Національна академія правових наук України

Науково-дослідний інститут вивчення проблем

злочинності імені академіка В. В. Сташиса

Національної академії правових наук України

ІННОВАЦІЙНІ МЕТОДИ, ЗАСОБИ ТА ТЕХНОЛОГІЇ В КРИМІНАЛІСТИЦІ ТА СУДОВІЙ ЕКСПЕРТИЗІ

Науково-практичний посібник

За редакцією академіка НАПрН України В. Ю. Шепітька

НАЦІОНАЛЬНА АКАДЕМІЯ ПРАВОВИХ НАУК УКРАЇНИ

НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ВИВЧЕННЯ ПРОБЛЕМ
ЗЛОЧИННОСТІ ІМЕНІ АКАДЕМІКА В. В. СТАШИСА
НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ

ІННОВАЦІЙНІ МЕТОДИ, ЗАСОБИ ТА ТЕХНОЛОГІЇ В КРИМІНАЛІСТИЦІ ТА СУДОВІЙ ЕКСПЕРТИЗІ

Науково-практичний посібник

За редакцією академіка НАПрН України
В. Ю. Шепітька

Електронне наукове видання

Харків
«Право»
2023

УДК 343.98:001.895
І -66

Автори:

Шепітько В. Ю. – передмова, підрозд. 1.1, 1.3, 2.1; *Авдєєва Г. К.* – підрозд. 2.2, 2.3, 3.2, *Коновалова В. О.* – підрозд. 2.4; *Негребецький В. В.* – підрозд. 1.6; *Соколенко М. В.* – підрозд. 1.5, *Тарнавська Л. М.* – підрозд. 1.4, *Шевчук В. М.* – підрозд. 3.1, 3.3; *Яремчук В. О.* – підрозд. 1.2.

Рецензенти:

Глинська Н. В. – доктор юридичних наук, старший науковий співробітник, завідувачка відділу дослідження проблем кримінального процесу та судоустрою НДІ вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України;

Сімакова-Єфремян Е. Б. – доктор юридичних наук, професор, заслужений діяч науки і техніки України, заступник директора з наукової роботи Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України

Рекомендовано до друку вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України (протокол № 14 від 13 грудня 2023 р.)

І -66 **Інноваційні** методи, засоби та технології в криміналістиці та судовій експертизі : наук.-практ. посібник : електрон. наук. вид. / [Шепітько В. Ю., Авдєєва Г. К., Коновалова В. О. та ін.] ; за ред. В. Ю. Шепітька ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2023. – 116 с.

ISBN 978-966-998-682-5

Науково-практичний посібник присвячено проблемам застосування інноваційних методів, засобів і технологій у криміналістиці та судовій експертизі. У роботі розглянуто сучасні науково-технічні засоби та технології здійснення правозастосовної діяльності, досліджено можливості використання цифрової інформації та систем штучного інтелекту в кримінальному провадженні, визначено інноваційні підходи до використання інформаційних технологій під час проведення судових експертиз.

Для наукових співробітників, викладачів, аспірантів і студентів юридичних навчальних закладів освіти, а також співробітників органів правопорядку, представників судової системи, адвокатів та експертів.

УДК 343.98:001.895

Видання в електронному вигляді розміщується у відкритому доступі на сайті НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України в розділі «Електронні джерела» (https://ivpz.kh.ua/uk/електронна-бібліотека/) вкладки «Інфопідтримка». Для опису видання чи посилання на нього слід використовувати пряме URL-посилання.

ISBN 978-966-998-682-5

ЗМІСТ

Розділ 3
Цифрові технології та використання штучного інтелекту у правозастосовній практиці

Передмова

У сучасних реаліях технологізації та інформатизації суспільства важливого значення набувають тенденції щодо запровадження інноваційних методів, засобів та технологій у криміналістичну та судово-експертну діяльність. Йдеться про так звані інноваційні розробки – розроблення та використання новітніх науково-технічних засобів для виявлення, збирання, дослідження доказів, а також використання програмних продуктів та цифрових технологій. Європейський вектор розвитку криміналістики та судової експертизи обумовив необхідність впровадження прогресивних інституцій, використання найбільш ефективних методів та передових технологій.

Пропонований науково-практичний посібник присвячений актуальним проблемам щодо розроблення, впровадження та використання інноваційних методів, засобів та технологій у криміналістиці та судовій експертизі. Підготування даного посібника є результатом роботи лабораторії «Використання сучасних досягнень науки і техніки у боротьбі зі злочинністю» Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України та дослідження нею фундаментальної теми: «Інноваційні методи та цифрові технології в криміналістиці та судовій експертизі». Специфічним є те, що всі автори посібника – співробітники зазначеної лабораторії.

У науково-практичному посібнику відзеркалено сучасний розвиток криміналістики та судової експертизи, звернено увагу на формування доктринальних підходів, прослідковано можливості використання інноваційних методів та технологій у правозастосовній та експертній практиці. Також у посібнику акцентовано увагу на проблему використання цифрової інформації (цифрових доказів) та штучного

інтелекту в кримінальному провадженні, підкреслено їх значення для розслідування воєнних злочинів в умовах повномасштабної війни РФ проти України. Пропонований матеріал ґрунтується на емпіричних дослідженнях: вивченні слідчої, судової та експертної української і зарубіжної практики. Окремі положення проілюстровані результатами анкетування та інтерв'ювання судових експертів.

За своєю структурою науково-практичний посібник складається з трьох розділів та тринадцяти підрозділів. У першому розділі висвітлюються проблеми щодо тенденцій розвитку криміналістики та судової експертизи, приділено увагу криміналістичним та судово-експертним інноваціям, питанням використання науково-технічних засобів у криміналістиці, можливостям алгоритмізації під час проведення слідчих (розшукових) дій, а також використанню біометричних технологій в криміналістичній та експертній діяльності. Другий розділ присвячений ролі цифрових доказів у кримінальному провадженні. У цьому сенсі досліджено місце цифрових доказів та інституту доказування в доктрині криміналістики та судової експертизи, розглянуто поняття цифрових доказів, можливість їх використання у кримінальному провадженні, аргументовано роль формування цифрової криміналістики. У третьому розділі розглянуто проблеми та можливості використання цифрових технологій та штучного інтелекту в правозастосовній діяльності та під час розслідування кримінальних правопорушень.

У посібнику надано посилання на важливі нормативно-правові акти, довідкові та інші літературні джерела. До кожного розділу посібника сформульовано запитання для самоконтролю.

Науково-практичний посібник розраховано на співробітників правозастосування та судових експертів, а також науковців, викладачів та студентів.

Розділ 1

ІННОВАЦІЙНІ МЕТОДИ В СТРУКТУРІ КРИМІНАЛІСТИЧНОГО ЗАБЕЗПЕЧЕННЯ ОРГАНІВ ПРАВОПОРЯДКУ ТА СУДОВО-ЕКСПЕРТНИХ УСТАНОВ УКРАЇНИ

1.1. Європейський вектор розвитку криміналістики та судової експертизи в Україні

У Конституції України вказано на «європейську ідентичність Українського народу і незворотність європейського та євроатлантичного курсу України»[1]. У сучасних умовах розвиток криміналістики та судової експертизи в Україні характеризується зміненням вектору свого розвитку і наближенням до єдиного європейського криміналістичного простору.

Дослідження криміналістики як форми знання свідчить про змінення парадигми криміналістики та формування криміналістичної доктрини в структурі правової (юридичної) доктрини України[2]. У цьому сенсі важливого значення набувають підходи до «європеїзації права» як «ієрархічного впливу, що сконцентрований на перенесенні європейських цінностей, норм, стандартів, моделей, ідей і доктрин на рівень інших держав (здебільшого, європейського континенту)»[3].

---

[1] Див.: Абзац п'ятий преамбули Конституції України. *https://*zakon.rada.gov.ua/*laws/show/254k/96-вр#Text*

[2] Правова доктрина України: у 5 т. Т. 5: Кримінально-правові науки в Україні: стан, проблеми та шляхи розвитку / В. Я. Тацій, В. І. Борисов, В. С. Батиргареєва та ін. за заг. ред. В. Я. Тація, В. І. Борисова. Харків: Право, 2013. 1240 с.

[3] Асоціація між Європейським Союзом і третіми країнами: сучасний стан і динамізм в умовах інтеграції та дезінтеграції: монографія / К. В. Смирнова, О. В. Святун, І. А. Березовська та ін. Київ: ВПЦ «Київський університет», 2021. С. 87.

У незалежній Україні відбулися суттєві зміни в суспільстві, відмова від тоталітарних (репресивних) методів в управлінні державою, виключення ідеологічної складової науки, перехід від «криміналістики на службі слідства» до «змагальної криміналістики».

Сучасний розвиток науки в цілому та її окремих галузей пов'язано не лише з неймовірним пришвидшенням цього процесу, «інформатизацією» і глобалізацією, процесами взаємного запозичення і адаптації методів та технологій з інших наук, що призводить до появи якісно нових наукових дисциплін, але й необхідністю перманентного перегляду своїх теорій і концепцій, а на певних етапах й зміненню парадигм науки[1]. Доктринальні положення є результатом проведення фундаментальних наукових досліджень, які пов'язані з удосконаленням понятійного апарату, глибоким та всебічним аналізом сутності правових явищ і процесів, з'ясування закономірностей та тенденцій розвитку юридичної практики[2].

У літературних джерелах справедливо підкреслюється, що дотримання засади верховенства права передбачає розслідування кримінальних правопорушень і судовий розгляд справ згідно з кращим міжнародним та європейським досвідом[3]. Європейські підходи простежуються у пропонуванні переліку (системи) стардартів доказування, які мають застосовуватися під час кримінального провадження.

Формування єдиного європейського простору в галузі криміналістики та судової експертизи обумовлює необхідність уніфікації термінологічного апарату, розвиток мови науки. Тому, нагальною потребою було підготування і опублікування *енциклопедії з кримінального права, криміналістики та судових наук*, яка являє собою збірку понад 1800 термінів англійською мовою, що перекладаються українською, тлумачаться та ілюструються необхідними зображеннями та фотографіями. Окрім того, у цій роботі для окремих термінів

---

[1] Malevski H. Correlation Problem of Tactics and Strategy in Criminalistics and Law Enforcement Bodies Activity. *A First Printed Criminalist.* 2014. №9. P. 99–120.

[2] Правова доктрина України: у 5 т. Т. 1:Загальнотеоретична та історична юриспруденція / В. Я. Тацій, О. Д. Святоцький, С. І. Максимов та ін. за заг. ред. О. В. Петришина. Харків: Право, 2013. С. 7.

[3] Чорноус Ю. М. Вплив міжнародних договорів і практики Європейського суду з прав людини на розвиток криміналістики в Україні. *Право України.* 2021. №8. С. 79.

запропоновано їх синоніми (антоніми), а також надаються приклади їх можливого використання в словосполученнях (також з перекладом англійською мовою)[1].

Важливим кроком у наближенні криміналістики та судової експертизи до єдиного європейського криміналістичного простору є діяльність неурядових, українських громадських організацій криміналістів та їх взаємодія з національними асоціаціями (товариствами) європейських країн (Литовським товариством криміналістів, Польським товариством криміналістів, Словацьким товариством криміналістів, Німецькою асоціацією криміналістів та ін.)[2]. Значною подією стало підписання представниками України (Міжнародний Конгрес Криміналістів), Литви (Литовське товариство криміналістів) та Польщі (Польське товариство криміналістів) Харківського акту фундації Європейської Федерації Національних Товариств Криміналістів (Харків, 12 жовтня 2021, Варшава, 25 листопада 2021)[3].

Суттевим кроком у взаємодії національних асоціацій (товариств) європейських країн є реалізація міжнародних проектів та грантів. Яскравим прикладом є підготування спільних монографічних досліджень та підручників. Зокрема, у 2016 р. було підготовлено перший том підручника «Криміналістика» англійською мовою («Textbook of Criminalistics. Volume I: General Theory», 2016). У 2023 р. вийшов друком другий том підручника англійською мовою («Textbook of Criminalistics. Volume II: Criminalistic Technique and Tactics»), в якому взяли участь криміналісти Литви, України, Польщі та Словаччини.

Останнім часом деякі дослідники підкреслюють значення у запровадженні європейських стандартів забезпечення прав і свобод людини у судово-експертній діяльності[4], а також здійснюють порів-

---

[1] Шепітько В., Шепітько М. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. 508 с.

[2] See: Role of International and National Non-Governmental Organizations (Associations) in Criminalistics Development in Ukraine. *A First Printed Criminalist.* 2020. №20. P. 10–18.

[3] Kharkiv Foundation Act of European Federation of National Associations of Criminalists. *A First Printed Criminalists.* 2021. №21–22. P. 165–167.

[4] Шинкаренко І. Р., Спіцина Г. О. Щодо запровадження європейських стандартів забезпечення прав і свобод людини у судово-експертній діяльності. *Актуальні питання досудового розслідування та тенденції розвитку криміналістичних методик.* Харків, 2018. С. 211–213.

няльні характеристики законопроектів про судово-експертну діяльність[1]. При цьому, роль у розвитку міжнародного співробітництва у сфері судово-експертної діяльності має належати інституціям і документам ООН, а також співробітництву судово-експертних установ у межах Інтерполу[2].

На перспективи європейського співробітництва в галузі судової експертизи певна увага зверталася в сучасних джерелах[3]. У розділі IV Закону України «Про судову експертизу» регламентовано можливість міжнародного співробітництва в галузі судової експертизи. Зокрема, у ст. 23 Закону України «Про судову експертизу» передбачено можливість залучення фахівців з інших держав для спільного проведення судових експертиз. У статті 24 цього Закону вказано, що державні спеціалізовані установи, що виконують судові експертизи, користуються правом встановлювати міжнародні наукові зв'язки з установами судових експертиз, криміналістики тощо інших держав, проводити спільні наукові конференції, симпозіуми, семінари, обмінюватися стажистами, науковою інформацією і друкованими видан-

---

[1] See: Юодкайте-Ґранскієне Ґ., Фролов М. Порівняльна характеристика законопроєктів про судово-експертну діяльність. *Теорія та практика судової експертизи і криміналістики:* Харків: ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», 2022. Вип. 1 (26). С. 24–51.

[2] Шепітько І. Судово-експертна діядьність та експертне забезпечення правосуддя в Україні: міжнародний досвід та євроінтеграційні процеси. *Criminalistics and Forensic Expertology: science, studies, practice.* XVIII International Congress. Vilnius, 2022. P. 51

[3] Клименко Н. І., Купрієвич О. А. Міжнародне співробітництво судово-експертних установ. *Вісник кримінального судочинства.* 2015. №4. С. 130–134; Негребецький В. Перспективи європейського міжнародного співробітництва в галузі судової експертизи. *The formation and peculiarities of the implementation of the European Union's Eastern policy.* P. 202–213. URL: http://www.baltijapublishing.lv/*omp/index.php/bp/catalog/dawnload/246/6941/14447–1?inline=1*; Полянський А., Юодкайте-Ґранскієне Ґ. Зарубіжний досвід взаємодії судово-експертних установ між собою та з правоохоронними органами й можливості його використання в Україні. *Теорія та практика судової експертизи і криміналістики.* 2021. Вип. 2 (24). С. 26–51; Шепітько І. Судово-експертна діядьність та експертне забезпечення правосуддя в Україні: міжнародний досвід та євроінтеграційні процеси. *Criminalistics and Forensic Expertology: science, studies, practice.* XVIII International Congress. Vilnius, 2022. P. 46–52 та ін.

нями та здійснювати спільні видання в галузі судової експертизи і криміналістики[1].

На сьогодні національні інституції судових експертиз мають взаємодіяти з установами (організаціями, лабораторіями, центрами) судових експертиз інших європейських країн. Міжнародне співробітництво експертних установ є необхідним для обміну досвідом, підвищення кваліфікації фахівців судово-експертних установ, врахування сучасних досягнень науки і техніки, створення стандартизованих експертних методик. Важливим напрямом співробітництва в галузі судової експертизи є створення і функціонування міжнародних (європейських) судово-експертних мереж.

Значний вплив на судово-експертну діяльності здійснює розвиток взаємовідносин в межах Європейської мережі судово-експертних установ (European Network of Forensic Institutions – ENFSI)[2], що охоплює участь у цій організації, питання стандартизації та уніфікації судово-експертної діяльності, проведення тематичних конференцій, семінарів та симпозіумів, обмін експертними методиками, технологіями і довідковими матеріалами[3].

