В. Я., Рибалко Я. В. та ін. Криміналістичне дослідження слідів рук: наук.-практ. посібник / за заг. ред. Я. Ю. Кондратьєва. Київ: Атіка, 2000. 152 с.

41. Експертизи у судовій практиці / КНДІСЕ, Акад. адвокатури України: наук.-практ. посібник; за заг. ред. В. Г. Гончаренка. 2-ге вид., перероб. і доп. Київ: Юрінком Інтер, 2010. 400 с.

42. Експертна спеціальність 9.5 «Молекулярно-генетичні дослідження». URL: https://dndekc.mvs.gov.ua/

43. Елинський В. И. Основы методологии теории оперативно--розыскной деятельности: монография. Москва: Изд. Шумилова И. И., 2001. 228 с.

44. Єдиний звіт про кримінальні правопорушення за січень-грудень 2019 р. URL: https: //www.gp.gov.ua/ua/stst2011.html?dir_id=113 897&libid= 100820&c=edit&_c=fo

45. Єрофєєв В. Кримінальний аналіз – це ефективна робота поліції та безпека громадян. URL: http://mvs.gov.ua/ua/news/10309_Kriminalniy_ analiz_ce_efektivna_robota_policii_ta_ bezpeka_gromadyan_FOTO.htm

46. Задорожний Ю. А. Проблемы информационно-аналитического обеспечения ОРД в современных условиях. Виявлення, фіксація та використання доказів у процесі досудового слідства. *Вісник ЛАВД імені 10-річчя незалежності України. Спеціальний випуск.* Луганськ, 2005. С. 89–99.

47. Задорожный Ю. А. Проблемы информатизации органов внутренних дел. *Вісник Луганського державного університету внутрішніх справ.* 2007. № 2. С. 215–228.

48. Застосування спеціальних знань і техніко-криміналістичних засобів під час проведення слідчого огляду: метод. рекомендації / укл. Р. І. Благута, О. В. Захарова, М. Ю. Ковальська та ін. Львів: ЛьвДУВС, 2019. 104 с.

49. Захаров В. П. Проблеми інформаційного забезпечення боротьби зі злочинністю: монографія. Львів: Львів. держ.ун-т внутр. справ, 2008. 472 с.

50. Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. Львів: ЛьвДУВС, 2015. 492 с.

51. Зима Л. М. Протидія кіберзлочинності у банківській сфері: стан, проблеми та шляхи їх вирішення. Протидія злочинам, які вчиняються з використанням комп'ютерних мереж: тези доповідей Міжнарод. наук.-практ. конф. (м. Севастополь, 1–2 жовт. 2010 р.). Суми: ДВНЗ «УАБС НБУ», 2010. С. 74–80.

52. Зинин А. М. Фоторобот (история создания и внедрения в практику органов внутренних дел). 85 лет Экспертно-криминалистической службе органов внутренних дел России: сб. статей. Москва, 2004. С. 218–230.

53. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції: монографія / В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін.; за ред. В. Ю. Шепітька, В. А. Журавля. Харків: Апостіль, 2017. 260 с.

54. Інформатика та інформаційні технології: навч. посібник / Б. В. Щур, І. С. Керницький, В. В. Сеник та ін. Львів: Львів. держ. ун-т внутр. справ, 2010. 536 с.

55. Клименко Н. І. Криміналістичні знання: поняття, структура, розвиток / Криміналістика XXI століття: матеріали Міжнар. наук.-практ. конф. (м. Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 26–30.

56. Кобзар С. І., Сегай М. Я. Криміналістичне дослідження слідів рук людини (праксіологічний аспект): монографія. Луганськ: РВВ ЛДУВС, 2006. 208 с.

57. Кодекс адміністративного судочинства України; Кодекс, Закон від 06.07.2005 № 2747-IV. URL: https://zakon.rada.gov.ua/laws/ term/40260

58. Кодекс поведінки посадових осіб з підтримання правопорядку: резолюція 34/169 Генеральної Асамблеї ООН 17 грудня 1999 р. URL: http://zakon5.rada.gov.ua/laws/show/995_282

59. Компьютерная преступность и кибертерроризм: сборник научных статей / под ред. В. А. Голубева, Э. В. Рыжкова. Запорожье: Центр исследования компьютерной преступности, 2005. Вып. 3. 448 с.

60. Конвенція про кіберзлочинність. *Офіційний вісник України.* 2007. № 65. С. 107. Ст. 2535. Офіц. пер.

61. Концепція створення Єдиного державного реєстру фізичних осіб, затверджена постановою Кабінету Міністрів України від 9 листопада 2004 р. № 1500. *Офіційний вісник України.* 2004. № 45. С. 25. Ст. 2972.

62. Корухов Ю. Г. Криминалистическое распознавание и криминалистическая диагностика: содержание и соотношение понятий. *Уголовный про-*

*цесс и криминалистика на рубеже веков.* Москва: Академия управления МВД России, 2000. С. 112–119.

63. Криминалистика: учеб. для вузов / Т. В. Аверьянова, Р. С. Белкин, Ю. Г. Корухов, Е. Р. Росинская; под ред. Р. С. Белкина. 2-е изд., перераб. и доп. Москва: Норма, 2004. 992 с.

64. Криминалистика: учебник / под ред. проф. В. А. Образцова. Москва: Юристъ, 1995. 592 с.

65. Криминалистика: учебник / Т. В. Аверьянова, Е. Р. Россинская, Р. С. Белкин, Ю. Г. Корухов. 4-е изд., перераб. и доп. Москва: Норма; НИЦ Инфра-М, 2019. 928 с.

66. Криміналістика (криміналістична техніка): курс лекцій / П. Д. Біленчук, А. П. Гель, М. В. Салтевський, Г. С. Семаков. Київ: МАУП, 2001. 216 с.

67. Криміналістика: підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін. Київ, 2015. 544 с.

68. Криміналістика: підручник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін.; за ред. В. Ю. Шепітько. 5-те вид., переробл. та допов. Київ: Ін Юре, 2016. 640 с.

69. Криміналістика: підручник / Р. І. Благута, О. І. Гарасимів, О. М. Дуфенюк та ін.; за заг. ред. Є. В. Пряхіна. 3-тє вид. переробл. та допов. Львів: ЛьвДУВС, 2016. 948 с.

70. Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

71. Кримінальний процес: підручник / Р. І. Благута, Ю. В. Гуцуляк, О. М. Дуфенюк та ін.; за заг. ред. А. Я. Хитри, Р. М. Шехавцова, В. В. Луцика. Львів: ЛьвДУВС, 2019. Ч. 2. 616 с.

72. Кримінальний процесуальний кодекс України: Закон України від 13 квітня 2012 р. № 4651-VI. *Голос України* від 19.05.2012. № 90–91.

73. Кримінальний процесуальний кодекс України. Науково-практичний коментар: у 2 т. / за заг. ред. В. Я. Тація, В. П. Пшонки, А. В. Портнова. Харків: Право, 2012. Т. 1. 768 с. Т. 2. 664 с.

74. Кримінальний процесуальний кодекс України. Науково-практичний коментар / за заг. ред. В. Г. Гончаренка, В. Т. Нора, М. Є. Шумила. Київ: Вид-во «Юстиніан», 2012. 1224 с.

75. Кузнецов И. Н. Информация: сбор, защита, анализ: учебник по информационно-аналитической работе. Москва: ООО Изд. Яуза, 2001. 100 с.

76. Линдер И. Б., Чуркин С. А. Спецслужбы России за 1000 лет. Материалы секретных фондов. Москва: РИПОЛ классик, 2006. 736 с.

77. Лисиченко В. К., Шехавцов Р. М. Проблеми теорії та практики подолання протидії розслідуванню окремих різновидів злочинів, вчинених організованими групами, злочинними організаціями: монографія / МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. 2-ге вид., переробл. та доповн. Луганськ, 2012. 319 с.

78. Лосев М., Сидоров В. Интегрированные биометрические системы. Контроль доступа по радужной оболочке глаза. *ЭЛЕКТРОНИКА: Наука. Технология. Бизнес.* 2004. № 6. С. 13–15.

79. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів: монографія. Київ: Нац. акад. внутр. справ України, 2005. 360 с.

80. Лукашевич В. Г., Юнацький О. В. Моделювання у криміналістиці та пізнавальній діяльності слідчого: монографія. Київ, 2008. 184 с.

81. Лукашов В. А. Организация и методика информационно-аналитической работы в сфере оперативно-розыскной деятельности органов внутренних дел: лекция. Омск: ОВШМ МВД СССР, 1983. 32 с.

82. Маннс Г. Ю. Общее и специальное предупреждение в уголовном праве. Иркутск: Тип. изд-ва «Власть труда», 1926. 72 с.

83. Марченко А. Идентификация по кисти руки. *ЭЛЕКТРОНИКА: Наука, Технология. Бизнес.* 2004. № 6. С. 18–19.

84. Мельник В. Некрасов В. Як подолати ворога, багатшого за транснаціональні корпорації? URL: http://n-v.com.ua/yak-podolaty-voroga-bagatshogo-za-korporatsyi/

85. Минин А. Я., Попов В. И., Козлов В. И., Кувалдин В. П. Разведка и ее использование против организованной преступности и коррупции в США: учеб. пособие. Москва: МИ МВД России, 2000. 37 с.

86. Михайлов М. А. Проблема идентификации личности выходит за пределы, определяемые предметом криминалистики. *Ученые записки Таврического национального университета им. В. И. Вернадского. Серия «Юридические науки».* Т. 20 (59). 2007. № 2. С. 149–157.

87. Міжнародна поліцейська енциклопедія: у 10 т. / відп. ред.: В. В. Коваленко, Є. М. Моісеєв, В. Я. Тацій, Ю. С. Шемшученко. Київ: Атіка, 2010. Т. VI. Оперативно-розшукова діяльність поліції (міліції). 1128 с.

88. Movchan A. V. Actual issues of the obtaining of investigation and search information under modern conditions. *Наука і правоохорона.* 2014. № 1. С. 92–96.

89. Мовчан Анатолий. Компьютерные системы биометрической идентификации. Актуальные проблемы применения в правоохранительной деятельности: монография. Saarbrücken, Deutschland: *LAP LAMBERT Academic Publishing*. 2015. 80 с.

90. Мовчан А. В. Актуальні проблеми впровадження в органах Національної поліції України моделі поліцейської діяльності, керованої аналітикою. *Соціально-правові студії.* 2018. № 1. С. 17–22.

91. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності Національної поліції: навч. посібник. Львів: ЛьвДУВС, 2017. 244 с.

92. Мовчан А. В. Кібернетична безпека України в умовах глобальної нестабільності. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2015. № 1. С. 159–163.

93. Мовчан А. В. Модель підготовки фахівців у галузі інформаційних технологій для органів Національної поліції України. *Інформаційні технології і засоби навчання.* 2018. № 4. С. 149–161.

94. Мовчан А. В. Характеристика основних форм інформаційно-аналітичної роботи в оперативно-розшуковій діяльності. *Наука і правоохорона.* 2014. № 4. С. 241–247.

95. Мовчан А. В., Мовчан Д. А. Зарубіжний досвід застосування біометричної ідентифікації людини у протидії транснаціональній злочинності. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* Луганськ, 2009. № 1. С. 179–184.

96. Моїсєєв О. Технології в криміналістиці та в судовій експертології: співвідношення та розмежування. *Правничий часопис Донецького університету: науковий журнал.* 2010. № 2(24). С. 123–129.

97. Мороз А. О. Біометричні технології ідентифікації людини, огляд систем. *Математичні машини і системи.* 2011. № 1. С. 39–45.

98. Мотлях О. І. Поліграфологія та її місце в системі криміналістики. Актуальні питання кримінального процесу, криміналістики та судової експертизи: матеріали міжвід. наук.-практ. конф. (м. Київ, 24 листоп. 2017 р.): у 2 ч. Київ, 2017. Ч. 1. С. 179–180.