1.2. Використання криміналістичних інновацій у розслідуванні кримінальних правопорушень

На сьогодні криміналістика перебуває у постійному розвитку та розширенні власних меж. Цьому сприяє міжнародне співробітни-

---

[1] Закон України «Про судову експертизу» (Відомості Верховної Ради України (ВВР), 1994, №28, ст. 232. URL: *https://*zakon.rada.gov.ua*/laws/show/4038–12#Text*

[2] European Network of Forensic Institutions. URL: *https://tnfsi.eu*

[3] Див.: Заковирко О. М. Європейська мережа судово-експертних установ (ENFSI): історія створення та перспективи розвитку. *Актуальні питання стандартизації судово-експертного забезпечення правосуддя в Україні. Перспективи розвитку:* матер. міжнар. наук.-практ конф., присв. 105-річчю судової експертизи в Україні та 95-річчю з дня народження академіка М. Я. Сегая (4–5 липня 2018 р.). Київ: КНДІСЕ Мінюст України, 2018. С. 114; Клименко Н. І., Купрієвич О. А. Міжнародне співробітництво судово-експертних установ. *Вісник кримінального судочинства.* 2015. №4. С. 130–134; Лопата О. Зміст, завдання та форми міжнародного співробітництва у сфері судово-експертної діяльності. *Visegrad Journal on Human Rights.* 2016, №3. С. 97.

цтво та набуття українськими криміналістами і судовими експертами європейського досвіду щодо інноваційних положень криміналістики. Так, під час світової глобалізації зростає взаємозалежність країн світу, перетворення їх на єдиний глобальний організм, якому притаманні власні закони й тенденції розвитку. Не оминає глобалізація й питання розвитку права і юридичних наук[1] .

Криміналістика розвивається поряд із судовою експертизою та іншими судовими науками в цілому. Предмет судової експертизи пов'язаний із криміналістикою, оскільки дозволяє формувати й використовувати методики, що розроблені через застосування правил та алгоритмів, які були вироблені саме криміналістикою[2] .

В країнах Європи відсутнє єдине розуміння таких понять як «судова експертиза», «криміналістика» та «судова наука». Судовий експерт, формулюючи висновки за експертним провадженням, користується методиками та технологіями, які виробляються саме цими науками в різних наукових школах.

Використання інноваційного міжнародного досвіду у судовій експертизі та криміналістиці передбачає співпрацю між судовими експертами, криміналістами України та багатьох країн світу. У літературі вказується, що положення нормативно-правових актів національного та міжнародного характеру однозначно свідчать про те, що Україна є активним учасником міжнародного співробітництва у сфері судочинства, правоохоронної діяльності, юстиції та судово-експертної діяльності. Одним із важливих напрямів такої співпраці є обмін досвідом, спільне вирішення проблемних питань у зазначених галузях і визначення перспективних напрямів їх розвитку.[3]

---

[1] Сімакова-Єфремян Е. Б. До питання взаємозалежності європейських інтеграційних процесів і тенденцій інтегнрації спеціальних знань в Україні *Теорія та практика судової експертизи і криміналістики*: збірник наук. пр. Нац. наук. центр «Ін-т судових експертиз ім. Засл. проф. М. С. Бокаріуса, Нац. юрид. ун-т імені Ярослава Мудрого. Харків: ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса, 2017. Вип. 17. С. 152–158.

[2] Шепітько М. В. Концептуальні засади розвитку криміналістики та судових наук. *Архів кримінології та судових наук:* збірник наук. пр. Нац. наук. центр «Ін-т судових експертиз ім. Засл. проф. М. С. Бокаріуса, Нац. юрид. ун-т імені Ярослава Мудрого. Харків: ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса . 2020. Вип. 1. С. 94.

[3] Полянський А. , Юодкайте-Гранскієнє Габрієлє. Зарубіжний досвід взаємодії судово-експертних установ між собою та з правоохоронними органами й можливості

На сьогодні Україною укладена низка міжнародних договорів щодо співпраці у галузі судово-експертної діяльності із європейськими країнами та країнами близького і далекого сходу (Естонією, Грузією, Казахстаном, Латвією, Литвою, Молдовою, Узбекистаном, В'єтнамом, Китаєм, Македонією, Монголією, Польщею, Чехією та ін.). Ці акти встановили процедуру виклику експертів за кордон, гарантії захисту експертів, право на відшкодування експерту витрат на проїзд і перебування, право на оплату виконаної роботи та ін. Передбачено здійснення спільної наукової роботи з основних проблем судової експертизи, удосконалення наявних і створення нових методів і методик судової експертизи, обмін досвідом щодо інноваційної експертної практики [1]. Досвід європейських країн у галузі криміналістики і судової експертизи необхідно застосовувати в Україні. Зокрема, відбуваються постійні взаємообміни судовими експертами України та країн Європи. Приміром, експерти Київського інституту судових експертиз взяли участь у програмі обміну CEPOL 2021. У Словаччині вони ознайомилися із дослідженнями у галузі ідентифікаційних лазерних принтерів, документів особи, підробних банкнот різних країн, можливостями встановлення послідовності нанесення рукописних записів і друкованих текстів без їх спільних місць перетину[2]. Національним нуковим центром «Інститутом судових експертиз ім. Засл. проф. М. С. Бокаріуса» створені науково-дослідні проекти по запровадженню інноваційного досвіду європейських країн щодо криміналістики і судової експертизи: Український-латвійський науково-дослідний проєкт «Відкритий освітній ресурс: судов експертиза», Латвійсько-Естонський проєкт «Підтримка українських судових

його використання в Україні. Теорія та практика судової експертизи і криміналістики: збірник наук. пр. Нац. наук. центр «Ін-т судових експертиз ім. Засл. проф. М. С. Бокаріуса, Нац. юрид. ун-т імені Ярослава Мудрого. Харків: ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса 2021. Вип. 2 (24) 35 26–51

[1] Русецький А. А. Про організацію судово-експертної діяльності: міжнародний аспект. *Теорія та практика судової експертизи і криміналістики*: збірник наук. пр. Нац. наук. центр «Ін-т судових експертиз ім. Засл. проф. М. С. Бокаріуса, Нац. юрид. ун-т імені Ярослава Мудрого. Харків: ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса, 2017. Вип. 17. С. 161.

[2] Судовий експерт КНДІСЕ Сергій Науменко відвідав Словаччину за програмою обміну CEPOL. URL: https://kndise.gov.ua/sudovyj-ekspertkndise-sergij-naumenko-vidvidav-slovachchynu-za-programoyu-obminu-cepol/(дата звернення 20.11.2023)

експертів у документуванні військових злочинів, скоєних російською федерацією (ForUkraine)», Skeleton ID. [1]

На переконання К. С. Дмитрієвої, доцільно на законодавчому рівні внести до Закону України «Про судову експертизу» низку доповнень щодо міжнародного співробітництва судово-експертних установ, а також передбачити внесення відповідних змін до процесуального законодавства. Зокрема, повинно бути розроблено та впроваджено Стратегію розвитку міжнародного співробітництва судово-експертних установ України з компетентними органами іноземних держав та міжнародних організацій для забезпечення якості досліджень, застосування передових технологій та досвіду, вирішення стратегічних завдань, що виникають у нових соціально-політичних і економічних умовах[2].

Загальновідомо, що криміналістика є наукою, яка нині взаємодіє з різними галузевими науками. Є взаємозв'язок між криміналістичними знаннями, судовою експертизою і новітніми суміжними науковими знаннями з фундаментальних і прикладних наук. Інноваційним напрямком є дослідження, що мають комплексний характер та здійснюються разом криміналістами та спеціалістами з фізіології, кібернетики, біології, хімії тощо[3].

Є пропозиції утворити нові підрозділи науки криміналістики, а саме, аерокриміналістику, криміналістичну адвокатологію, судову графологію тощо, змінити зміст існуючих термінів, запроваджуючи інноваційні підходи. Варто відмітити про суміжні наукові дослідження, де застосовуються криміналістичні знання та знання з хімії, що проводяться у країнах Європи. Так, у журналі «Судова хімія» презентовані статті щодо застосування хімічних наук для криміналістичного аналізу, інноваційні дослідження щодо аналізу відбитків пальців, лікарських засобів, щодо виявлення та аналізу вибухових речовин, характеристик та порівняння слідів – скла, волокон, фарби

[1] Національний науковий центр «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса». Міжнародна діяльність URL:https://nncise.org.ua/diyalnist/mizhnarodna

[2] Дмитрієва К. С. Актуальні напрями розвитку міжнародного судово-експертного співробітництва. *Юридичний науковий електронний журнал*. Запоріжжя. 2022. С. 29.

[3] Юсупов В. В. Криміналістика в Україні у XX-XXI століттях: монографія. Київ: ФОП Маслаков, 2018. С. 445–461.

та полімерів, ґрунтів, чорнил та паперу, фальсифікованих ліків та інше[1]. Також виділимо інноваційний криміналістичний напрямок «судова архітектура». При Лондонському університеті працює дослідницьке агентство, що проводить новітні медіа- й архітектурні дослідження на вимогу міжнародних прокурорів, правозахисних організацій, політичних та екологічних правозахисних груп. Така діяльність сприяє отриманню нових видів доказів з використанням інноваційних науково-технічних засобів для моделювання події кримінального правопорушення, створення інтерактивних карт у міському або архітектурному масштабі, навігаційних 3D-моделей кримінального правопорушення[2]. Таким чином, дані про нові цифрові технології також мають використовуватися у криміналістиці та судовій експертизі з метою розкриття та розслідування кримінальних правопорушень.

Як приклад новітніх технічних засобів у галузі дактилоскопії можна назвати програму EVISCAN, розроблена у Німеччині дозволила експертам виявляти, покращувати якість та зберігати у цифровому вигляді маловидимі й невидимі відбитки пальців рук. Пристрій працює з відбитками без фізичного контакта і використання хімічних речовин. Відбитки пальців, речовини і ДНК зберігають у незмінному стані й придатні для ідентифікації через декілька років. Після вилучення, цифровий образ відбитку надсилається до різних баз даних, таких як, AFIS та EVRODAC і одразу використовується для ідентифікації осіб. AFIS є дактилоскопічною системою, що розроблена у США і на початку використовувалася ФБР під час розслідування кримінальних правопорушень, а потім для загальної ідентифікації. EVRODAC є дактилоскопічною базою даних Європейського Союзу для ідентифікації незаконних мігрантів й біженців. Крім того, для осіб, яких через вади пальців рук неможливо сканувати, вчені з Франції створили інноваційний сканер з «оптичною ко-герентною томографією», що спочатку використовували у медичних цілях для діагностування захворювань. Завдяки пристрою мож-

[1] José R. Almirall and Glen P. Jackson «Forensic Chemistry» Volume 14. 2019. URL: https://www.journals.elsevier.com/forensic-chemistry(дата звернення 12.11.2023).

[2] Forensic Architecture. URL: https://www.forensic-architecture.org/cases/(дата звернення 12.11.2023).

на отримати візерунок, що знаходиться під шкірою на глибині пів міліметра, який має ті самі топографічні ознаки, що і візерунок на зовнішньому шарі шкіри на пальцях рук. Щоб вийти на належний рівень впровадження інноваційних дактилоскопічних технологій, для правозастосовних органів України потребує оновлення матеріально-технічна база і обмін досвідом зі спеціалістами Західної Європи та США[1] У криміналістичній літературі перелічуються інноваційні техніко-криміналістичні засоби: 1) мас-спектрометри – для дослідження мікроскопічних частинок скла на місці події на рівні його атомної структури, приміром для порівняння мікрочасток скла на одязі злочинця з виявленими на місці події; 2) програма Xbox, що дозволила отримати доступ до прихованих файлів на жорсткому диску; 3) 3D реконструкція обличчя – для ідентифікації особи за знайденими залишками, зокрема за черепом; 4) секвенсер ДНК для дослідження давно вилучених кісток та зубів для ідентифікації особи; 5) дослідження змішаних зразків ДНК. Донедавна змішані зразки ДНК декількох осіб було неможливо розділити та ідентифікувати. Дослідники з Нової Зеландії розробили програму STRmix, що дозволило виокремити ДНК кожної особи; 6) гіперспектральна візуалізація видимої довжини хвилі дозволяє виявити найменші сліди крові та виокремити їх від інших слі-дів на місці події. Використовується камера, обладнена спеціальним жидкокристалістичним фільтром[2]. Слід звернути увагу і на нові прилади та комплекти багатофункціональних пристроїв для фіксації доказової інформації в «польових» умовах – «Польова міні фотолабораторія», що є комплектом сучасних науко-вотехнічних засобів, що дозволила співробітникам правоохоронних органів фіксувати доказову інформацію в «польових» умовах з використанням звукозапису, відео та фотозйомки, роздруковувати фотознімки високої якості, що дорівнює якості поліграфічного друку, без застосування комп'ютерної техні-

---

[1] Лапта С. П. Перспективні напрями розвитку дактилоскопії в зарубіжних країнах. *Вісник Харківського Національного університету внутрішніх справ* : зб. наук. пр. Харків : Харків. нац. ун-т внутр. справ, 2017. Вип. 3 (78). С. 59–66.

[2] Степанюк Р. Л. Новітнізарубіжнірозробкитаперспективнідослідженняугал узітехніко-криміналістичногозабезпеченняпротидіїзлочинності / Р. Л. Степанюк, С. П. Лапта . *Право і Безпека* : наук. журн. 2017. No 2. С. 96–101.

ки та електромережі, а також накопичувати, зберігати фонограми, фотознімки на електронному носії інформації.[1]

Важливим є запровадження до криміналістики та судової експертизи новітніх, інноваційних засобів та методів для розслідування військових кримінальних правопорушень. Допомогу надають колеги з інших країн, які використовують інноваційні науково-тнхнічні засоби, методи і методики криміналістики, що впровадженні у різних державах світу.

Актуальним є запровадження інноваційних криміналістичних науково-технічних засобів при розслідуванні воєнних злочинів. Так 3D-сканери, надані міжнародними партнерами, були використані для документування місць вчинення військових кримінальних правопорушень. Суттєву допомогу українським криміналістам та судовим експертам надають фахівці з Франції, Іспанії, Словаччини[2]. Польща надала Україні лазерні сканери «Z+F Imager 5016» для фіксування в 3D-моделі наслідків ракетних ударів по житлових будинках та критичній інфраструктурі (виробничим підприємствам, електростанціям, нафтопереробним заводам, мостам) документування пошкоджень багатоквартирних будинків, вулиць, торгових центрів, також фіксація наслідків артилерійських обстрілів та бомбардувань[3].

Криміналістикою розробляється такий новий її розділ, як аерокриміналістика, положення якої вже застосовані на практиці під час оглядів зруйнованих об'єктів внаслідок обстрілів рф. У Харківській області військові, правоохоронці здійснюють фіксацію за допомогою квадрокоптерів китайського, американського, литовського виробництва наслідків військових дій за допомогою квадрокоптерів. Відзняті відео дозволили зафіксувати масштаб руйнувань будівель і деталі, що не помітні з землі. Використання дронів під час слідчих (розшу-

---

[1] Інформаційні технології у правозастосовній діяльності. *Практикум з криміналістики* : навч. посібник / за ред.В. Ю. Шепітька. Київ : Ін Юре, 2013. 128 с.

[2] Міжнародна підтримка розслідувань воєнних злочинів. URL: https://yur-gazeta.com/publications/practice/mizhnarodne-pravo-investiciyi/mizhnarodna-pidtrimka-rozsliduvan-voennih-zlochiniv.html(дата звернення 12.11.2023).

[3] Буняк В. Нацполіція використовуватиме новітні 3D-сканери для документування російськихвоєннихзлочинівURL:https://ms.detector.media/withoutsection/post/33567/2023-11-25-natspolitsiya-vykorystovuvatyme-novitni-3d-skanery-dlya-dokumentuvannya-rosiyskykh-voiennykh-zlochyniv(дата звернення 12.11.2023).

ковых) дій убезпечує правоохоронців, адже є важкодоступні місця, де відбуваються руйнування, а також заміновані території[1].