99. Мусієнко О. Л. Новітні технології у криміналістиці: проблеми та перспективи. Правове життя сучасної України: матеріали Міжнар. наук. конф. проф.-викл. та аспірант. складу / відп. за вип. В. М. Дрьомін; НУ ОЮА, Півд. регіон. центр НАПрН України. Одеса: Фенікс, 2014. Т. 1. С. 757–759.

100. Наукові та організаційно-правові засади протидії підрозділами карного розшуку обігу майна, одержаного злочинним шляхом: монографія / Баб'як А. В., Крєпаков І. О., Мазур Л. А., Стащак М. В.; за заг. ред. С. М. Гусарова, В. В. Шендрика. Львів: ВД «Панорама», 2014. 160 с.

101. Національний звіт за 2017 рік щодо наркотичної ситуації в Україні (за даними 2016 року). Поглиблений огляд наркоситуації в Україні для Європейського моніторингового центру з наркотиків та наркотичної залежності / Державна установа «Український моніторинговий та медичний центр з наркотиків та алкоголю Міністерства охорони здоров'я України». 2017. С. 161–164.

102. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ: навч.-практ. посібник / Б. І. Бараненко, О. В. Бочковий, К. А. Гусева та ін.; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. 416 с.

103. Нежданов И. Ю. Конкурентная разведка в России. Нежданов Игорь Юрьевич – частный взгляд на проблему. URL: http://analitirus.blogspot.com

104. Непорада А. С. Новітні технології в криміналістиці: 3D-сканування при огляді місця події. *Криміналістичний вісник.* 2016. № 2 (26). С. 141–143.

105. Никифорчук Д. Й., Бусол О. Ю., Бірюков Г. М. Аналітична робота в оперативно-розшуковій діяльності: навч.-практ. посібник. Київ: НАВС, 2012. 152 с.

106. Овчинский А. С. Информация и оперативно-розыскная деятельность: монография / под ред. В. И. Попова. Москва: ИНФРА-М, 2002. 97 с.

107. Овчинский В. Технологии будущего против криминала. Litres, 31 серп. 2019 р. URL: http://www.books.google.com.ua/

108. Овчинский С. С. Оперативно-розыскная информация / под ред. А. С. Овчинского и В. С. Овчинского. Москва: ИНФРА-М, 2000. 367 с.

109. Овчинский А. С., Каретников М. К. Проблемы подготовки специалистов в области применения современных информационных технологий. *Вестник МВД России.* 2000. № 4–5. С. 129–135.

110. Оперативне розпізнавання: монографія / В. А. Некрасов, В. Я. Мацюк, Н. Є. Філіпенко, Л. В. Родинюк. Київ: КНТ, 2007. 216 с.

111. Оперативно-розшукова діяльність: посібник для вищих навчальних закладів. Київ: «Видавництво Людмила», 2019. 240 с.

112. Оперативно-розшукова діяльність підрозділів карного розшуку Національної поліції України: навч. посібник / А. В. Баб'як, Ю. І. Дмитрик, В. П. Захаров, В. Я. Ільницький, М. А. Лісовий, А. В. Мовчан. Львів: ЛьвДУВС, 2018. 256 с.

113. Оперативно-розыскная деятельность: учебник / под ред. К. К. Горяинова, В. С. Овчинского, Г. К. Синилова, А. Ю. Шумилова. 2-е изд., доп. и перераб. Москва: ИНФРА-М, 2004. 848 с.

114. Орлов Ю. Ю. Застосування лазерного сканування під час огляду місця події. *Науковий вісник Національної академії внутрішніх справ.* 2011. № 4. С. 196–201.

115. Ортинський В. Л. Протидія нелегальній економіці засобами оперативно-розшукової діяльності: монографія. Львів, 2004. 436 с.

116. Осипенко А. Л. О некоторых особенностях раскрытия сетевых компьютерных преступлений. Москва: Научный портал МВД России, 2010. № 2. С. 42–47.

117. Осипенко А. Л. Оперативно-розыскная деятельность в киберпространстве: ответы на новые вызовы. *Научный вестник Омской академии МВД России.* Омск, 2010. № 2 (37). С. 38–43.

118. Осипенко А. Л. Осуществление оперативно-розыскных мероприятий при раскрытии сетевых компьютерных преступлений / Информатизация и информационная безопасность правоохранительных органов: сб. трудов XIII Межд. науч. конф. (г. Москва, 25–26 мая 2004 г.). Москва: Акад. упр. МВД России, 2009. С. 204–209.

119. Осипенко А. Л. Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Изд-во Омск. акад. МВД России, 2009. 480 с.

120. Основи кримінального аналізу: посіб. з елементами тренінгу / О. Є. Користін, С. В. Албул, А. В. Холостенко та ін. Одеса: ОДУВС, 2016. 112 с.

121. Основи оперативно-розшукової діяльності: навч. посібник / С. В. Албул, С. В. Андрусенко, Р. В. Мукоіда, Д. О. Ноздрін; за заг. ред. С. В. Албула. Одеса: ОДУВС, 2016. 270 с.

122. Основи управління в органах внутрішніх справ: навч. посібник / О. М. Бандурка, В. М. Бевзенко, В. М. Василенко та ін. Харків: Харк. нац. ун-т внутр. справ, 2010. 590 с.

123. Отримання та використання первинної оперативно-розшукової інформації оперативними підрозділами ОВС України: монографія / А. В. Баб'як, В. П. Сапальов, М. В. Стащак, В. В. Шендрик. Львів: Каменяр, 2010. 167 с.

124. Пеньков С. В., Шендрик В. В. Впровадження Інтернет-технологій у діяльність Національної поліції України для отримання оперативно-розшукової інформації. *Право і безпека.* 2017. № 2 (65). С. 80–85. URL: http://dspace.univd.edu.ua/xmlui/handle/123456789/2410

125. Перепелиця М. М., Манжай О. В., Шендрик В. В. Здійснення оперативно-розшукових заходів шляхом використання кіберпростору: навч.-практ. посібник. Київ: ДП «Друкарня МВС України», 2010. 146 с.