До України надходить також інноваційне криміналістичне обладнання. Наприклад, французькі фахівці надали українським правоохоронцям мобільну ДНК-лабораторію, яку вперше застосували в місті Ізюм Харківської області.Проведені сотні ексгумацій та встановлення осіб загиблих, в тому числі, із застосуванням судовими експертами ДНК аналізу. Так, під час ексгумації тіл поблизу міста Ізюм, із місць поховань дістали 447 тіл загиблих. З них 215 жінок, 194 чоловіка, 22 військовослужбовця, 5 дітей. Загиблі мають ознаки насильницької смерті, а 30 з них сліди катувань. Є тіла з мотузкою на шиї, з поламаними кінцівками, зі зв'язаними руками, з вогнепальними ушкодженнями. Крім того, виявили рештки 11 осіб, стать яких наразі неможливо визначити. Їх передали для проведення судово-медичної експертизи. Загалом призначено більше тисячі судових експертиз, які допоможуть встановити причини загибелі громадян[2].

Звичайно, для України необхідна допомога фахівців іноземних країн, зокрема, Європи та США щодо проведення криміналістичних досліджень та судових експертиз із впровадженням інноваційних методів та методик. Так, В. Ю. Шепітько вважає, що сьогодні національні інституції судових експертиз мають взаємодіяти з установами (організаціями, лабораторіями, центрами) судових експертиз інших країн. Міжнародна співпраця експертних установ потрібна для урахування сучасних досягнень науки і техніки, підвищення кваліфікації фахівців судово-експертних установ, обміну досвідом, створення стандартизованих експертних методик[3] . Розслідування російських

[1] Байрачна Ю. На Харківщині за допомогою квадрокоптерів обстежили тисячі зруйнованих об'єктів. URL: https://www.ukrinform.ua/rubric-technology/3655812-aero kriminalistika-ak-droni-z-ludskimi-imenami-fiksuut-zlocini-rosian.html (дата звернення 12.11.2023).

[2] Баланчук І. В Ізюмі закінчили ексгумацію – підняли 447 тіл, серед них багато жінок, є діти. URL: https://www.pravda.com.ua/news/2022/09/23/7368817/ (дата звернення 12.11.2023)

[3] Шепітько В. Ю. Судова експертиза та судово-експертна діяльність: погляд крізь призму думок експертів. *Теорія та практика судової експертизи і криміналістики*. зб. наук. пр. Нац. наук. центр «Ін-т судових експертиз ім. Засл. проф. М. С. Бокаріуса, Нац. юрид. ун-т імені Ярослава Мудрого. Харків: ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса. 2023. Вип. 1. (30). С. 17.

воєнних злочинів наразі проводяться фахівцям у 21 державі, а також за підтримки Міжнародого кримінального суду. Їх роботі сприяє Консультативна група з розслідування кримінальних правопорушень проти людяності, створена у червні 2022 року ЄС, США та Великою Британією[1]. Варто відмітити, що у березні 2022 року створено спільну слідчу групу для розслідування кримінальних правопорушень росії, вчинених на території нашої держави, до якої увійшли Литва, Польща, Естонія, Латвія, Словаччина та Румунія. Дана група проводить збирання та зберігання доказів воєнних кримінальних правопорушень вчинених в Україні, такі як фотографії, відео та аудіозаписи, супутникові знімки, а також ДНК індикатори та відбитки пальців. Під час спільної діяльності групи правоохоронні органи країн-учасників оперативно обмінюються інформацією щодо ходу розслідування військових кримінальних правопорушень[2].

Отже, сьогодні у всьому світі застосовуються інноваційні підходи до формування багатьох наук. Не оминув цей процес і науки криміналістика і судова експертиза. Система криміналістики та судової експертизи постійно розвивається у взаємозв'язку з зі змінами наукових знань з фундаментальних і прикладних наук у світі. Для українських вчених, правоохоронців та судових експертів в умовах війни важлива міжнародна співпраця.

1.3. Інновації в судово-експертній діяльності

Судова експертиза є складовою ефективного правосуддя. Тому від належного реформування та оптимізації судово-експертної діяльності залежить відкриття істини, можливість вирішення справи за суттю, досягнення справедливості. Використання спеціальних знань у різних

[1] Собенко Н. Європол створив нову групу для розслідування злочинів росіян в Україні URL: https://suspilne.media/623791-evropol-stvoriv-novu-grupu-dla-rozsliduvanna-zlociniv-rosian-v-ukraini/(дата звернення 12.11.2023).

[2] Матола В. Міжнародна підтримка України у розслідуванні воєнних злочинів. URL: https://varosh.com.ua/vijna/mizhnarodna-pidtrymka-ukrayini-u-rozsliduvanni-vijskovyh-zlochyniv/ (дата звернення 12.11.2023).

формах судочинства (провадження) забезпечується завдяки здійсненню судово-експертної діяльності – особливого виду пізнавальної діяльності судового експерта. Останнім часом судова експертиза розглядається на рівні доктринальних підходів[1] та обранням нею європейського вектора свого розвитку[2]. У зв'язку із необхідністю визначення ролі судової експертизи в доказуванні та оптимізації судово-експертної діяльності виникла ідея звернення до позицій самих суб'єктів, що її здійснюють та проводять експертизи.

У 2022 році з метою визначення шляхів оптимізації судово-експертної діяльності було заплановано та проведено анкетування судових експертів державних спеціалізованих установ та інших фахівців (експертів) з відповідних галузей знань. В анкетуванні взяли участь 172 судових експерти зі стажем експертної роботи до 1 року було залучено 32 експертів (18,6%), від 1–3 років – 22 експертів (12,8%), від 3–5 років – 15 експертів (8,7%), від 5–10 років – 22 експертів (12,8%), від 10–15 років – 17 експертів (9,9%), від 15–20 років – 24 експертів (13,6%), понад 20 років – 40 експертів (23,3%)[3].

Опитані експерти були фахівцями з різних галузей науки, техніки, мистецтва або ремесла: природничі та технічні науки представляли 112 експертів (65,1%), гуманітарні науки – 33 експерти (19,2%), юридичні науки – 21 експерт (12,2%), інші напрямки – 6 експертів (3,5%).

---

[1] Див.: Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. *Право України*. 2021. №8. С. 12–27; Клюєв О., Сімакова-Єфремян Е. Доктринальні підходи до судової експертизи в Україні. *Право України*. 2021. №8. С. 28–43.

[2] Журавель В. А., Шепітько В. Ю. Розвиток криміналістики та судової експертизи в Україні: наближення до єдиного європейського простору. *Правова наука України: сучасний стан, виклики та перспективи розвитку:* монографія. Харків: Право, 2021. С. 651–669; Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України.* 2022. №2. С. 76–90.

[3] Результати проведеного анкетування судових експертів України були опубліковані раніше. Див.: Шепітько В. Ю. Судова експертиза та судово-експертна діяльність: погляд крізь призму думок судових експертів. *Теорія та практика судової експертизи і криміналістики.* 2023. Вип. 1(30). С. 12–22. URL: https://khrife-journal.org/index.php/journal

За навантаженням щодо здійснення експертної діяльності експерти розподілилися у такий спосіб: мають дуже високе навантаження 88 експертів (51,2%), надмірне – 72 експерти (41,9%), низьке – 9 експертів (5,2%), інше – вказали 3 експерти (1,7%). Причинами дуже високого навантаження експерти назвали: великий обсяг роботи щодо проведення експертизи – вказав 71 експерт (41,3%), складність дослідження – 42 експерти (24,4%), значна кількість звернень до проведення таких досліджень – 34 експерти (19,8%), відсутність (неналежна кількість) експертів за відповідною спеціальністю – 27 експертів (15,7%), інше – 3 експерти (1,7%).

Під час анкетування судових експертів були поставлені запитання щодо розуміння сутності спеціальних знань. Спеціальні знання – це знання у галузі науки, техніки, мистецтва, ремесла та знання і навички в конкретних видах діяльності, необхідні для їх використання у судочинстві[1].

На думку опитаних судових експертів спеціальними знаннями є: знання у галузі науки, техніки, мистецтва або ремесла вказали 96 експертів (56,4%), знання в конкретних видах діяльності – 68 експертів (39,5%), знання юридичні – 3 експерта (1,7%), знання загальнодоступні – 2 експерта (1,2%), інше – 3 експерта (1,7%).

Судова експертиза є процесуальною формою використання спеціальних знань і науково-технічних досягнень в юридичному провадженні. Судова експертиза – дослідження судовим експертом на основі спеціальних знань матеріальних (матеріалізованих) об'єктів (речових доказів) та різного роду матеріалів і документів, які містять доказову інформацію, з метою встановлення фактичних даних, що мають значення для правильного вирішення справи (провадження)[2].

Під час анкетування судових експертів було з'ясовано позицію щодо співвідношення судової експертизи та судово-експертної діяльності. Більшість судових експертів – 102 експерти (59,3%) вважа-

---

[1] Велика українська юридична енциклопедія у 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 325.

[2] Велика українська юридична енциклопедія у 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія / редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 257.

ють, що судова експертиза та судове-експертне дослідження повністю співпадають. 59 експертів (34,3%) зайняли позицію, що судова експертиза є ширшою за судово-експертне дослідження, а 6 експертів (3,5%) вказали, що судове-експертне дослідження є ширшим за судову експертизу. 5 експертів (2,9%) мали іншу думку з цього приводу.

На сьогодні національні інституції судових експертиз мають взаємодіяти з установами (організаціями, лабораторіями, центрами) судових експертиз інших країн. Міжнародне співробітництво експертних установ є необхідним для обміну досвідом, підвищення кваліфікації фахівців судово-експертних установ, врахування сучасних досягнень науки і техніки, створення стандартизованих експертних методик. Важливим напрямом співробітництва в галузі судової експертизи є створення і функціонування міжнародних (європейських) судово-експертних мереж. Значний вплив на судово-експертну діяльності здійснює розвиток взаємовідносин в межах Європейської мережі судово-експертних установ (European Network of Forensic Institutions – ENFSI), що охоплює участь у цій організації, питання стандартизації та уніфікації судово-експертної діяльності, проведення тематичних конференцій, семінарів та симпозіумів, обмін експертними методиками, технологіями і довідковими матеріалами[1].

Значна кількість опитаних експертів схиляються до думки про необхідність міжнародного співробітництва у сфері здійснення судово-експертної діяльності. Позитивну відповідь щодо необхідності у такому співробітництві надали 164 експерти (95,3%). При цьому, на їх думку таке співробітництво може виявлятися: у входженні до міжнародних експертних організацій (наприклад, ENFSI) – вказали 94 експерта (54,7%), у наданні допомоги з боку зарубіжних колег у програмному та технічному забезпеченні – 83 експерта (48,3%),

[1] Див.: Заковирко О. М. Європейська мережа судово-експертних установ (ENFSI): історія створення та перспективи розвитку. *Актуальні питання стандартизації судово-експертного забезпечення правосуддя в Україні. Перспективи розвитку:* матер. міжнар. наук.-практ конф., присв. 105-річчю судової експертизи в Україні та 95-річчю з дня народження академіка М. Я. Сегая (4–5 липня 2018 р.). Київ: КНДІСЕ Мінюст України, 2018. С. 114; Клименко Н. І., Купрієвич О. А. Міжнародне співробітництво судово-експертних установ. *Вісник кримінального судочинства.* 2015. №4. С. 130–134; Лопата О. Зміст, завдання та форми міжнародного співробітництва у сфері судово-експертної діяльності. *Visegrad Journal on Human Rights.* 2016, №3. С. 97.

у проведенні спільних наукових досліджень з проблем судової експертизи – 77 експертів (44,8%), у проведенні спільних наукових заходів з судової експертизи – 70 експертів (40,7%), у проведенні комісійних судових експертиз за участю зарубіжних експертів – 63 експерта (36,6%), у підвищенні якості послуг з проведення судової експертизи – 52 експерта (30,2%), у запрошенні зарубіжних експертів до проведення судових експертиз – 47 експертів (27,3%), у виданні спільних наукових видань (збірників, журналів, тощо) – 46 експертів (26,8%), інше – 3 експерта (1,7%).

Законодавчі зміни передбачають підвищення якості судово-експертної діяльності та її оптимізацію, недопущення підготування неправдивих висновків, зменшення кількості помилок в експертній практиці. Сьогодні в Україні до невідкладних заходів віднесено розробку низки законопроектів, які стосуються й реформування судово-експертної діяльності і, зокрема, запровадження рецензування висновку судового експерта. У цьому сенсі виникає ціла низка запитань: яка мета такого рецензування, кому це вигідно, хто буде оцінювати висновок експерта і здійснювати рецензування? Важливим є й питання, що стосується процесуальної сутності рецензії на висновок експерта. Висновок експерта – джерело доказів, а що таке «рецензія»? У сучасних умовах однією з особливостей оцінки висновку експерта є необхідність спеціального мотивування підстав, за якими відкидається висновок. Окрім того, якщо є сумніви щодо результатів судової експертизи можливо призначення та проведення повторної експертизи, залучення комісії експертів, проведення допиту експерта в суді.

Анкетування судових експертів продемонструвало добросовісність підходу фахівців до своєї діяльності та результатів експертизи. Більшість експертів висловили позитивне ставлення до рецензування висновку експерта іншим судовим експертом (експертами). На запитання про відношення до рецензування висновку експерта позитивно відповіли 102 експерта (59,3%), негативно – 56 експертів (32,6%), 14 експертів (8,1%) висловили іншу думку.

Проведення судових експертиз передбачає використання різних методів, методик та технологій. Зокрема, методика проведення судової експертизи – це комплекс рекомендацій щодо організації і здійснення судовим експертом своїх професійних функцій під час про-

ведення судової експертизи з метою формування свого висновку (*forensic report*) або судження (*expert opinion*)[1].

Під час анкетування судових експертів було з'ясовано, яким чином опитувані визначаються із методами дослідження під час проведення судової експертизи. Отримані такі відповіді: користуюся експертною методикою, яка розміщена в електронному реєстрі – Реєстрі методик проведення судових експертиз – позначили 88 експертів (51,2%), обираю залежно від сфери спеціальних знань і конкретного предмета дослідження – відмітили 80 експертів (46,5%), маю власну експертну методику – вказали 3 експерта (1,7%), інше – зазначив 1 експерт (0,6%).

Правова регламентація судово-експертної діяльності має бути спрямована на оптимізацію та підвищення рівня якості проведення судових експертиз. З цією метою запроваджуються різні електронні реєстри (електронні бази даних). Зокрема, в Україні розрізняють атестованих судових експертів, які внесені до державного Реєстру атестованих судових експертів. Ведення цього реєстру покладається на Міністерство юстиції України.

В Україні запроваджено Реєстр методик проведення судових експертиз з метою оптимізації роботи судових експертів. У ст. 8 Закону України «Про судову експертизу» зазначається, що методики проведення судових експертиз (крім судово-медичних та судово-психіатричних) підлягають атестації та державній реєстрації в порядку, що визначається Кабінетом Міністрів України.

Результати опитування продемонстрували відношення судових експертів до чинного Реєстру методик проведення судових експертиз. У цьому сенсі були отримані такі дані: Реєстр потребує свого вдосконалення – зазначили 70 експертів (40,7%), Реєстр має важливе практичне значення – вказали 64 експерта (37,2%), Реєстр не містить змісту експертних методик – відмітили 34 експерта (19,8%), інше позначили – 4 експерта (2,3%).

Під час анкетування судових експертів було з'ясовано питання про їх позицію до запровадження практики підготування розгорну-

[1] Шепітько В., Шепітько М. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. С. 286.

того висновку експерта (з наданням дослідницької частини). За результатами опитування отримані такі відповіді: необхідно залишити існуючу практику – вказали 136 експертів (79,7%), необхідно відмовитись від практики готування розгорнутих висновків експерта, а надавати лише відповіді на поставлені запитання – зазначили 35 експертів (20,3%), іншу думку мав 1 експерт (0,6%).

Судово-експертна діяльність віднесена до пізнавальної діяльності. Анкетування ставило за мету визначити методи пізнання, до яких звертається судовий експерт під час проведення експертизи. Зокрема, на запитання про те, чи висуває експерт версії під час проведення судової експертизи позитивно відповіли 110 експертів (64%), негативно – 58 експертів (33,7%), іншу думку висловили – 4 експерта (2,3%).

У сучасних умовах проведення судових експертиз пов'язано із інноваційними підходами та застосуванням інформаційних технологій. За результатами анкетування судових експертів було встановлено, що 92 експерта (53,5%) використовує у своїй практиці Автоматизоване робоче місце (АРМ) експерта, 75 експертів (43,6%) – не використовує Автоматизоване робоче місце (АРМ) експерта, 5 експертів (2,9%) – вказали на іншу позицію.