126. Пєчніков В. С. Є така служба…: в 2 т.; за ред. І. П. Красюка. Київ, 2011. Т. 1. Ч. 1. 576 с.

127. Плэтт В. Стратегическая разведка. Основные принципы. Москва: Форум, 1997. 376 с.

128. Погорецький М. А., Сергєєва Д. Б., Старенький О. С. та ін. Доказування слідчими Служби безпеки України контрабанди наркотичних засобів: монографія / за заг. ред. М. А. Погорецького. Київ: Нац. акад. СБ України, 2018. 238 с.

129. Погорецький М. А., Шеломенцев В. П. Поняття кіберпростору як середовища вчинення злочину. *Інформаційна безпека людини, суспільства, держави.* Київ, 2009. № 2. С. 77–81.

130. Погорецький М. А., Шеломенцев В. П. Поняття організації оперативно-розшукової діяльності. *Кримський юридичний вісник*. 2010. № 1 (8). С. 30–39.

131. Погорецький М. А., Шеломенцев В. П. Кіберзлочини: до визначення поняття. *Вісник прокуратури.* 2012. № 8. С. 89–96.

132. Порядок фіксації біометричних даних іноземців та осіб без громадянства під час прикордонного контролю в пунктах пропуску (пунктах контролю) через державний кордон та у контрольних пунктах в'їзду-виїзду, а також здійснення провадження у справах про адміністративні правопорушення: наказ МВС України від 24 квітня 2019 року № 310. URL: https://zakon.rada.gov.ua/laws/show/z0496-19?lang=en

133. Потапов С. М. Принципы криминалистической идентификации. Москва: Сов. гос. и право. 1940. № 1.

134. Практикум з криміналістики: навч. посібник / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель та ін. Київ, 2013. С. 11–12.

135. Применение интеллектуальной системы криминального анализа в реальном времени (RICAS) для аналитического сопровождения оперативно-розыскной деятельности и досудебного расследования / Д. Ю. Узлов, В. М. Струков, О. Б. Григорович та ін. *Право і безпека.* 2015. № 2 (57). С. 132–139.

136. Про державну таємницю: Закон України від 21 січ. 1994 р. № 3855-XII. *Відомості Верховної Ради України.* 1994. № 16. Ст. 93.

137. Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійснення оперативно-розшукової діяльності, дізнання і досудового слідства: постанова Пленуму Верховного Суду України від 28 березня 2008 р. № 2 (із змінами, внесеними згідно з Постановою Верховного Суду № 8 від 4 квітня 2010 р.). *Вісник Верховного Суду України.* 2008. № 4. С. 4.

138. Про деякі питання здійснення слідчим суддею суду першої інстанції судового контролю за дотриманням прав, свобод та інтересів осіб під час застосування заходів забезпечення кримінального провадження: лист Вищого спеціалізованого суду України від 5 квітня 2013 р. № 223-558/0/4-13. *Судовий Вісник.* 2013. № 4.

139. Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус: Закон України від 20.11.2012 № 5492-VI. *Голос України*. 2012. № 231.

140. Про затвердження Інструкції з організації функціонування криміналістичних обліків експертної служби МВС України: наказ МВС від 10 вересня 2009 р. № 390, зареєстрований в Міністерстві юстиції України 15 жовтня 2009 р. за № 963/16979.

141. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні: наказ ГПУ, МВС, СБУ, АДПС, Мінфіну, Мін'юсту від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5.

142. Про затвердження Інструкції про порядок ведення єдиного обліку в органах поліції заяв і повідомлень про вчинені кримінальні правопорушення та інші події: наказ МВС від 6 листопада 2015 р. № 1377, зареєстрований в Міністерстві юстиції України 1 грудня 2015 р. за № 1498/27943.

143. Про затвердження Інструкції про порядок використання правоохоронними органами можливостей НЦБ Інтерполу в Україні у попередженні, розкритті та розслідування злочинів: наказ МВС, ГПУ, СБУ, Держкомітету у справах охорони державного кордону, Держмитслужби, ДПА від 9 січня 1997 р. № 3/1/2/5/2/2.

144. Про затвердження плану заходів з виконання Концепції реалізації державної політики у сфері профілактики правопорушень на період до 2015 року: Постанова Кабінету Міністрів України від 8 серпня 2012 р. № 767. *Урядовий кур'єр.* 2012. № 159.

145. Про затвердження Плану заходів із створення системи контролю іноземців та осіб без громадянства, що в'їжджають на територію України, з фіксуванням їх біометричних даних: розпорядження Кабінету Міністрів України від 12 березня 2008 р. № 439-р.

146. Про затвердження Положення про єдину цифрову відомчу телекомунікаційну мережу МВС: наказ МВС України від 4 липня 2016 р. № 596, зареєстрований в Міністерстві юстиції України 28 липня 2016 р. за № 1055/29185.

147. Про затвердження Положення про Інтегровану інформаційно-пошукову систему органів внутрішніх справ України: наказ МВС України від 12 жовтня 2009 р. № 436. *Офіційний вісник України.* 2010. № 101. Ст. 3569.

148. Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів які перетинають державний кордон: наказ АДПС, ДМС, ДПА, МВС, МЗС, Мінпраці, СБУ, Служби зовнішньої розвідки від 3 травня 2008 р. № 284/287/214/150/64/175/266/75, зареєстрований в Міністерстві юстиції України 12 травня 2008 р. за № 396/15087. *Офіційний вісник України.* 2008. № 37. Ст. 1249.

149. Про затвердження Положення про Міністерство внутрішніх справ України: постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 878. *Урядовий кур'єр* від 6 листопада 2015 р. № 207.

150. Про затвердження Положення про Національну поліцію: постанова Кабінету Міністрів України від 28 жовтня 2015 р. № 877. *Урядовий кур'єр* від від 06.11.2015 № 207.

151. Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань: наказ ГПУ від 6 квітня 2016 р. № 139, зареєстрований в Міністерстві юстиції України 5 травня 2016 р. за № 680/28810. *Офіційний вісник України.* 2016. № 46. Ст. 1674.

152. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджене Постановою Кабінету Міністрів України від 29 березня 2006 р. № 373. *Урядовий кур'єр* від 18.04.2006. № 73–74.

153. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 5 липня 1994 р. № 80/94-ВР. *Відомості Верховної Ради України.* Київ, 1994. № 31. Ст. 286.

154. Про захист персональних даних: Закон України Закон від 1 червня 2010 р. № 2297-VI. *Відомості Верховної Ради України.* 2010. № 34. Ст. 481.

155. Про інформацію: Закон України від 02.10.1992 № 2657-XII. *Відомості Верховної Ради України.* 1992. № 48. Ст. 650.

156. Про Концепцію Національної програми інформатизації: Закон України від 4 лютого 1998 р. № 75/98-ВР. *Відомості Верховної Ради України.* 1998. № 27–28. Ст. 182.

157. Про Національну поліцію: Закон України від 2 липня 2015 р. № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40–41. Ст. 379.

158. Про Національну програму інформатизації: Закон України від 4 лют. 1998 р. № 74/98-ВР. *Відомості Верховної Ради України.* 1998. № 27–28. Ст. 181.

159. Про окремі питання здійснення слідчим суддею суду апеляційної інстанції судового контролю за дотриманням прав, свобод та інтересів осіб у кримінальному провадженні: рекомендаційні роз'яснення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ від 29.01.2013 № 223-158/3/4-13. Київ: ВВСУ, 2013. 12 с.

160. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303.

161. Про організаційно-правові основи боротьби з організованою злочинністю: Закон України від 30 червня 1993 р. № 3341-XII. *Відомості Верховної Ради України.* 1993. № 35. Ст. 358.

162. Про основні засади забезпечення кібербезпеки України: Закон України. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.

163. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 9 січня 2007 р. № 537-V. *Відомості Верховної Ради України.* 2007. № 12. Ст. 102.

164. Про першочергові завдання щодо впровадження новітніх інформаційних технологій: Указ Президента України від 20 жовтня 2005 р. № 1497. *Урядовий кур'єр* від 1 листопада 2005 р. № 207.

165. Про схвалення Концепції Державної цільової правоохоронної програми встановлення сучасних систем безпеки, застосування засобів зовнішнього контролю (спостереження) та швидкого реагування на період до 2016 року: розпорядження Кабінету Міністрів України від 6 лютого 2013 р. № 51-р. *Урядовий кур'єр.* 2013. № 29.

166. *Про телекомунікації: Закон України від 18.11.2003 № 1280-IV. Відомості Верховної Ради України (ВВР).* 2004. № 12. Ст. 155.

167. Психологія безпеки професійної діяльності в системі МВС України: навч.-практ. посібник / Б. І. Бараненко, Д. О. Бабічев, В. О. Криволапчук та ін.; за ред. Б. І. Бараненка, О. В. Шаповалова; МВС України, ДНДІ МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 200 с.

168. Психологія оперативного спілкування в діяльності оперативних підрозділів органів внутрішніх справ: навч.-практ. посібник / Б. І. Бараненко, В. А. Глазков, О. С. Звонок та ін.; за ред. Е. О. Дідоренка; МВС України, Луган. держ. ун-т внутр. справ. Луганськ: РВВ ЛДУВС, 2007. 552 с.

169. Работа полиции. Системы полицейской информации и разведки: пособие по оценке систем уголовного правосудия. Нью-Йорк: Управление Организации Объединенных Наций по наркотикам и преступности. Вена, 2010. С. 25. URL: https://www.unodc.org/pdf/ criminal_justice/10-52547_ 1_Policing_4_ebook.pdf

170. Реєстр операторів, провайдерів телекомунікацій станом на 27.08.2019. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=55& language=uk

171. Рибальський О. В., Соловйов В. І., Журавель В. В. , Шабля О. М. Деякі аспекти побудови вітчизняної системи інструментарія експертизи матеріалів та засобів цифрового звукозапису. Криміналістика і судова експертиза. 2018. Вип. 63 (2). С. 81–92.

172. Рішення Конституційного Суду України від 20 січня 2012 р. № 2-рп у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України. *Офіційний вісник України.* 2012. № 9. С. 106. Ст. 332.

173. Розкриття та розслідування умисних вбивств, учинених на замовлення: навч. посібник / В. І. Василинчук, А. Ф. Волобуєв, В. Я. Горбачевський та ін. Київ: Упр. вид.-полігр. діяльності МВС України, 2010. 288 с.

174. Салтевський М. В. Криміналістика (у сучасному викладі): підручник. Київ: Кондор, 2008. 588 с.

175. Сара Мюррей. Биометрия против терроризма. Деловая неделя. URL: http://www.dn-weekly.kiev.ua

176. Семенов В. В., Терешкевич А. І. Використання новітніх технологій та досягнень науки й техніки в кримінальному провадженні. *Криминалистика и судебная экспертиза.* 2015. Вып. 60. С. 117–125.

177. Семеновский П. С. Дактилоскопия как метод регистрации. Москва: Изд-во «Розыск республики», 1923. – 113 с.

178. Сергєєва Д. Б. Співвідношення пізнання і доказування у кримінальному процесі. *Науковий вісник Київського національного університету внутрішніх справ.* 2010. Вип. 4 (71). С. 144–149.

179. Сергєєва Д. Б. Напрями використання результатів негласних слідчих (розшукових) дій у кримінальному процесуальному доказуванні. Вісник кримінального судочинства. 2018. № 2. С. 81–91.

180. Сергій Демедюк. Для протидії сучасній злочинності правоохоронці потребують якісних інструментів реверсної інженерії. URL: https://cyberpolice.gov.ua/news/sergij-demedyuk-dlya-protydiyi-suchasnij-zlochynnosti-pravooxoronczi-potrebuyut-yakisnyx-instrumentiv-reversnoyi-inzheneriyi-1575/

181. Середа В. В., Хатнюк Ю. А. Організаційно-правові основи діяльності підрозділів Національної поліції України, що здійснюють аналітичну роботу. *Науковий вісник Львівського університету внутрішніх справ. Серія юридична.* 2018. № 4. С. 189–198.