1.4. Проблеми використання науково-технічних засобів в криміналістиці

Протидія злочинності спрямована на забезпечення прав людини. Під час досудового розслідування та судового розгляду мають бути дотримані права людини і громадянина з метою того, «щоб кожний, хто вчинив кримінальне правопорушення, був притягнутий до відповідальності в міру своєї вини, жоден невинуватий не був обвинувачений або засуджений, жодна особа не була піддана необґрунтованому процесуальному примусу і щоб до кожного учасника кримінального провадження була застосована належна правова процедура» (ст. 2 КПК України). Досягти такої мети можна тільки із використанням

належних науково-технічних засобів в кримінальному провадженні. Слід звернути увагу, що такі науково-технічні засоби можуть використовувати як сторона обвинувачення, так і сторона захисту. Хоча зрозуміло, що сторона обвинувачення у використанні науково-технічних засобів має домінування (використання слідчої валізи, приладів, інструментів, які дозволяють фіксувати доказову інформацію). У сучасних умовах важливими стають науково-технічні засоби, які дозволяють зафіксувати цифрову інформацію (з комп'ютерів, гаджетів, мереж та серверів). Загальною тенденцією у світі стає залучення спеціалістів та судових експертів до процесу фіксації, дослідження та оцінки доказової інформації, які використовують науково-технічні засоби та спеціальне лабораторне обладнання.

Таким чином, науково-технічні засоби у протидії злочинності відіграють важливу роль в забезпеченні прав людини, що впливає на ефективне поновлення у правах компетентними національними судами та обґрунтованість пред'явленого кримінального обвинувачення.

Історія використання науково-технічних засобів в криміналістиці

Відомий вчений та батько криміналістики Ганс Гросс[1] отримав славу фундатора обґрунтування криміналістики як науки, практичної діяльності та університетської дисципліни, ввів у науковий обіг термін «криміналістика», заснував Інститут криміналістики Грацького університету імені Карла і Франца (K. K. Krimianalistischen Universitatinstitutes) та часопис «Archiv fur Kriminal-Anthropologie und Kriminalistik», розробив Музей криміналістики Грацького університету імені Карла і Франца, винайшов слідчий портфель (tatortkoffer), реформував правоохоронну та судову системи, вищої юридичної системи Австрійської імперії та інших європейських держав, був активним учасником Міжнародного криміналістичного союзу (Internationale Kriminalistische Vereinigung).[2]

Дослідження біографії Ганса Гросса дозволяють вказати на те, що його життя завжди було пов'язано із створенням інноваційних

[1] Mühlbacher T. Elementary, my Dear Holmes! Hans Gross, Father of Criminalistics, and Arthur Conan Doyle. *A First Printed Criminalist*. # 18, 2019. P. 11–23.

[2] Шепітько В., Шепітько М., Нежурбіда С. Hans Gross. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. С. 204.

криміналістичних засобів та новітніх інституцій, які діяли з метою найбільш ефективної боротьби зі злочинністю. Одним із таких новітніх на той час науково-технічних засобів боротьби зі злочинністю стало створення Гансом Гроссом слідчої валізи (портфеля). Він був створений з метою пошуку та фіксації слідів на місці події та за деякими даними був представлений на виставці криміналістичної техніки в Дрездені (1903)[1].

Зразок відомої слідчої валізи, створеної Гансом Гроссом, зберігається в Криміналістичному музеї імені Ганса Гросса (Hans Gross Kriminalmuseum) Грацького університету і є його центральним об'єктом[2]. На офіційному сайті Криміналістичного музею вказується, що Ганс Гросс зібрав інструменти, необхідні для роботи на місці злочину. Ці предмети він носив із собою у так званій «комісійній сумці» (commissionstasche) – «валізи місця злочину» (tatortkoffer). Вона містить технічне обладнання, вимірювальні прилади та речовини, необхідні для проведення хімічних аналізів, а також файли, письмові матеріали та офіційні печатки[3]. Також відзначається, що «для допиту дітей у слідчій валізі міститься банка з цукерками, тому що: «цей простий засіб перетворює дитину, що плаче, повзає, в сміливого, оповідаючого, довірливого свідка». Сигари повинні служити подібній меті: «кілька запасних сигар можуть мати таке ж значення для курців, оскільки в поспіху часто забувають портсигар або погано його наповнюють. Розтин без куріння досить дратує, принаймні для нас, юристів, навіть з великим досвідом»[4]. Онлайн екскурсія Криміналістичним музеєм імені Ганса Гросса дає можливість не тільки детального ознайомлення із наповненням слідчої валізи, але й надає його розміри –

[1] Чисников В. Н. Ганс Гросс – основоположник науки криминалистики и кримінальной психологии (к 170-летию со дня рождения). *Криміналістичний вісник*, №2 (28), 2017. С. 150.

[2] Bacchiesl C. The Hans Gross Museum of Criminology at the Karl-Franzens-University Graz. URL: https://edoc.hu-berlin.de/bitstream/handle/18452/9291/32.pdf?sequence=1

[3] Hans Gross Kriminalmuseum. URL: https://gams.uni-graz.at/

[4] Swoboda N. CSI Graz – und das vor mehr als 100 Jahren. *Austria Forum*. Mit freundlicher Genehmigung zur Verfügung gestellt von der Kleinen Zeitung (Montag, 28. Dezember 2015). URL: https://austria-forum.org/af/Wissenssammlungen/Essays/Bildung/Hans_Gross

15,8 х 54 х 42 см[1]. Фактично відоме Керівництво для судових слідчих[2] став порадником, яке могли напряму використовувати слідчими разом із слідчою валізою для досягнення найбільш ефективного результату. Потрібно погодитися із С. І. Нежурбідою, що «діяльність Гросса, його здобутки, прагнення до досконалості в своїй справі, вважаємо, мають стати яскравим прикладом у діяльності сучасних науковців»[3].

Слідча валіза стала настільки вдалим, своєчасним та зручним науково-технічним засобом, що використовуються вже більше 100 років і залишається актуальним сьогодні. І саме з розроблення Гансом Гроссом слідчої валізи як науково-технічного засобу можна розпочати історію використання таких засобів в криміналістиці.

Поняття науково-технічних засобів в криміналістиці. Науково-технічний прогрес та цифровізація забезпечують створення умов як для вчинення нових кримінальних правопорушень (за прикладом кіберзлочинності), так і для протидії її проявам. У сучасних реаліях протидія злочинності здійснюється представниками правоохоронних органів (правопорядку) через застосування комплексу заходів та науково-технічних засобів, які дозволяють збирати, досліджувати, використовувати та оцінювати докази.

В. Ю. Шепітько визначає науково-технічні засоби як «прилади, пристосування та матеріали, які використовуються для збирання, дослідження та використання доказів або створення умов, що ускладнюють вчинення злочинів»[4]. В. В. Пясковський підтримує та фактично повторює цей підхід, однак розширюючи його певним чином. Так, він визначає науково-технічні засоби як «прилади, інструменти, пристосування і матеріали, які використовуються для збирання і до-

[1] Hans Gross Kriminalmuseum. URL: https://gams.uni-graz.at/o:km.9063

[2] Gross H. Handbuch fur Untersuchungsrichter Polizeibeamte, Gendarmern u.s.w. Graz, 1893. 620 p.

[3] Нежурбіда С. Ганс Гросс: людина, вчений, вчитель. Вісник академії прокуратури України, № 3, 2006. С.121.

[4] Шепітько В. Ю. Засоби науково-технічні (техніко-криміналітичні). Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертиза, юридична енциклопедія / редкол. В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 299.

слідження доказів або створення умов, що утрудняють учинення злочинів»[1].

Більш широкого підходу дотримується Р. В. Комісарчук, акцентуючи увагу на криміналістичній техніці крізь «окремі матеріальні засоби», таким чином фактично включаючи науково-технічні засоби у «засоби криміналістичної техніки». При цьому Р. В. Комісарчук відносить до засобів криміналістичної техніки: «прилади, інструменти, пристрої, матеріали, речовини, їх набори й комплекти, що застосовуються для виявлення, вилучення, фіксації та дослідження слідів злочину й інших речових доказів»[2]. Подібного підходу дотримуються й інші автори, вказуючи на засоби криміналістичної техніки та їх класифікацію[3]. На нашу думку, такий підхід є дещо спірним оскільки за його використання необхідно розмежувати «науково-технічні засоби» та «засоби криміналістичної техніки» та надати визначення засобів криміналістичної техніки (замість надання їх переліків) та класифікувати їх. Видається, що засоби криміналістичної техніки є більш ширим явищем, ніж науково-технічні засоби, та можуть поділятися на: 1) науково-технічні засоби в криміналістиці; 2) інші засоби криміналістичної техніки (матеріали та речовини, які застосовуються в криміналістичних цілях).

З метою визначення науково-технічних засобів в криміналістичних засобів необхідним є виокремлення ознак цього явища. У цілому слід відзначити, що в криміналістиці не здійснювався аналіз ознак науково-технічних засобів. Разом із цим В. Г. Гончаренко та група авторів академічного курсу з криміналістики все ж таки акцентують увагу на одній, проте важливій загальній ознаці всіх комплектів науково-теххнічних засобів, – «найбільш можлива їх універсальність для оптимального виконання окремими суб'єктами своїх професійних функцій»[4].

---

[1] Пясковський В. В. Фондова лекція з навчальної дисципліни «Криміналістика» «Загальні положення криміналістичної техніки». Київ: НАВС, 2016. С. 9.

[2] Комісарчук Р. В. Техніко-криміналістичні засоби й методи, що застосовуються для виявлення, фіксації, вилучення та дослідження доказів. Кримінаілстика: підручник. За ред. В. В. Тіщенка. Одеса: Гельветика, 2017. С. 105.

[3] Криміналістика: підручник / В. В. Пясковський,, Ю. М. Чорноус, А. В. Іщенко, , О. В. Алєксєєв та ін. Київ: Центр учбової літератури, 2020. С. 69–72.

[4] Криміналістика: академічний курс / Варфоломеева Т. В., Гончаренко В. Г., В. І. Бояров, Гончаренко С. В., Попелюшко В. О. Київ: Юрінком Інтер, 2011. С. 60.

Важливою ознакою науково-технічних засобів є їх предмет. Так, науково-технічними засобами в криміналістиці прийнято вважати прилади, інструменти, пристосування і матеріали (В. Ю. Шепітько, В. В. Пясковський). На нашу думку, враховуючи популярність використання засобів криміналістичної техніки з цього переліку необхідно виключити матеріали, та віднести їх до «інших засобів криміналістичної техніки».

Також важливою ознакою стає мета використання науково-технічних засобів в криміналістиці. На нашу думку, слід виходити з того, що такі науково-технічні засоби можуть використовуватися не тільки під час збирання, дослідження, та використання доказів, але й під час їх оцінки. Зрозумілий акцент того, що науково-технічні засоби можуть використовуватися під час збирання, дослідження та виористання доказів, а також «для створення умов, що утрудняють учинення злочинів» (В. Ю. Шепітько, В. В. Пясковський). Однак, на нашу думку, перспективний стає їх використання і під час оцінки доказів, що особливо виявляється в перспективах застосування штучного інтелекту (ШІ)[1], коли прийняття оцінка доказів та прийняття рішення буде здійснюватися з елементами ШІ, відповідної програми та науково-технічного засобу.

Важливою ознакою визначення науково-технічного засоба в криміналістиці стає й суб'єкт їх застосування. На нашу думку, таким суб'єктом є професійний учасник кримінального провадження – слідчий, детектив, прокурор, дізнавач, оперативний співробітник, суддя, адвокат, спеціаліст чи судовий експерт.

З врахуванням названих ознак ***науково-технічним засобами в криміналістиці*** слід вважати *прилади, інструменти та пристосування, які використовуються слідчим, детективом, прокурором, ді-*

[1] Андрощук Г. Штучний інтелект у системі правосуддя: інтерв'ю з ChatGTP. Юридична газета online. URL: https://yur-gazeta.com/publications/practice/zahist-intelektualnoyi-vlasnosti-avtorske-pravo/shtuchniy-intelekt-u-sistemi-pravosuddya-intervyu-z-chatgtp.html; Колумбійський суддя використав штучний інтелект ChatGPT для вирішення справи. Юридична газета online. URL: https://yur-gazeta.com/golovna/kolumbiyskiy-suddya-vikoristav-shtuchniy-intelekt-chatgpt-dlya-virishennya-spravi.html$; Штучний інтелект vs судді: пілотний проєкт від Вищої ради правосуддя. Everlegal. URL: https://everlegal.ua/shtuchnyy-intelekt-vs-suddi-pilotnyy-proekt-vid-vyschoyi-rady-pravosuddya

знавачем, оперативним співробітниом, суддею, адвокатом, спеціалістом або судовим експертом для збирання, дослідження, оцінки та використання доказів або створення умов, що ускладнюють вчинення кримінального правопорушення.

Види науково-технічних засобів в криміналістиці

В. Ю. Шепітько виокремлює такі науково-технічні засоби і розподіляє їх на декілька груп: «1) запозичені з різних галузей науки і техніки без спеціального пристосування до задоволення потреб криміналістики (фото-, відеоапаратура загального призначення, засоби звукозапису, персональні комп'ютери персональні комп'юетри, тощо); 2) запозичені з різних галузей науки і техніки та спеціально пристосовані до задоволення потреб криміналістики (мікроскопи, електроліхтарі зі спеціальними насадками); 3) спеціально створені для задоволення потреб криміналістики (фотороботи, набори для виявлення слідів рук шляхом окурювання парами йоду, магнітні дактилоскопічні щіточки, набори для дактилоскопіювання, роботи з мікрооб'єктами, експрес-аналізу наркотичних засобів, тощо)»[1].

На нашу думку, важливе місце серед науково-технічних засобів займає слідча валіза, яка отримала популярність при його первинній розробці ще Гансом Гроссом *(див. вище)*. Слідча валіза (слідчий портфель, слідча сумка) на сьогодні розуміється як «набір або комплект техніко-криміналістичних та інших засобів (приладів, пристосувань, інструментів, матеріалів) для роботи з доказами під час проведення слідчих (розшукових) дій – слідчого огляду, обшуку, слідчого експерименту та ін.»[2]. Також окремо наголошується, що слідча валіза «використовується при проведенні різних слідчих (розшукових) дій для вивчення та фіксації матеріальної обстановки злочину, виявлення, фіксації, вилучення і збереження доказів, їх попереднього дослідження, а також при підготовці об'єктів для експертизи. Слідчі

[1] Шепітько В. Ю. Засоби науково-технічні (техніко-криміналітичні). Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертиза, юридична енциклопедія / редкол. В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. С. 299.

[2] Шепітько В. Валіза слідча.Велика українська юридична енциклопедія: у 20 т.: Т. 20: Криміналістика, судова експертиза, юридична психологія. Харків: Право, 2018. С. 62.

валізи бувають трьох типів: універсальна (призначена для вирішення різноманітних завдань), спеціалізована (для роботи експерта-криміналіста, працівника дорожньої поліції, спеціаліста-вибухотехніка та ін.) і набір зі змінним змістом (формуються безпосередньо перед проведенням певної слідчої (розшукової) дії)». Також відзначається, що в Україні розроблено комплект пошукових засобів слідчого (набір-пошук), комплект науково-технічних засобів огляду місця ДТП, комплект науково-технічних засобів для огляду місця пожежі (набір-пожежа), комплект науково-технічних засобів для огляду ВП і місця вибуху (набір-вибух), комплект науково-технічних засобів для роботи з мікрооб'єктами (набір «Мікро» або «Молекула»), комплект науково-технічних засобів роботи зі слідами рук (дактилоскопічний набір), комплект слідчого для огляду документів, оперативний одорологічний комплект[1]. У іноземній традиції створення слідчих валіз (*crime scene investigation kit, forensic kit*) відзначається формування спеціалізованих валіз для збирання доказів зґвалтування (*rape kit*)[2] або сексуального насильства (*sexual assault kit*)[3]. Важливим також стає те, що «з розвитком техніко-криміналістичних засобів спостерігається зміщення у їх використанні від слідчого до спеціаліста та судового експерта на місці вчинення кримінального правопорушення»[4].

Прикладом таких науково-технічних розробок може стати універсальний криміналістичний комплект слідчого (модифікація «С»), який випускається компанією «Кримтех експерт». Такий засіб являє собою комплект техніко-криміналістичних та інших засобів (прикладів, пристосувань, інструментів, матеріалів) для роботи зі слідами та речовими доказами під час огляду та інших слідчих дій, який призначений для органів досудового слідства[5].

---

[1] Шепітько В. Валіза слідча.Велика українська юридична енциклопедія: у 20 т.: Т. 20: Криміналістика, судова експертиза, юридична психологія. Харків: Право, 2018. С. 62/

[2] Шепітько В., Шепітько М. Rape Kit. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. С. 350.

[3] Шепітько В., Шепітько М. Sexual Assualt Kit. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. С. 377.

[4] Шепітько В., Шепітько М. Forensic Kit. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. С. 182.

[5] Кримтех експерт здійснює. Криміналіст першодрукований, № 1, 2010. С. 78.

Таким чином, Гансу Гроссу, батькові криміналістики, вдалося створити науково-технічний засіб, – слідчу валізу, – яка пережила її створювача на більше ніж століття. При цьому, актуальність використання слідчої валізи та інших подібних криміналістичних та експертних комплектів не втрачається. Нові типи та види таких валіз створюються та отримують нові рішення. що дозволяють ефективніше працювати із доказами з метою їх збирання та дослідження. Таким чином, підкреслюємо перспективність використання комплектів (наборів) науково-технічних засобів, перш за все, з метою збирання, дослідження та використання доказів.

Особливу цінність становить в цілях судово-експертного забезпечення здійснення правосуддя складає лабораторне обладнання (включаючи пересувні лабораторії), яке використовується судовими експертами (спеціалістами, інспекторами-криміналістами, техніками-криміналістами) під час досудового розслідування або судового розгляду. Таке лабораторне обладнання стає залежним від матеріалів та речовин, певних криміналістичних та судово-експертних реєстрів, криміналістичних та судово-експертних методів, які ними використовуються.

У цілому науково-технічні засоби є змінюваним, на що впливає науково-технічний прогрес та загальна цифровізація інформації. Вже відбувся перехід від плівкових на цифрові фотоапарати, кінокамер на цифрові відеокамери та фотоапаратами, сканери можуть здійснювати 3D фіксацію, відтворення дій, обстановки, обставин певної події може здійснюватися у віртуальному просторі, що дозволяє не тільки зберегти інформацію, але й отримати додаткову і встановити механізм вчинення кримінального правопорушення.

У цьому сенсі слід звернути увагу не тільки на аудіо-, фото-, відео-, комп'ютерну, лабораторну техніку, за допомогою, якою здійснюється фіксація інформації або її дослідження, але й серйозний розвиток програмного забезпечення, методів та технологій, які дозволяють отримати додаткові криміналістично-значущі дані для розслідування злочинів.

На нашу думку, слід звернути увагу на створення фотороботів, методів автоматичної обробки фото-, відеоданих (в тому числі з ви-

користанням штучного інтелекту), створення 3D зображень та мапування вчинених кримінальних правопорушень. Так, «науково-технічним засобом, який забезпечує комплексну фіксацію оточуючий обстановки із здійсненням точного відображення зовнішнього вигляду, форми, вимірюванням відстаней між об'єктами, їх взаємного розташування та розмірів є лазерний 3D сканер»[1].

У цілому такі підходи підвищують вірогідність встановлення механізму вчинення кримінальних правопорушень, відшукування слідів на місці вчинення кримінального правопорушення навіть через певний час, здійснювати їх дослідження (в тому числі судово-експертне) за допомогою спеціальних програм. Саме тому, на нашу думку, таке спеціальне програмне забезпечення, може бути віднесено до науково-технічних засобів спеціально створених для задоволення потреб криміналістики.

Пандемія, викликана COVID-19 та повномасштабна російська агресія проти України також здійснили суттєвий вплив як на форми здійснення кримінального судочинства, так і на методи збирання та дослідження доказів воєних злочинів. Так, участь учасників кримінального провадження під час досудового розслідування/судовому засіданні стала можлива в режимі відеоконференції (ст.ст. 35, 206–1, 232 КПК України). Розвиток також отримали й комп'ютерна форенсіка (кіберкриміналістика) та цифрова криміналістика. Кіберкриміналістику прийнято розуміти як здійснення дослідження комп'ютера та інформаційних мереж спеціалістом (судовим експертом) для досудового розслідування та судового розгляду з метою встановлення незаконного обігу інформації та імовірних осіб причетних до таких дій[2], а цифрову криміналістику – як окрему криміналістичну теорію та вид судової експертизи, що ставить своїм завданням дослідження цифрових доказів з використанням криміналістичної техніки та наявних методик в цілях досудового розслідування та судового розгляду[3].

[1] Семенов В. В. Перспективні технічні засоби та методи в розслідуванні злочинів. Сучасні тенденції розвитку криміналістики та кримінального процесу. Харків: ХНУВС, 2017. С. 193.

[2] Шепітько В., Шепітько М. Кримінальне право, криміналістика та судові науки: енциклопедія Харків: Право, 2021. С. 121.

[3] Шепітько В., Шепітько М. Кримінальне право, криміналістика та судові науки: енциклопедія Харків: Право, 2021. С. 121.

Такі окремі напрями криміналістики вказують на те, що такі дослідження можуть здійснюватися лише через використання спеціально створених програм, методик дослідження цифрової інформації, що певним чином видозмінює розуміння науково-технічного засобу, яке в більшості зводилося до певного предмету матеріального світу (пристроїв, апаратури, інструментів, їх наборів, тощо). Так, С. Белл вважає найбільш вражаючою зміною в розслідуванні злочинів за останні 25 років з'явлення цифрового отримання зображень, що дозволило отримати потужні засоби для збирання, аналізу та збереження зображень[1]. Подібний перехід пізніше відбувся й щодо реконструкції вчинених кримінальних правопорушень (наприклад, пов'язаних із ДТП).

Таким чином, науково-технічний прогрес вказує на те, що самі науково-технічні засоби змінюють свої якості, надають можливість як зберігати, так і досліджувати криміналістично-значущу інформацію в цифровій формі. Слід констатувати, що змінюється акцент з дослідження предметів матеріального світу на віртуальні (цифрові), що потребує змінення підходів як в розумінні науково-технічних засобів, так і в їх використанні.

1.5. Використання можливостей алгоритмізації під час проведення слідчих (розшукових) дій

В сучасних умовах важливою передумовою підвищення ефективності розслідування кримінальних правопорушень виступає активне впровадження в практику діяльності органів досудового розслідування сучасних досягнень науки і техніки, вагомими з яких є цифрові (комп'ютерні) технології. Серед основних науково-технічних засобів оптимізації діяльності слідчого слід назвати персональний комп'ютер, обладнаний спеціалізованими програмами, базами та відповідними

[1] Bell S. Forensic Science. An Introduction to scientific and investigative techniques. 5th edition. Boca Raton, London, New York, 2019. 348 p.

периферійними пристроями. На сьогодні суттєво розширилися потенційні можливості використання слідчим цифрових технологій за багатьма напрямками його професійної діяльності.

Перспективним напрямом оптимізації слідчої діяльності необхідно визнати можливість запровадження кібернетичних підходів і пов'язаних з цим перспектив використання цифрової техніки шляхом побудови і застосування відповідних алгоритмів слідчих (розшукових) дій. Адже алгоритми здатні істотно скоротити витрати часу для підготовки і проведення слідчих (розшукових) дій, надати цьому процесу більшої керованості, оскільки слідчий, спираючись на розроблені в науці алгоритми, має можливість в тих випадках, коли є готові типові рішення не займатися їх винаходом, а брати і використовувати апробовані, оптимальні прийоми та їх системи.

Алгоритми слідчих (розшукових) дій можуть бути надані в описовій чи формалізованій формах. На теперішній час більш поширеною є описова форма, що являє собою узагальнені рекомендації, викладені на десятках сторінок відповідних посібників або у вигляді спеціальних таблиць. Формалізована форма подання алгоритмів допиту передбачає можливість використання цифрових засобів роботи із необхідними даними, що зосереджені у пам'яті комп'ютера і реалізовані у відповідних програмах. Вона дозволяє більш швидко і зручно скористатися певною інформацією, отримати методичну допомогу, сприяє поповненню відсутніх досвіду та знань. Таким чином, можна зробити висновок, що формалізація численних практичних рекомендацій на теперішній час та у майбутньому потрібніше слідчій практиці, чим їх детальний опис.

При цьому треба мати на увазі, що алгоритм це лише елемент програми, причому далеко не єдиний. Систематизовані відповідним чином алгоритми слідчих (розшукових) дій в сукупності з іншими практичними рекомендаціями утворюють програму, що включає різні алгоритми дій слідчого, провадження кожного з яких, у свою чергу, може програмуватися. Вказана програма повинна містити не тільки жорстко детерміновану систему дій (алгоритмів), а також правила рекомендаційного характеру, що забезпечують можливість багатоваріантного підходу до визначення шляхів і засобів вирішення

завдань, залежно від ситуації, що склалася. Перевага цифрових (комп'ютерних) програм полягає у тому, що вони характеризуються множинністю кроків та варіативністю ситуацій. Алгоритми, у свою чергу, завжди мають лише вихідну слідчу ситуацію, певне типове завдання і чітку послідовність застосування тактичних прийомів. Тобто, програма має більш узагальнену структуру у порівнянні з алгоритмом і за своїм змістом менш формалізована, аніж останній.

Алгоритмізація являє собою розробку та використання алгоритмів діяльності слідчого або, в більш вузькому розумінні, підхід до проведення слідчих (розшукових) дій, що заснований на запровадженні оптимальних варіантів рішень в залежності від слідчих ситуацій, що склалися. Алгоритмізація здатна допомогти слідчим продуктивно користуватись узагальненими знаннями, прийомами, зменшити кількість помилок і упущень. При цьому алгоритми слідчих (розшукових) дій виступають своєрідним акумулятором значного досвіду, підвищують ефективність слідчої діяльності, перетворюють її на програмно-керовану й більш прогнозовану.

Разом з цим, на базі алгоритмізації слідчих (розшукових) дій стає можливим підбір оптимальних тактичних прийомів, запровадження кращих варіантів їх обрання залежно від ситуацій. Водночас важливим є те, щоб алгоритм не обмежувався вичерпним переліком прийомів, слідчих дій, тактичних операцій, а насамперед орієнтував слідчого на послідовність і порядок їх здійснення. Враховуючи ту обставину, що слідчий працює в умовах дефіциту часу й екстремальних ситуацій, то алгоритми повинні бути чіткими та лаконічними, тобто мати опис процедури здійснення прийомів у формі певної цифрової (комп'ютерної) програми.

Необхідно зазначити, що алгоритмізація слідчих (розшукових) дій можлива саме тому, що оптимальний перелік дій залежить не від випадкових факторів, а від різноманітних, але все ж типових та прогнозованих слідчих ситуацій. Але зважаючи на неоднорідність і неповторність конкретних ситуацій, що складаються при проведенні слідчих (розшукових) дій, це істотно ускладнює розробку алгоритмів. Тому мова повинна йти не про жорстку формалізацію діяльності слідчого, а лише про окремі її аспекти. Водночас, зазначене не може

бути підставою для відмови від алгоритмізації, оскільки при всій формалізації алгоритм зберігає евристичний характер, що забезпечує свободу прийняття рішення слідчим при проведенні слідчих (розшукових) дій.

Тому важливим є те, що індивідуальність кожної слідчої (розшукової) дії вимагає творчого підходу до реалізації кожного кроку алгоритму, можливості його зміни або використання іншого, більш відповідного. Враховуючи, що слідча (розшукова) дія у більшості випадків визначається тією слідчою ситуацією, що складається у даний момент часу, а остання є тим фактором, що визначає необхідність та доцільність провадження оптимальної системи прийомів, тобто обумовлює побудову певних алгоритмів. При цьому різні за ступенем складності ситуації вимагають побудови різних алгоритмів.

Так, проста ситуація передбачає наявність більш чітких, сталих алгоритмів, з меншою кількістю варіантів на виконання. Йдеться про управлінські алгоритми, наприклад, алгоритми, що визначають характер і послідовність дій слідчого до виїзду на місце події, після прибуття на місце тощо. І, навпаки, складна ситуація, котра має декілька варіантів вирішення, потребує більш ускладненого, з різноманітною кількістю кроків алгоритму, зокрема встановлення психологічного контакту при проведенні допиту, подолання надання неправдивих відомостей допитуваним.

Дійсно, при підготовці до допиту перед слідчим за будь-яких ситуацій постають завдання інформаційної, організаційної та технічної спрямованості. При вирішенні інформаційних завдань слідчий зобов'язаний ретельно ознайомитись із матеріалами кримінальної справи, отримати додаткову інформацію про особу допитуваного та його стосунки із оперативних джерел, отримати необхідні консультації від спеціалістів в тій чи іншій галузі знань. У свою чергу, організаційні завдання передбачають з'ясування місця і часу допиту, кола його учасників, складання плану допиту. Технічні пов'язані із процедурою застосування передбачених чинним законодавством додаткових засобів фіксації результатів допиту. Всі ці завдання за своїм характером є усталеними і повторюються щодо різних суб'єктів допиту, а тому їх розв'язання можливе за рахунок застосування певних

алгоритмічних приписів, які викладені у вигляді цифрових (комп'ютерних) програм і надані в розпорядження слідчих.

Як видається, найбільш стабільними є ситуації при розв'язанні не пізнавальних, а організаційних завдань, що виникають на етапі підготовки до проведення слідчих (розшукових) дій. Саме на цьому етапі завдання є найбільш спрощеними, такими, що повторюються і піддаються розчленуванню на свої складові, а тому придатні до розв'язання формалізованими засобами. Виходячи із вищезазначеного можна констатувати, що найбільш придатною сферою для побудови алгоритмів слідчих (розшукових) дій слід визнати його підготовчий етап.

Отже, алгоритмізація здатна забезпечити правильну організацію роботи слідчого (детектива), істотно зменшити кількість помилок і невдач, сприяє зваженому, раціональному вирішенню завдань, що постають перед ним. Водночас, недостатність наукових розробок щодо створення та впровадження алгоритмів дій професійних учасників кримінального процесу в різноманітних ситуаціях вимагають більш поглибленого дослідження проблем алгоритмізації як на теоретичному, так і на практичному рівнях.

1.6. Біометричні технології в криміналістиці та судовій експертизі

У зв'язку з війною в Україні особлива роль відводиться роботі правоохоронних органів щодо посилення національної безпеки, попередження і профілактики кримінальних та інших правопорушень, створення безпекового середовища для підтримання і розвитку країни в цей важливий час. Останнє можливе через впровадження в правоохоронну діяльність сучасних систем захисту і контролю доступу до життєво важливих інформаційних цифрових систем і мереж, доступ до яких є у більш ніж однієї людини. Захист необхідно для забезпечення схоронності інформації, надійної працездатності й запобігання несанкціонованого доступу в систему. Для виконання покла-

дених функцій така система безпеки виконує ідентифікацію користувачів, перевіряє особу й визначає їхні повноваження.

Історично ідея перевірки особи була пов'язана з використанням документа, що підтверджував особу, і ґрунтувалася переважно на використанні певних даних. Цей же принцип ліг в основу новітніх технологій з використанням пластикових бейджів, магнітних смарт-карток з електронним чи оптичним пристроєм запам'ятовування. В цих системах передбачений досить високий рівень захисту від підробок, копіювання і фальсифікації. Разом з тим технічним системам притаманна одна дуже суттєва вада: орієнтування на верифікацію самого предмета авторизації – картку, бейдж, посвідчення, а не на саму персону-власника. Система контролю доступу в даному разі відстежує проходження карток без підтвердження ідентичності персони, що скористалась ними. Іншими словами, картка може бути загублена, викрадена, передана і використана іншою особою.

Для більш точного й однозначного визначення користувача інформаційної системи застосовують біометричну ідентифікацію, яка охоплює збір і аналіз поведінкових і фізіологічних особливостей людини. У якості біометричних характеристик людини можуть виступати: райдужна оболонка й сітківка ока, відбитки пальців, геометрія руки, геометрія зовнішності людини, голос, хода, почерк тощо. На відміну від традиційних систем ідентифікації, біометричні методи мають ряд переваг – немає необхідності намагатися не забути або не втратити ключ доступу, пароль та ін. Крім того, біометричні пристрої відрізняються зручністю використання, і вписуються в сучасні стандарти безпеки.