182. Середа В. В., Серкевич І. Р. Тероризм: кримінологічна детермінація і кримінально-правова протидія: монографія / за заг. ред. В. С. Канціра. Львів: ЛьвДУВС, 2016. 188 с.

183. Синилов Г. К. Правовые, информационные и тактические основы ОРД советской милиции. Москва, 1975. 320 с.

184. Скулиш Є. Д. Негласні слідчі (розшукові) дії за кримінально-процесуальним законодавством України. *Вісник Національної академії прокуратури України.* 2012. № 2. С. 15–23.

185. Словарь иностранных слов. 14-е изд., испр. Москва: Рус. яз., 1987. 608 с.

186. Словник спеціальних термінів правоохоронної діяльності / за ред. Я. Ю. Кондратьєва. Київ: Нац. акад. внутр. справ України, 2004. 560 с.

187. Советский энциклопедический словарь / гл. ред. А. М. Прохоров. 3-е изд. Москва: Сов. Энциклопедия, 1984. 1600 с.

188. Соколова О. А. Некоторые направления использования инновационных технологий при получении диагностической информации о человеке. URL: https://cyberleninka.ru/ journal/n/izvestiya-tulskogo-gosudarstvennogo-universiteta-ekonomicheskie-i-yuridicheskie-nauki

189. Стащак Н. В., Перепелица Н. Н. Информационно-аналитическое обеспечение оперативной разработки лиц, которые готовятся к совершению преступлений в составе организованной группы. *Журнал научных публикаций аспирантов и докторантов.* 2014. Вып. 12. С. 67–71.

190. Степанюк Р. Л., Лапта С. П. Новітні зарубіжні розробки та перспективні дослідження у галузі техніко-криміналістичного забезпечення протидії злочинності. Право і безпека. 2017. Вип. 2 (65). С. 96–101.

191. Тероризм: теоретико-прикладні аспекти: навчальний посібник / кол. авторів; за заг. ред. В. К. Грищука. Львів: ЛьвДУВС, 2011. 328 с.

192. Тищенко В. В. Система криминалистики: проблемы оптимизации. Криміналістика XXI століття: матеріали Міжнар. наук.-практ. конф. (м. Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 46–50.

193. Топчій В. В., Тичина Д. М. Запобігання використанню сучасних інформаційних технологій у злочинних цілях. *Правовий часопис Донбасу.* 2018. № 1. С. 159–166.

194. Торвальд Ю. Век криминалистики; пер. с нем.; под ред. Ф. М. Решетникова. Москва: Прогресс, 1991. 3-е изд. 323 с.

195. Удалова Л. Д. Теорія та практика отримання вербальної інформації у кримінальному процесі України: монографія. Київ, 2005. 324 с.

196. Халиков А. Н., Яковец Е. Н., Журавленко Н. И. Юридическое, техническое и информационно-аналитическое обеспечение оперативно-розыскной деятельности: учеб. пособие / под ред. А. Н. Халикова. Москва: Юрлитинформ, 2010. 472 с.

197. Хараберюш И. Компьютерная преступность – проблемы противодействия преступности в сфере новых информационных технологий. URL: http//crème-research.ru

198. Хараберюш І. Ф. Використання спеціальної техніки щодо протидії злочинності в Україні: теоретичні, правові та організаційні аспекти: монографія. Донецьк, 2011. 234 с.

199. Хахановський В. Г. Інформаційно-аналітичне забезпечення оперативно-розшукової діяльності: основні поняття та нормативно-правова база. *Науковий вісник ЛІВС.* 2003. № 2 (1). С. 191–195.

200. Хахановський В. Г., Дабіжа Д. В., Пясковський В. В. Особливості використання обліків та автоматизованих інформаційних систем при розслідуванні кримінальних правопорушень: метод. реком. Київ: 2017. 36 с.

201. Цивільний кодекс України. *Відомості Верховної Ради України.* Київ, 2003. № 40–44. Ст. 356.

202. Цивільний процесуальний Кодекс України; Кодекс, Закон від 18.03.2004 № 1618-IV. URL: https://zakon.rada.gov.ua/laws/term/40260

203. Чаплинський К. О. Тактичне забезпечення розслідування діяльності злочинних угрупувань: монографія. Дніпропетровськ: Ліра ЛТД, 2010. 304 с.

204. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування: монографія. Київ: Хай-Тек Прес, 2010. 624 с.

205. Черняк Л. Internet і кібернетика. URL: http://www.icfcst.kiev.ua museumEP/cibernetic_r.html

206. Чисніков В. М. Правові витоки карно-розшукової служби України (історичний аспект). Теорія оперативно-службової діяльності правоохоронних органів України: наук. вид.; за ред. В. Л. Регульського. Львів: Львів. ін-т внутр. справ, 2000. С. 302–309.

207. Чорноус Ю. М. Криміналістика: напрями розвитку та вдосконалення. Актуальні питання кримінального процесу, криміналістики та судової експертизи: матеріали міжвід. наук.-практ. конф. (м. Київ, 24 листоп. 2017 р.): у 2 ч. Київ, 2017. Ч. 1. С. 189–190.

208. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів: монографія. Вінниця: ТОВ «Нілан-ЛТД», 2017. 492 с.

209. Шевчук В. М. Современные тенденции противодействия контрабанде наркотических средств в Украине (криминалистический анализ).

*Збірник наукових праць Харківського Центру вивчення організованої злочинності спільно з Американським університетом у Вашингтоні.* 2004. Вип. 9. С. 230–277.

210. Шеломенцев В. П. Організована кіберзлочинність: до визначення поняття. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Київ: Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю, 2009. № 21. С. 314–322.