Ідея створення біометричних систем була пов'язана з необхідністю створення систем безпеки до стратегічних об'єктів. Така технологія потрібна для того, щоб в автоматичному режимі розпізнати конкретну особу, якій у випадку підтвердження особи буде наданий доступ до об'єкта.

Біометричні системи розповсюджені й широко використовуються в різних сферах життя людини. Завдяки автоматизації та швидкості роботи розпізнавання особи біометричні технології є дуже корисними в будь-якій галузі діяльності людини, де необхідно перевірити і підтвердити особу за її біометричними характеристиками. Це може бути

безпека, оборона, міграційні процеси, банківська сфера та моніторинг, та ін. Причому дати вичерпний перелік сфер застосування біометричних технологій на сьогодні вже є неможливим, оскільки сама ідея перевірки й підтвердження особи людини вже більше і більше стає привабливою і асоціюється з безпекою.

Історично розробка й провадження біометричних систем було пов'язано з необхідністю створення систем безпеки до важливих об'єктів. Така технологія потрібна для того, щоб в автоматичному режимі розпізнати конкретну особу, якій у випадку підтвердження особи буде наданий доступ до об'єкта[1].

Біометрична технологія – це автоматизовані методи розпізнавання особи людини, засновані на фізіологічних або поведінкових характеристиках.[2] Прикладами розпізнавання за фізіологічними характеристиками є ідентифікація людини за формою обличчя, термограмою обличчя, за відбитком пальця, за формою кисті руки, за розташуванням вен на лицьовій стороні долоні, за сітківкою ока, за райдужною оболонкою ока. До поведінкових характеристик належать особливості або характерні риси, такі що їй притаманні від природи або були придбані в процесі навчання: динаміка підпису, ідентифікація голосу, динаміка натискання на клавіші.

Для того, щоб технологія була біометричною, необхідно, щоб вона була придатна для використання автоматизованими засобами, тобто без участі людини – контролера, швидко в реальному часі.

Немаловажною характеристикою біометричної технології є здатність одержання так званого біометричного зразка (або вибірки) з наданих для аналізу ознак об'єкта. Наприклад, в автоматизованих системах дактилоскопічної реєстрації спочатку отримують дактилокарту, яка далі перетворюється в цифровий графічний файл. Далі система в автоматичному режимі аналізує й розпізнає ідентифікаційні ознаки будови папілярних ліній. У результаті на екрані комп'ютера

---

[1] Мороз А. О. Біометричні технології ідентифікації людини: огляд систем. Математичні машини і системи. 2011. №1. С.39–45. URL:http://dspace.nbuv.gov.ua/handle/123456789/83397.

[2] Велика українська юридична енциклопедія: У 20 т. Т.20: Криміналістика, судова експертиза, юридична психологія / редкол. В. Ю. Шепітько та ін. Харків : Право, 2018. с.50.

відображається дактилокарта з розпізнаними ознаками. Далі оператор має можливість підкорегувати розміщення ідентифікаційної ознаки на графічному зображенні, якщо відбулася помилка розпізнавання. Після підтвердження оператором правильності дій програма зберігає біометричний зразок.

Якщо технологія біометрична, то до зразка пред'являються такі вимоги: він не повинен займати багато місця. Згідно з існуючими у світі стандартами для різних біометричних технологій − це декілька кілобайт. Це пов'язане з тим, що біометричний зразок може бути переданий по каналах зв'язку, і важлива швидкодія такої системи. Чим менше місця займає зразок у біометричній базі, тем менше сама база й швидше проводиться пошук.

Необхідною характеристикою біометричної системи є ступінь стійкості до помилок[1]. Це означає низький відсоток помилок, які можуть бути допущені при розпізнаванні. Причому мова йде про два різновиди помилок: 1. помилка неправильної відмови (FRR – False Reject Rate); 2. помилка неправильного пропуску (FAR – False Accept Rate). Помилка неправильної відмови виникає у випадку, якщо система не розпізнала об'єкт по наявному зразку, а помилка неправильного пропуску – у випадку, якщо система розпізнала об'єкт, який не відповідає зразку. Біометрична система допускає лише невеликий відсоток помилок, тому характеризується підвищеною точністю.

На даний час наука біометрія, як сукупність методів і технологій автоматичної ідентифікації й підтвердження особи людини, активно розвивається. В наукових дослідженнях біометрії активну участь беруть десятки наукових центрів при університетах, деякі наукові організації, Biometrics Research Group (Michigan State University, USA)[2] , Biometrics Institute[3] та комерційні фірми Biomerics[4] .

Відповідно в розслідуванні кримінальних правопорушень поширене використання біометричних технологій. Однак на сьогодні

---

[1] Швець В. А., Фесенко А. А. Основні біометричні характеристики, сучасні системи і технології біометричної аутентифікації.. *Безпека інформації* (Ukrainian Scientific Journal of Information Security). 2013. №2. С.102.

[2] Biometrics Research Group. URL: https://biometrics.cse.msu.edu.

[3] Biometrics Institute. URL: https://biometricsinstitute.org.

[4] Biometrics. URL: https://biomerics.com/.

вже навіть така розповсюджена слідча (розшукова) дія, як допит в разі наявності у допитуваної особи біометричного паспорту (ID-card) передбачає використання біометричної технології для перевірки і підтвердження особи допитуваного. Істотно, що такі біометричні документи вже розповсюджені, і існують готові технічні розв'язання для реалізації цього завдання. Так, продовж довгого часу широке розповсюдження набули автоматизовані дактилоскопічні ідентифікаційні системи (АДІС), що використовуються в кримінальній реєстрації. В Харкові в 2002 році була введена в експлуатацію АДІС «Дакто-2000». Перевага такої системи, стало очевидним, коли в період із серпня 2002 р. по березень 2010 р. завдяки використанню цієї системи було встановлено 988 осіб, причетних до нерозкритих злочинів, установлені особи 629 невпізнаних трупів, 164 випадку приховання особами своїх анкетних даних, об'єднано 27 кримінальних проваджень[1]. Взагалі в експертній службі МВС України за роки існування функціонувало біля 10 різних видів і версій АДІС («Папилон», «Дактомат», «Монна Ліза», «Сонда», «Сонда+», «DEX», «УкрDEX» та ін.)[2].

З метою розшуку підозрюваних осіб використовуються біометричні системи. Так, у 2018 р. співробітники поліції в Чжэнчжоу, Китай одержали для роботи незвичайні сонцезахисні окуляри, оснащені програмним забезпеченням для розпізнавання осіб[3]. Ці устрої поліція Китаю досить успішно застосовує для піймання розшукуваних злочинців.

На Україні компанією «Техносерв Україна» ще в 2011 році було запропоновано «Каскад-Потік» – система автоматичної ідентифікації особи по відеозображенню обличчя в потоці людей, що дозволяє виконувати пошук на транспортних об'єктах, в місцях масового скупчення людей і в пунктах пропуску.

---

[1] Удовиченко О. А. Функціонування регіонального дактилоскопічного обліку в Науково-дослідному експертно-криміналістичному центрі при ГУМВС України в Харківській області. Криміналістичний вісник. 2010. №2. С.142.

[2] Хахановський В. Г. Автоматизація експертних дактилоскопічних досліджень. *Форум права*. 2011. №1. С.1081.

[3] Китайська поліція знаходить підозрюваних через окуляри. URL: https://www.bbc.com/ukrainian/news-42979942.

Столичне комунальне підприємство «Інформатіка» впроваджено новий аналітичний модуль відеоспостереження в рамках проекту «Безпечне місто» (Kyiv Smart Safe City)[1]. Унікальний модуль дозволяє шукати злочинців не тільки завдяки спеціалізованим камерам розпізнавання особи. Він фіксує зображення з будь-якої камери, установленої в рамках мережі й порівнює їх з наявною базою правопорушників. Якщо система виявляє подібність, оператор відразу одержує тривожний сигнал. Отже, правоохоронці зможуть швидше відслідковувати небезпечних злочинців. До складу нового аналітичного модуля розпізнавання осіб входить аналітична система й база даних, що полягає зі списку розшукуваних людей.

В криміналістичній літературі цифрові біометричні технології розглядають в основному як автоматизовані засоби безпеки в різних галузях життя суспільства. Але стосовно процесу розслідування злочинів, в літературних джерелах розглянуто лише окремі можливості використання біометричних систем і технології, причому в основному йдеться про боротьбу з тероризмом. Але місце і роль цих технологій в самому процесі розслідування кримінальних правопорушень, в тому числі транснаціонального масштабу залишаються недостатньо висвітленою.

Так, торгівля дітьми як кримінальне правопорушення має транснаціональний характер і створює загрозу Національній безпеці і оборони України, при цьому суттєво впливає на демографічні, міграційні, та інші процеси. Україна у глобальній системі торгівлі дітьми розглядається як країна походження «живого товару». Неповнолітніх в основному вивозять до країн Європи, Росії, країн Східної Азії. Дітей, якими торгують всередині країни, в основному використовують у сільському господарстві, на будівництві, ринках, у жебракуванні, злочинній діяльності та проституції. Так Мінсоцполітики України оприлюднило таку статистику за 2019 рік: 185 громадянам було встановлено статус особи, яка постраждала від торгівлі людьми, з яких 184 громадянина України та 1 іноземець

[1] У рамках проекту «Безпечне місто» запущено новий аналітичний модуль відеоспостереження, що прискорить пошук правопорушників. URL: https://kyivcity.gov.ua/news/u_ramkakh_proektu_bezpechne_misto_zapuscheno_noviy_analitichniy_modul_videosposterezhennya_scho_priskorit_poshuk_pravoporushnikiv/.

(громадянин Російської Федерації)[1]. Серед осіб, яким встановлено зазначений статус, 53 жінок, 119 чоловіків та 13 дітей (3 хлопчиків та 10 дівчаток). Протягом 2019 року: 65 осіб постраждало від торгівлі людьми в Україні, 120 осіб – від торгівлі людьми за кордоном. За видами експлуатації 85 осіб постраждало від трудової експлуатації, 40 осіб втягнуто у злочинну діяльність, 37 осіб від сексуальної експлуатації, 17 осіб використано у збройних конфліктах, 3 осіб використано у порнобізнесі, 1 особу залучено до жебракування, 1 особа постраждала від змішаної експлуатації (трудова та сексуальна експлуатації), 1 дитину було продано третім особам. Основними країнами призначення були: Російська Федерація – 65 осіб, Україна – 65 осіб, Республіка Польща – 11 осіб, Німеччина – 10 осіб, Чеська Республіка – 6 осіб, Турецька Республіка – 5 осіб, Республіка Білорусь – 4 особи, Китайська Народна Республіка – 4 особи, Італійська Республіка –3 осіб, Словацька Республіка – 2 особи, Королівство Бельгія – 2 особи, Об'єднані Арабські Емірати – 1 особа, Республіка Словенія – 1 особа, Республіка Казахстан – 1 особа, Федеративна Республіка Бразилія – 1 особа, Французька Республіка – 1 особа, Угорщина – 1 особа, Держава Ізраїль – 1 особа, Арабська Республіка Єгипет – 1 особа.

Біометричні технології успішно використовуються в діяльності міграційних служб майже у всіх країнах світу. Ідея перевірки й підтвердження особи людини при перетинанні державного кордону вже більше і більше стає привабливою і асоціюється з безпекою.

Біометричними називають документи, що посвідчують особу та містять електронний носій інформації, на якому записано інформацію про біометричні дані власника документу з метою його ідентифікації. Передбачається, що такі документи найбільш захищені від підробок та виключають можливість користування ними будь-якою особою, окрім власника. Головна ідея впровадження більш захищених документів, які забезпечують ідентифікацію особи – це суттєве підвищення захищеності суспільства від проявів злочинності та міжнародного тероризму.

[1] Мінсоцполітики відзвітувалося ГРЕТА про проведені у 2019 році Урядом України заходи щодо протидії торгівлі людьми. URL: https://www.msp.gov.ua/news/18685.html

Біометричні паспорти набувають все більшого поширення у світі[1]. Відповідно до інформації всесвітньої організації цивільної авіації (ІСАО) більше 90 країн з 193 держав-членів ООН в даний час видають такі документи, при цьому ще більше двадцяти держав готові до впровадження таких документів в найближчі роки.

Близько 45 країн з числа тих, які видають біометричні документи, зберігають на документах одночасно і відбитки пальців, і зображення особи, в той же час більше 30 країн використовують лише оцифроване фото власника документа. Решта країн в даний час використовують тільки зображення обличчя, але найближчим часом планують використовувати і дані дактилоскопії.

За даними ІСАО, більше 15 країн в даний час використовують автоматизовані контрольно-пропускні системи для власників електронних паспортів. Для того, щоб пройти процедуру паспортного контролю, мандрівник може скористатися «електронними воротами», які в автоматичному режимі звіряють його біометричні дані з інформацією, що зберігається на чипі документа. Серед країн, які читають (сканують) е-паспорта в аеропортах і на кордонах США, Великобританія, Сінгапур, Португалія, Нова Зеландія, Японія, Індонезія і Німеччина.

Ініціатором впровадження біометричних паспортів на державному рівні були США: в 2002 р. Конгрес США прийняв Закон про безпеку державних кордонів, відповідно до якого громадяни країн, які мали угоди зі США про безвізовий режим, могли безперешкодно в'їжджати на територію США строком до 90 днів тільки за умови наявності в них біометричних документів[2].

З 2004 р. у США розпочато програму US-Visit, що передбачала введення системи зняття відбитків пальців і фотографування всіх, що прибувають в Америку іноземців (115 аеропортів, 14 морських портів, 104 контрольно-пропускних пункти, біометрична база даних

---

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

[2] Homeland Security Act of 2002. URL: https://www.govinfo.gov/link/plaw/107/public/296?link-type=html

більш ніж на 5 млн осіб). Більш 80 країн миру (включаючи Афганістан, Бахрейн, Кувейт, Оман, Катар, Саудівську Аравію й ОАЭ) використовують програми електронних ID-card, у яких утримуються біометричні дані[1].

Найбільшої у світі системою біометричної ідентифікації в цей час є Aadhaar (Індія). Aadhaar-це індійський онлайн-сервіс ідентифікації, що надається державним агентством UIDAI. Станом на кінець березень 2021 р., у системі зареєстроване більш 1,28 млрд людей, що становить близько 90% громадян Індії[2].

З березня 2018 року посольство Саудівської Аравії в Україні запровадило обов'язкову процедуру зняття відбитків пальців у всіх бажаючих отримати візу до країни[3]. Процедура проводиться після подачі документів в попередньо призначений день і час.

На Україні 20.11.2012 р. було прийнято Закон «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» № 5492-VI, відповідно до якого передбачено введення документів з електронним носієм, на якому передбачається розміщення біометричних даних про особу[4]. В 2017 році Уряд України затвердив Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства[5]. Документом визначено, що це автоматизована система, створена в інтересах національної безпеки, економічного добробуту та прав людини, за допомогою якої забезпечується встановлення особи іноземця та особи без громадянства, які в'їжджають в Україну, виїжджають з України, здійснення контролю за додержанням ними правил перебування на території нашої держави.

---

[1] United States Visitor and Immigrant Status Indicator Technology (US-VISIT). URL: https://www.epic.org/privacy/us-visit/

[2] Unique Identification Authority Of India. URL: https://uidai.gov.in.

[3] Візу до Саудівської Аравії українцям необхідно отримати перед поїздкою. URL: https://tourpoint.com.ua/ua/vizy/asia/saudi-arabia.

[4] 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 . URL: https://zakon.rada.gov.ua/go/5492–17.

[5] Положення про національну систему біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства: Постанова КМУ від 27.12.2017 № 1073. URL: https://zakon.rada.gov.ua/laws/show/1073–2017-п#Text.

Державна прикордонна служба у грудні 2017 р. презентувала систему фіксації біометричних даних іноземців та осіб без громадянства[1]. Демонстрація роботи системи відбулася в столичному аеропорту «Київ». Ця система фіксації біометричних даних іноземців та осіб без громадянства розгортається прикордонним відомством на виконання Указу Президента України від 30 серпня 2017 року № 256 «Про рішення Ради національної безпеки та оборони України від 10 липня 2017 року «Про посилення контролю за в'їздом в Україну, виїздом з України іноземців та осіб без громадянства, додержання ними правил перебування на території України». Вона є однією з підсистем відомчої автоматизованої системи прикордонного контролю. Держприкордонслужба активно працює над вдосконаленням безпекової складової на кордонах України. Сьогодні технічні засоби Держприкордонслужби дозволяють зчитувати виготовлені за міжнародними стандартами ІКАО закордонні паспорти, в тому числі з вбудованим чіпом, ID-картки та водійські посвідчення. При цьому постійно вивчається досвід передових країн світу, європейських та американських партнерів щодо побудови систем автоматизації паспортного контролю. Кращі зразки обладнання впроваджуються у відомчу інформаційно-телекомунікаційну систему. 157 діючих пунктів пропуску обладнано засобами для зчитування інформації з біометричних документів, а 126 пунктів пропуску підключено до баз даних Інтерполу. З серпня 2017 року інформаційна система прикордонного відомства автоматично підраховує кількість дозволених діб перебування іноземців в Україні.

Запуск системи фіксації біометричних даних Держприкордонслужби – це ще один крок щодо покращення безпекової складової при перетинанні кордону та вдосконалення системи прикордонного контролю. під час паспортного контролю інспектори Держприкордонслужби здійснюватимуть перевірку паспортних документів іноземців, в тому числі за базами Інтерполу. Також відбуватиметься зчитування інформації (відбитки пальців) за допомогою рідерів, яка надходитиме

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

до підсистеми обробки біометричних даних відомства. Крім того, через міжвідомчу інформаційно-телекомунікаційну систему «Аркан» вона надходитиме до Національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства Державної міграційної служби. При повторному перетині особою кордону здійснюватиметься процес ідентифікації особи. При цьому інспектор бачитиме чи здавала людина свої біометричні дані і здійснюватиме їх перевірку. У разі не співпадіння даних особу буде направлено на додатковий контроль для з'ясування обставин.

Під час провадження окремих видів судових експертиз біометричні технології використовуються як елемент методики ідентифікаційного експертного дослідження. На сьогодні вже навіть під час проведення розповсюдженого різновиду криміналістичної експертизи, як дактилоскопічної, доцільне використання автоматизованої дактилоскопічної інформаційної системи (АДІС) на основі автоматичного аналізу і розпізнавання папілярних візерунків. Проте, такі інноваційні інформаційні судово-експертні системи на сьогодні розповсюджені тільки в кримінальній реєстрації. Так, продовж довгого часу широке розповсюдження набули автоматизовані дактилоскопічні ідентифікаційні системи (АДІС), що використовуються в кримінальній реєстрації. В Харкові в 2002 році була введена в експлуатацію АДІС «Дакто-2000»[1]. АДІС «Дакто-2000» використовується для криміналістичного обліку за слідами рук. За допомогою дактилоскопічного сканеру отримують зображення папілярних візерунків пальців, придатних для ідентифікації. Отримання зразків дактилоскопічної інформації зі сканера «Kojak 10 print roll scanner» зайняло 17 хвилин, відбитки мають необхідний розмір та розширення файлів bmp, png, що завантажуються в робочу програму АДІС «Дакто-2000», після цього спеціаліст отримує якість зображення достатню для розставлення інтегральних характеристик, встановлення загальних та індивідуальних ознак папілярних візерунків (ліній). Після подальшого програмного кодування та здійснення пошуку у базі даних за дактилоскопічним масивом інформації регіонального та, за необхідності,

[1] Удовиченко О. А. Функціонування регіонального дактилоскопічного обліку в Науково-дослідному експертно-криміналістичному центрі при ГУМВС України в Харківській області. Криміналістичний вісник. 2010. №2. С.140–144.

центрального рівнів АДІС «Дакто-2000» буде отримано перелік кандидатів для порівняння. Загальний час на отримання зразків, завантаження, опрацювання та перевірку за автоматизованим дактилоскопічним масивом АДІС складає до 30 хвилин[1].

При провадженні судових експертиз з метою ідентифікації причетних осіб використовуються цифрові технології біометричної ідентифікації. Зокрема, яскравим прикладом є судово-фоноскопічна експертиза (експертиза відеозвукозапису). Ідентифікація за голосом заснована на акустичних особливостях вимовляння, які у кожної людини унікальні. Голос відбиває як низку анатомічних особливостей (наприклад, розмір і форму горла та рота), так і звички, що набуваються людиною упродовж життя (гучність голосу, манера розмови).

Сучасна голосова біометрична технологія розбиває кожне вимовлене слово на низку сегментів. Записаний голосовий «відбиток» перетворюється на біометричний зразок, який зберігається в спеціальному банку даних. Для проведення ідентифікації індивідуума його просять відповісти на декілька питань здебільшого їх кількість не перевищує трьох), відповіді на які легко запам'ятовуються. Наприклад, повідомити прізвище, ім'я, по батькові та дату народження. Сучасні комп'ютерні системи автоматично створюють цифрову модель («відбиток») голосу, що надалі може зіставлятись із будь-якою фразою, вимовленою людиною[2].

За аналогічним алгоритмом працює голосова біометрія в банківській сфері. Так, на весні 2022 року Приватбанк впровадив технологію голосової авторизації, і вже станом на середину осені кількість користувачів, які скористалися функцією, перевищила мільйон людей[3]. Механізм роботи наступний:

---

[1] Осуховський Р. В., Кизименко С. Г. Використання технічних засобів дактилоскопіювання для ідентифікації осіб // Використання досягнень сучасної науки й техніки в розкритті злочинів: матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лютого 2021 р.). С.174–179. URL: https://www.naiau.kiev.ua/files/kafedru/ord/2021/ks-250221.pdf

[2] Захаров В. П., Рудешко В. І. Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. Львів: ЛьвДУВС, 2015. С.149.

[3] Що таке голосова біометрія: як працює і в чому переваги. URL: https://psm7.com/uk/technology/chto-takoe-golosovaya-biometriya-kak-rabotaet-i-v-chem-preimushhestva.html.

клієнт дзвонить у службу підтримки та починає пояснювати роботу (віртуальному асистенту) причину звернення;

у цей час технологія робить зліпок голосу і порівнює його з наявними у базі даних варіантами;

вже через кілька секунд клієнт ідентифікований, що суттєво прискорює та спрощує процес взаємодії.

Процедура біометричної ідентифікації за голосом дозволяє користувачеві позбутися тривалого і для багатьох заплутаного процесу підтвердження ризикованих операцій.

Яскравим прикладом використання біометричної технології в діяльності судового експерта є генотипоскопічна експертиза, або ДНК-аналіз, тобто дослідження мікрослідів на клітинному рівні. Це дозволяє ідентифікувати злочинця по слідах біологічного походження: крові, слини, (сперми), клітинах епітелію, частинах тканин і органів людини, волоссю.

Судова молекулярно-генетична експертиза розв'язує завдання ідентифікації особи методом ДНК-аналізу, в т.ч.: встановлення приналежності об'єктів біологічного походження (кров, сперма, слина, волосся, м'язова та кісткова тканини) певній особі, встановлення слідів біологічного походження конкретної особи у змішаних слідах, встановлення ідентичності останків у випадках розчленування трупа та ідентифікації жертв катастроф, коли живі близькі родичі, визначення спадковості певних генетичних ознак людини (біологічна спорідненість) – встановлення батьків дитини у випадках спірного батьківства, дітовбивства, крадіжки, підміни дітей[1].

Ідентифікація за ДНК ґрунтується на унікальності послідовності дезоксирибонуклеїнової кислоти у кожної людини. Процес починається з підготовки зразка ДНК індивідуума (що звичайно називається «контрольним зразком»). Для відібрання зразків використовується щічний мазок, а також кров, слина, інші виділення організму людини, тканини. Контрольний зразок з використанням спеціальної біометричної технології і обладнання аналізується для створення ДНК-профілю

[1] Види судових експертиз, які проводяться у лабораторії біологічних досліджень та питання які вони вирішують: Інформаційний лист. ДНДЕКЦ МВС України, Київський НДЕКЦ МВС України, 2017. URL: https://ndekc.kiev.ua/wp-content/uploads/2017/02/Інф.лист_ДНК-2017.pdf

людини. Такий профіль потім можна порівняти з іншим зразком, щоб визначити, чи є генетична тотожність. Процес отримання ДНК-профілю займає певний час. Тому сам метод для автоматичної ідентифікації особи в реальному часі ще не є придатним. Але для проведення судово-експертних досліджень метод ДНК-аналізу став поширеним. Метод використовується при провадженні судових експертиз, наприклад за кримінальними провадженнями при розслідуванні умисних вбивств[1].

Істотною особливістю є тісна інтеграція криміналістичних обліків та інформаційних біометричних систем. Так, актуальним аспектом використання судової генетики в системі кримінального правосуддя є створення та розширення централізованих національних баз даних. Такі бази містять генетичні профілі, які встановлюються і зберігаються відповідно до критеріїв, визначених у законодавстві кожної країни використання криміналістичних обліків генетичних ознак людини з інформаційно-пошуковими автоматизованими системами[2]. Автоматизовані криміналістичні обліки призначені для накопичування та зберігання отриманих в процесі дослідження даних, з метою подальшої перевірки шляхом порівняння їх з тими даними, що вже зберігаються в базі. Автоматизований облік генетичних ознак людини функціонує на центральному та обласних рівнях. Створення криміналістичних обліків генетичних ознак людини сприяло проведенню генетичного аналізу отриманих на місці злочину біологічних зразків, що багато в чому спростило роботу слідчих. Вони отримали надійний інструмент, що дозволяє ідентифікувати злочинця або його жертву, добувати незаперечні докази і розкривати злочини.

Використання автоматизованих систем реєстрації біометричних характеристик людини в зоні бойових дій надає можливості контролювати та запобігати кримінальні правопорушення. Так, в Іраку і Афганістані для збору даних американські військові використову-

---

[1] Вирок Немирівський районний суд Хмельницької області від 10.12.2021 по справі №930/1478/21. База даних «Єдиний реєстр судових рішень». URL: https://reyestr.court.gov.ua/Review/101784354.

[2] Ірина Єпринцева Актуальні питання криміналістичних обліків генетичних ознак людини. *Молодий вчений*. №9 (85) (2020). URL: https://molodyivchenyi.ua/index.php/journal/article/view/703/679.

вали системи BAT (Biometrics Automated Toolset) або HIIDE (Handheld Interagency Identity Detection Equipment)[1].

Комплект BAT складається з чотирьох частин-ноутбука, цифрової фотокамери, сканера відбитків пальців і сканера райдужної оболонки. Зібрані дані перевіряються по базі даних, яку містить ноутбук[2]. База періодично синхронізується з центральним сервером групи біометричних технологій. HIIDE − це мобільний термінал, який дозволяє фіксувати відбитки пальців, фотографії, зображення сітківки та біографічні дані, отримані в результаті опитування. Для збору даних про екіпажі морських суден і човнів застосовується спеціальний комплект, захищений від впливу води і підвищеного вібраційного впливу. Система HIIDES була розроблена для того, щоб Збройні сили США могли легко ідентифікувати людей в польових умовах і відрізняти друга від ворога.

Отже, використання цифрових біометричних технологій в розслідуванні і запобіганні кримінальним й іншим правопорушенням і судово-експертній діяльності, під час підтримання правопорядку в умовах воєнного стану на Україні є край доцільним. Проведене дослідження дозволяє визначити найдоцільніші напрями застосовування біометричних технологій і систем: 1) в системі механізмів Національної безпеки і оборони України; 2) в системах контролю та запобіння кримінальним правопорушенням в зоні бойових дій; 3) в автоматизованих системах відеоспостереження й розшуку з технологією біометричної ідентифікації; 4) в автоматизованих системах, що забезпечують використання біометричних документів для посвідчення особи (наприклад, біометричний паспорт); 5) в автоматизованих системах кримінальної реєстрації з метою накопичення криміналістично значущої інформації для використання її в майбутньому, в тому числі як матеріалів для судової експертизи; 6) в судово-експертній діяль-

[1] Kelsey Atherton. The enduring risks posed by biometric identification systems (09.02.2022). URL: https://www.brookings.edu/techstream/the-enduring-risks-posed-by-biometric-identification-systems/

[2] Biometric Automated Toolset (BAT) and Handheld Interagency Identity Detection Equipment (HIIDE). URL: https://www.nist.gov/system/files/documents/2021/03/23/ansi-nist_archived_vermury-bat-hiide.pdf

ності при проведенні окремих видів ідентифікаційних досліджень (судово-фоноскопічна експертиза, генотипоскопічна).

Запитання для самокотролю

1. Які сучасні тенденції у розвитку криміналістики та судової експертизи в Україні?
2. Які перспективи європейського співробітництва в галузі судової експертизи в сучасних умовах?
3. Які новітні галузі криміналістики пов'язані з інноваційним розвитком?
4. Які науково-технічни засоби впроваджуються як інноваційні в діяльність органів правопорядку?
5. Що відноситься до інновацій у судово-експертній діяльності?
6. Що таке науково-технічні засоби в криміналістиці?
7. Які існують види науково-технічних засобів у криміналістиці?
8. Хто розробив першу слідчу валізу?
9. Що таке біометрична технологія?
10. Які біометричні технології використовуються в криміналістичних та експертних цілях в сучасних умовах?

Розділ 2

РОЛЬ ЦИФРОВИХ ДОКАЗІВ В ДОКАЗУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

2.1. Місце цифрових доказів в доктрині криміналістики та судової експертизи

На сьогодні розвиток криміналістики та судової експертизи обумовлений науково-технічним прогресом світового співтовариства, запровадженням новітніх технологій. Прикладами використання новітніх інформаційних технологій є пропонування дистанційних форм досудового розслідування та судового розгляду, проведення процесуальних дій у дистанційному режимі, режимі відеоконференцзв'язку, формування електронного кримінального провадження (справи), розроблення та впровадження різного роду єдиних реєстрів (наприклад, єдиний реєстр судових рішень, єдиний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань, єдиний реєстр боржників, державний реєстр атестованих судових експертів, реєстр методик проведення судових експертиз та ін.).

Певним брендом цифрової держави (держава в смартфоні) в Україні визнано мобільний застосунок, веб-портал – «Дію». Значним досягненням є й те, що в Україні запроваджується інформаційно-телекомунікаційна система досудового розслідування[1]. При цьому, у ч. 1 ст. 106–1 КПК передбачено, що «інформаційно-телекомунікаційна система досудового розслідування – це система, яка забезпечує ство-

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

рення, збирання, зберігання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні».

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

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

Певним синтезом у дослідженні доктринальних підходів до криміналістики та судової експертизи, а також змінення їх парадигми є стаття «Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору» в журналі «Право України» (2022, № 2)[1].

У криміналістиці існує аксіома, яка свого часу була запропонована доктором Е. Локаром (принцип Локара) «кожний контакт – залишає слід». Можна констатувати, що будь-яке кримінальне правопорушення завжди залишає сліди (матеріально-фіксовані, ідеальні, віртуальні або електронні). Тому розслідування і судовий розгляд має відбува-

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

тися шляхом пізнання події, що відбулася, засобами криміналістики у встановленому законом порядку.

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

Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню.

Окремої уваги заслуговують так звані цифрові докази (цифрова інформація) – інформація, яка створена за допомогою високих інформаційних технологій. У наукових джерелах зарубіжних країн широкого застосування набув термін «digital evidence» (цифрові докази), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютерної чи іншої техніки[1].

Цифрові докази – це фактичні дані, що подані у цифровій формі та зафіксовані на будь-якому типі носія[2]. Поряд із терміном «цифрові докази» використовуються й інші, наприклад: «електронні докази», «електронні сліди», «цифрові джерела інформації», «електронні документи» тощо.

У ч. 2 ст. 99 КПК України вказано, що до документів, зокрема, можуть належати «матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні). У ч. 4 ст. 99 КПК України регламентовано, що «дублікат документа, а також копії інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних

---

[1] Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція. 2013. №5. С. 257.

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

системах, їх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа».

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

Фактично можна констатувати появу окремого криміналістичного напрямку – *«цифрової криміналістики»*[1] (Digital Forensic, Digital Forensic Science or Digital Criminalistics). У спеціальних джерелах для позначення даного напрямку використовуються й інші терміни – «комп'ютерна криміналістика» (Computer Forensic) або «криміналістика в комп'ютерних системах».