211. Шепітько В. Ю. Природа і предмет вивчення криміналістики в системі наукового знання. Вибрані твори. Харків, 2010. С.14–19.

212. Шепітько В. Ю., Авдєєва Г. К. Інновації в діяльності органів кримінальної юстиції. *Криминалистика и судебная экспертиза: Междуведомственный научно-методический сборник.* Вып. 59 / отв. ред. И. И. Емельянова. Киев: Министерство юстиции Украины, 2014. С. 3–11.

213. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю*: зб. наук. праць / редкол.: В. І. Борисов та ін. Харків: Право, 2011. Вип. 21. С. 39–45.

214. Шехавцов Р. М. Впровадження технологій 3D моделювання у розслідуванні злочинів: правові та криміналістичні проблеми. Криміналістика XXI століття: матеріали Міжнар. наук.-практ. конф. (м. Харків, 25–26 листоп. 2010 р.). Харків, 2010. С. 166–170.

215. Шмонин А. В. Методология криминалистической методики: монография. Москва: Юрлитинформ, 2010. 416 с.

216. Шумилов А. Ю. Основы уголовно-правовой оценки сыскной информации. Москва: Изд-ль Шумилова И. И., 2000. 140 с.

217. Юрченко О. М., Стрельбицька Л. М., Вертузаєв О. М. Застосування новітніх інформаційних технологій в інформаційно-аналітичному забезпеченні оперативно-службової діяльності правоохоронних органів. *Науковий вісник Київського національного університету внутрішніх справ.* К., 2006. № 3. С. 40–49.

218. Юсупов В. В. Криміналістика в Україні у XX–XXI століттях: монографія. Київ: ФОП Маслаков, 2018. 556 с.

219. Якимов И. Н. Криминалистика. Уголовная тактика. Москва: Изд-во НКВД РСФСР, 1929. 312 с.

220. Яковец Е. Н. Основы информационно-аналитического обеспечения оперативно-розыскной деятельности: учеб. пособие. Москва: Щит-М, 2009. 464 с.

221. Яковец Е. Н. Проблемы аналитической работы в оперативно-розыскной деятельности органов внутренних дел: монография. Москва: Издательский дом Шумиловой И. И., 2005. 219 с.

222. Яппаров Р. М. Информационные технологии и компьютерные преступления в сети Интернет. *Информационные технологии, связь и защита информации МВД России.* Москва: ВНИИ МВД России, 2012. С. 93–99.

223. Amos B., Harkes J., Wang J. et al. OpenFace models. GitHub [Internet]; 2016 [cited 2016 Jan 27]. URL: https://github.com/ cmusatyalab/openface/tree/master/models/openface

224. Becker W.D. 10 Modern Forensic Science Technologies // Forensic Colleges: site / Sechel Ventures. URL: http://www.forensicscolleges.com/blog/resources/10-modern-forensic-science-technologies

225. Bedeli M., Geradts Z. & Eijk E. Clothing identification via deep learning: forensic applications. J Forensic Sci. 2018; 33: 219-229.

226. Bejek Z., Paróczai R., Illyés Á., et al. The influence of walking speed on gait parameters in healthy people and in patients with osteoarthritis. Knee Surgery, Sport Traumatol Arthrosc. 2006. 14: 612-622.

227. Birch I., Gwinnett C., Walker J. Aiding the interpretation of forensic gait analysis: development of a features of gait database. Sci Justice. 2016; 56: 426–430.

228. Birch I., Vernon W., Walker J., et al. Terminology and forensic gait analysis. Sci Justice. 2015. 55: 279-284.

229. Bouchrika I., Goffredo M., Carter J., et al. On using gait in forensic biometrics. J Forensic Sci. 2011; 56: 882–889.

230. Bulman Ph., McLeod-Henning D. Applying Carbon-14 Dating to Recent Human Remains. National Institute of Justice Journal. Iss. No. 269. March 2012. URL: https://www.nij.gov/journals/269/pages/carbondating.aspx

231. Carter J. G., Phillips S. W., Gayadeen S. M. Implementing Intelligence-Led Policing: An Application of Loose-Coupling Theory. Journal of Criminal Justice. 2014. № 42. P. 435.

232. Chen Q., Huang J., Feris R., et al. Deep domain adaptation for describing people based on fine-grained clothing attributes. IEEE Conference on Computer Vision and Pattern Recognition; 2015 Jun 7-12; Boston, MA, USA: IEEE Press; 2015; p. 5315–5324.

233. Coxworth B. New fingerprint-lifting compound could make life easier for CSIs // NEW ATLAS: site / Gizmag Pty Ltd. October 29, 2013. URL: http://newatlas.com/lumicyano-fingerprint-lifting/29582/

234. Dodds A. J., Pollock E. M. «Chip», Land D. P. Forensic Glass Analysis by LA-ICP-MS: Assessing the Feasibility of Correlating Windshield Composition and Supplier: final tech. rep. URL: http://www.ncjrs.gov/ pdffiles1/nij/grants/232134.pdf

235. Don Braggins. Fingerprint sensing and analysis. Sensor Review. 2001.Vol. 21. № 4. P. 272–277.

236. Feris R., Bobbitt R., Brown L., et al. Attribute-based people search: Lessons learnt from a practical surveillance system. International Conference on Multimedia Retrieval; 2014 Apr 1–4; Glasgow, UK: ACM Press; 2014; p. 153–160.

237. Fydanaki A. & Geradts Z. Evaluating OpenFace: an open-source automatic facial comparison algorithm for forensics. J Forensic Sci. 2018; 33: 202–209.

238. Gebel E. Analyzing Fingerprints With A Dash Of Turmeric // c&en: Chemical & Engineering News: site / *American Chemical Society.* May 8, 2013. URL: http://cen.acs.org/articles/91/web/2013/05/Analyzing-FingerprintsDash-Turmeric.html?h=-519488094

239. Gupta S., Gupta V., Vij H., Vij R., Tyagi N. Forensic Facial Reconstruction: *The Final Frontier. Journal of Clinical and Diagnostic Research.* 2015. Sep. Vol. 9 (9).

240. Hatzichronoglou T. Revision of the High-Technology Sector and Product Classification. URL: OECD library // *OECD Science, Technology and Industry Working Papers.* Paris: OECD Publishing, 1997. 1997/2. 26 p.

241. Hossain M. A., Makihara Y., Wang J. et al. Clothing-invariant gait identification using part-based clothing categorization and adaptive weight control. *Pattern Recogn.* 2010. 43: 2281–2291.

242. Intelligence-Led Policing: the cutting edge of modern law enforcement. URL: http://euam.php7.postbox.kiev.ua/ua/news/opinion/inte lligence-led-policing-the-cutting-edge-of-modern-law-enforcement/

243. Jain A. K., Klare B., Park U. Face recognition: Some challenges in forensics. IEEE International Conference on Automatic Face & Gesture Recognition and Workshops. 2011. March 21–25; Santa Barbara, CA: IEEE Press; 2011. P. 726–733.

244. John G., Weiss A., Dutta S. Marketing in Technology-Intensive Markets: Toward a Conceptual Framework. *Journal of Marketing.* Volume 63, no. Special. 1999. P. 78–91.

245. Kreeger L. R., Weiss D. M. Forensic DNA Fundamentals for the Prosecutor. Be not Afraid / American Prosecutors Research Institute; National District Attorneys Association. Nov. 2003. III. 39 p. URL: http://www.ndaa.org/pdf/forensic_dna_fundamentals.pdf

246. Lao B., Jagadeesh K. Convolutional neural networks for fashion classification and object detection [cited 2016. June 26]. Available from: http://cs231n.stanford.edu/reports/BLAO_KJAG_CS231N_FinalPaperFashion Classification.pdf

247. Larsen P. K., Simonsen E. B., Lynnerup N. Gait analysis in forensic medicine. SPIE-IS&T. 2007; 6491.

248. Larsen P. K., Simonsen E. B., Lynnerup N. Gait analysis in forensic medicine. J Forensic Sci. 2008; 53: 1149–1153.

249. Li B., Beveridge P., O'Hare W. T., Islam M. The application of visible wavelength reflectance hyperspectral imaging for the detection and identification of blood stains. Science & justice. 2014. Dec. Vol. 54, Iss. 6. P. 432–438. DOI: 10.1016/j.scijus.2014.05.003.

250. Li F. F., Karpathy A., Johnson J. CS231n: Convolutional neural networks for visual recognition; University Lecture; 2015.

251. Metz R. Market Place: Collins Versus The Middle Man. The New York Times. April 24, 1969. p. 64.

252. Metz R. Market Place: Keeping an Eye On Big Trends. The New York Times. November 4, 1969. p. 64.

253. Movchan A. V. and Taranukha V. Yu. Constructing an Automation System to Implement Intelligence-Led Policing Into the National Police of Ukraine. *Cybernetics and Systems Analysis.* Vol. 54. № 4. July. 2018. P. 643–649.

254. Nina M. Van Mastrigt, Kevin Celie, Arjan L. Mieremet, Arnout C. C. Ruifr ok &Zeno Geradts. Critical review of the use and scientific basis of forensic gait analysis. J Forensic Sci. 2018; 33: 183-193.

255. Nixon M. S., Bouchrika I., Arbab-Zavar B., et al. On use of biomet rics in forensics: gait and ear. Eur Signal Process Conf. 2010; 44: 1655-1659.

256. Parker G. J., Leppert T., Anex D. S. and others. Demonstration of Protein-Based Human Identification Using the Hair Shaft Proteome. PLoS ONE. 11 (9): e0160653. 2016. DOI: 10.1371/journal.pone.0160653

257. Salomon J. What is Technology? The Issue of its origins and definitions. Historiy of technology. 1984. Vol. 1. P. 113–156.

258. Schroff F., Kalenichenko D., Philbin J. FaceNet: A unified embed-ding for face recognition and clustering. IEEE Conf Comput Vis Pattern Recognit; 2015 Jun 8-10; Boston (MA). 2015. p. 815–823.

259. Shanklin W. L., Ryans J. K. Marketing high technology. Mass: Lexington Books, 1984. xix, 216 p.

260. Steward I. New Kiwi crime tool unravels mixed DNA. URL: http://www.stuff.co.nz/science/9577038/NewKiwi-crime-tool-unravels-mixed-DNA

261. Strohmeier B. Chemical Characterization of Material Surfaces Using X-ray Photoelectron Spectroscopy (XPS): The Perfect Complement to Electron Microscopy Techniques. Microscopy and Microanalysis. Vol. 20. Iss. S3. P. 2062–2063. DOI: 10.1017/S1431927614012045.

262. Thimmesch D. 3D Printing Takes the Place of Traditional Clay Modeling in Forensic Facial Reconstruction // 3Dprint.com: site / 3DR Holdings, LLC. URL: https://3dprint.com/20664/3d-printing-facial-reco nstruct/

263. Yang M., Yu K. Real-time clothing recognition in surveillance videos. 18th IEEE International Conference on Image Processing (ICIP); 2011 Sept. 11–14; Brussels, Belgium: IEEE Press; 2011. P. 2937–2940.

НАУКОВЕ ВИДАННЯ

**Благута Роман Ігорович,**
кандидат юридичних наук, професор,
професор кафедри кримінального процесу та криміналістики
Львівського державного університету внутрішніх справ

**Мовчан Анатолій Васильович,**
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ

# НОВІТНІ ТЕХНОЛОГІЇ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ: СУЧАСНИЙ СТАН І ПРОБЛЕМИ ВИКОРИСТАННЯ

*Монографія*

Редагування *Андріана Кузьмич-Походенко*

Макетування *Надія Лесь*

Друк *Іван Хоминець*

Підписано до друку 30.04.2020 р.
Ум. друк. арк. 14,9. Зам. № 24-20.
Наклад 100 прим.

Львівський державний університет внутрішніх справ
79007, Львів, вул. Городоцька, 26.
www.livs.lviv.ua
E-mail: publaw@livs.lviv.ua