Цифрова криміналістика – «окрема криміналістична теорія та вид судової експертизи, що ставить своїм завданням дослідження цифрових доказів з використанням криміналістичної техніки та наявних методик в цілях досудового розслідування та судового розгляду»[2]. При цьому, деякі науковці навіть розглядають комп'ютерну криміналістику як «прикладну науку про розслідування злочинів (інцидентів), пов'язаних із комп'ютерною інформацією, при дослідженні цифрових доказів, методів пошуку, отримання і фіксації таких доказів»[3].

Розвиток цифрової криміналістики відбувається у трьох основних напрямах: 1) формування окремої наукової галузі в криміналістиці; 2) застосування спеціальних знань під час роботи з цифровими доказами; 3) проведення судових експертиз (зокрема, комп'ютерно-технічної експертизи)[4].

---

[1] Шепітько В. Ю. Інновації в криміналістиці як віддзеркалення розвитку науки. Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці: матер. міжнар. «круглого столу» (Харків, 12 грудня 2019 р.). Харків: Право, 2019. С. 148.

[2] Шепітько В. Ю., Шепітько М. В. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. С. 130.

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

[4] Шепітько В., Шепітько М. Доктрина криміналістики та судової експертизи: формування, сучасний стан і розвиток в Україні. Право України. 2021. № 8. С. 21.

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

Глобальна цифровізація створює нові виклики та можливості для поліції. Соціальні мережі, інтернет-магазини та інші платформи електронної торгівлі, приховані мережі типу darknet активно використовують злочинці для торгівлі всім, починаючи від диких тварин, заборонених речовин, людських органів, культурних цінностей і контрафактної продукції. Окремі суб'єкти використовують віртуальні валюти та альтернативні банківські платформи для відмивання своїх незаконних доходів, тоді як організована злочинність і терористичні групи вдаються до нових (зашифрованих) комунікаційних технологій і платформ для зв'язку та прихованої взаємодії[1]. Разом із цим з'явились нові інструменти для запобігання, розслідування та боротьби зі злочинністю, а також – для взаємодії правоохоронних органів між собою та громадськістю.

У найближчі десятиліття правоохоронні органи зіткнуться зі все більш оцифрованим і складним світом. За даними міжнародної корпорації Deloitte, у недалекому майбутньому від 20 до 30% діяльності поліцейських може бути автоматизована[2].

Відповідно до ст. 2 Закону України «Про оперативно-розшукову діяльність» під час проведення негласних слідчих (розшукових) дій, розвідувальних та контррозвідувальних заходів передбачається застосування оперативних та оперативно-технічних засобів[3]. Застосу-

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

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

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

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

Спеціальними технічними засобами є пристрої, обладнання, апаратура, прилади та програмне забезпечення, спеціально розроблені, виготовлені, запрограмовані або пристосовані для негласного отримання інформації[1]. Перелік спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації, а також критерії належності спеціальних технічних засобів для зняття інформації з каналів зв'язку та інших технічних засобів негласного отримання інформації наведені у додатку № 16 Постанови Кабінету міністрів України № 669 від 22 вересня 2016 р.[2]

В окремих випадках під час проведення ОРЗ та НСРД використовуються такі побутові електронні технічні засоби, як мобільні телефони, диктофони, фото- та відеокамери, GPS-трекери. Завдяки своїм невеликим розмірам, багатофункціональності, можливості негласного фіксування інформації вони правомірно використовуються уповноваженими співробітниками оперативних підрозділів[3].

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

---

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

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

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

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

Оперативним працівникам під час проведення ОРЗ часто доводиться звертатися за інформацією до криміналістичних обліків, які формуються з об'єктів (їх копій, зображень) і (або) відомостей про них та складаються з оперативно-пошукових та інформаційно-довідкових колекцій. Криміналістичні обліки можуть вестися з використанням комп'ютерної техніки та програмного забезпечення і містити фотокопії об'єктів у вигляді їх цифрових зображень[1]. Це дозволило створити криміналістичні реєстри у вигляді автоматизованих інформаційно-пошукових систем (АІПС). Прикладом такої АІПС слугує ідентифікаційна балістична система «BALSCAN» виробництва компанії Laboratory Imaging s.r.o. (Чехія), яка спеціалізується на цифровій обробці й порівняльному аналізі зображень. Ця система використовується в Україні з 2019 року. База даних системи містить зображення стріляних із зареєстрованої вогнепальної зброї куль та гільз, а також дозволяє сканувати і порівнювати сліди вогнепальної зброї навіть на деформованих кулях і їх фрагментах з метою ідентифікації конкретного екземпляра вогнепальної зброї.

Збройна агресія РФ проти України прискорила створення за допомогою системи «BALSCAN» електронної бази цифрових копій слідів вогнепальної зброї на гільзах, яка на сьогодні включає більше 600 тисяч зображень гільз зі слідами більше 200 тисяч одиниць зброї. Ці гільзи вилучені з місць вчинення правопорушень та гільз, стріляних з втраченої зброї або такої, яка зареєстрована на певних осіб[2].

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

---

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

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

і учасників міжнародних організованих злочинних груп з АІПС «Millennium», яка створена Міжнародною міжурядовою організацією кримінальної поліції «Інтерпол». Бази даних цієї системи містять персональні та біометричні дані, фотознімки, індивідуальні ознаки, зв'язки з організованими злочинними організаціями та ін. [1]. Інтерпол надає можливість правоохоронним органам 196 країн-членів здійснювати обмін службовою інформацією захищеною мережею під назвою I-24/7 та користуватися 19 поліцейськими базами даних з цифровою інформацією про злочини та злочинців (від імен і відбитків пальців до викрадених паспортів), до яких країни мають доступ у режимі реального часу[2].

В базах даних Інтерполу накопичується безліч інформації у цифровій формі, яка аналізується і структурується за допомогою системи з елементами штучного інтелекту Criminal Analysis Files. На основі такого аналізу для країн-членів (в т.ч. – для України) формуються розвідувальні звіти, акумулюється соціально-демографічна інформація про злочинців (вік, стать, вид діяльності, злочинні зв'язки), а також час і місце злочинної діяльності[3].

Інтерпол для правоохоронних органів країн-учасниць також надає доступ до Автоматизованої системи ідентифікації осіб за відбитками пальців AFIS та до системи розпізнавання облич за допомогою портативних пристроїв для збирання біометричних даних[4].

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

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

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

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

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

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

Співробітникам оперативно-розшукових органів під час виконання своїх службових обов'язків доводиться використовувати цифрові фотознімки та відеозаписи, виконані свідками або потерпілими за допомогою власних мобільних телефонів. Така цифрова інформація процесуально не оформлена і може в подальшому використовуватись як докази лише за умови встановлення її автентичності (справжності). На жаль, лише деякі мобільні телефони (Samsung, Apple) залишають у своїх записах певні «мітки» (метадані), за яким судовий експерт може встановити автентичність файлу. В усіх інших випадках для отримання записів з такими «мітками» необхідно заздалегідь на телефон встановити мобільний додаток eyeWitness to Atrocities, який дозволяє робити фотографії та знімати відео, в які в момент зйомки вшиваються метадані, необхідні для підтвердження їх справжності в суді[1].

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

---

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

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

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

Для пошуку розшукуваних осіб з 2022 р. правоохоронні органи України використовують систему розпізнавання осіб за ознаками зовнішності американської компанії Clearview AI[1], а для збирання інформації про осіб за допомогою інформації з відкритих джерел – систему BigDataPeople української компанії Artellence[2]. З моменту повномасштабного вторгнення РФ в Україну підрозділи кримінального аналізу здійснюють ідентифікацію військових злочинців, колаборантів, зрадників, диверсантів та ін. Загалом протягом минулого року підрозділами кримінального аналізу ідентифіковано майже 5.5 тис. осіб, причетних до збройної агресії[3].

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

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

[1] War in Ukraine. Clearview AI : website. URL: https://www.clearview.ai/

[2] Open Data matters now. Artellence : website. URL: https://artellence.com/

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

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

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

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

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

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

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

Незважаючи на значну кількість публікацій із проблем використання цифрових доказів у судочинстві, окремі питання потребують подальшого дослідження. Зокрема, невирішеними залишаються проблеми законодавчого закріплення поняття «цифровий доказ», процесуального регламентування їх вилучення, фіксації та зберігання з урахуванням досвіду США.

Особливої актуальності проблеми використання цифрових доказів у кримінальному судочинстві набули після відкритого повномасштабного збройного вторгнення військ РФ на територію України, що грубо порушило права громадян України, закріплені в розд. I Конвенції про захист прав людини й основоположних свобод (далі – *Конвенція*) і її протоколах, а саме: право на життя (ст. 2 Конвенції), заборона катувань (ст. 3 Конвенції), заборона рабства (ст. 4 Конвенції), заборона дискримінації (ст. 14 Конвенції), право на власність (ст. 1 Протоколу № 1), право на освіту (ст. 2 Протоколу № 1), право на свободу і особисту недоторканність (ст. 5 Конвенції), право на справедливий суд (ст. 6 Конвенції), заборона покарання без закону (ст. 7 Конвенції) та ін.[1]

Спільними зусиллями правоохоронних органів України та правозахисних організацій світу створено декілька електронних ресурсів для збирання відомостей про воєнні злочини. За даними Генеральної прокуратури України станом на грудень 2022 р. зафіксовано цифрову інформацію щодо приблизно 70 тисяч таких злочинів[2], яка згодом (разом з іншими доказами) дасть змогу не лише довести, що ці злочини було скоєно, а й пов'язати їх із конкретними особами (злочинцями), висунути їм обґрунтовані обвинувачення та притягнути до відповідальності. Однак у слідчих і суддів часто виникають труднощі у збиранні й оцінюванні цифрових доказів через відсутність у законодавстві України їх визначення, порядку фіксації й оцінки. Також суди України іноді не визнають цифрових доказів допустимими, а напрацюваннями у цьому напрямі науковців і юристів ЄС та США

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

[2] Офіс Генерального прокурора / Офіц. сайт. URL: https://gp.gov.ua/

найчастіше послуговуються журналісти-розслідувачі. Тобто законодавство України не встигає за стрімким розвитком інформаційних технологій, а прогалини правового регулювання часто доводиться заповнювати судовою практикою.

У 2012 р. прийнято спеціальний міжнародний стандарт ISO / IEC 27037:2012[1], який містить настанови щодо роботи із цифровими доказами. Дотримуючись цього стандарту, журналісти-розслідувачі інтернет-видання *Bellingcat* на основі аналізу цифрової інформації (телефонних розмов, відеозаписів, супутникових знімків та ін.) установили, що до авіакатастрофи пасажирського Boeing-777 MH17 причетні конкретні військові РФ. Національний стандарт України ДСТУ ISO / IEC 27037:2017[2] є єдиним в Україні офіційним документом, який стосується цифрових доказів. У ньому викладено настанови щодо ідентифікації, збирання, здобуття та збереження цифрових доказів, однак законодавчого закріплення ці рекомендації поки що не мають.

Офіс Верховного комісара ООН з прав людини та Центр з прав людини Каліфорнійського університету в Берклі 2020 р. представили *«практичний посібник щодо ефективного використання цифрової інформації у відкритому доступі для розслідування порушень міжнародного кримінального права з прав людини та гуманітарного права»*, який містить стандарти й методологічні підходи до *«збору, збереження та аналізу інформації у відкритому доступі, яка може бути представлена як доказ у кримінальних процесах»*[3]. У Протоколі Берклі викладено алгоритми пошуку, накопичення, аналізу та збереження цифрової інформації з відкритих джерел із дотриманням принципів об'єктивності, компетентності, підзвітності, відповідності законодавству, безпеки, точності, незалежності, прозорості, дотримання прав людини та ін. Автори Протоколу Берклі надають рекомендації щодо визначення меж вирішуваного завдання з метою

[1] ISO / IEC 27037:2012. URL: https://www.iso.org/standard/44381.html

[2] ДСТУ ISO / IEC 27037:2017. URL: http://online.budstandart.com/ua/catalog/doc-page?id_doc=74978

[3] Протокол Берклі з ведення розслідувань з використанням відкритих цифрових даних. С. 6. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

економії часу й убезпечення свідків і потерпілих, а також апаратного і програмного забезпечення.

Сучасними завданнями цифрової криміналістики є пошук і аналіз цифрових слідів, аналіз даних (зокрема – метаданих[1]), збирання доказової інформації у цифровому середовищі. Найбільш складними й масштабними є завдання із пошуку у відкритому доступі й аналізу потенційних джерел доказів – величезної кількості загальнодоступних відео- та аудіозаписів, фото- та супутникових знімків, текстів, звітів, публікацій у соціальних мережах. Електронні пристрої є сховищем загальної та особистої інформації, цифрової інформації про різного роду події та явища, дії окремих осіб тощо. Оскільки сучасні мобільні телефони мають широку добірку функцій (здійснення і приймання дзвінків, телефонна книга і диктофон, фото- і відеокамера, створення і редагування текстових файлів та повідомлень, інтернет-пошук і використання хмарних сховищ, електронна пошта й соціальні мережі, месенджери і сервіси спілкування та ін.), вони зберігають цифрові сліди користування цими функціями і є своєрідними архівами особистої інформації. Така інформація може стати складовою доказової бази лише за умови її виявлення, вилучення, дослідження та процесуального закріплення із дотриманням прав людини та з урахуванням захисту персональних даних.

Науковці в галузі кримінально-правових наук одночасно використовують терміни «електронні» та «цифрові» докази, хоча ці терміни не є тотожними. Сьогодні цифрові пристрої цілком витіснили аналогові, а різниця між аналоговою та цифровою інформацією полягає в тому, що аналогова інформація безперервна, а цифрова – дискретна. Слід погодитися з думкою Н. Зозулі про те, що термін «цифровий доказ» є більш точним і *«краще відображає кібернетичний аспект передачі, обробки та збереження інформації з огляду на процеси перетворення інформації за допомогою бінарного (двійкового) коду»*, а *«пристрої та машини, які здійснюють обробку та збереження цифрової інформації, слід називати електронними»*[2]. Якщо точніше,

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

[2] Зозуля Н. Електронні чи цифрові докази: удосконалення змін до процесуального законодавства. *Українське право*. 08.05.2018. URL: https://www.bitlex.ua/uk/blog/news/post/elektronni_chy_tsyfrovi_dokazy__udoskonalennya_zmin_do_protsesualnogo_zakonodavstva

то доказами є *«фактичні дані, отримані з належних джерел, а їх матеріальною основою слугує вже не саме джерело, а штучно створений відповідний процесуальний носій. <…> Доказ являє собою єдність фактичних даних та їх процесуальних носіїв»*[1].

Д. М. Цехан під цифровими доказами розуміє *«фактичні дані, що представлені у цифровій (дискретній) формі та зафіксовані на будь-якому типі носія та після обробки ЕОМ стають доступними для прийняття людиною»* [2]. Це визначення потребує уточнення. Зокрема, не всі носії здатні зберігати інформацію у цифровій формі (папір і магнітна плівка також є носіями інформації). Також для розшифровування й дослідження деяких видів цифрової інформації потрібні не ЕОМ, а спеціальні електронні прилади зі спеціальним програмним забезпеченням (наприклад, для перегляду записів бортових реєстраторів літальних апаратів). Тому ***цифровими доказами*** *слід вважати фактичні дані, які представлені у вигляді бінарного (двійкового) коду та містять інформацію, що має значення для об'єктивного вирішення справи.*

На відміну від Цивільного процесуального кодексу України (ст. 100)[3], Господарського процесуального кодексу України (ст. 96)[4] і Кодексу адміністративного судочинства України (ст. 99)[5], у КПК відсутні положення про електронні (цифрові) докази. Інформація в цифровій формі у КПК належить до документів / електронних документів як процесуальних джерел доказів (ч. 2 ст. 84)[6]. До документів також належать *«матеріали фотозйомки, звукозапису, відеозапи-*

---

[1] Тертишник В. М. Кримінальний процес України. Загальна частина : підручник. Академічне видання. Київ, 2014. С. 288.

[2] Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юриспруденція*. 2013. Вип. 5. С. 257. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58

[3] Цивільний процесуальний кодекс України від 18.03.2004 р. № 1618-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1618–15#Text.

[4] Господарський процесуальний кодекс України від 06.11.1991 р. № 1798-XII (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1798–12#Text

[5] Кодекс адміністративного судочинства України від 06.07.2005 р. № 2747-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2747–15#Text.

[6] Кримінальний процесуальний кодекс України від 13.04.2012 р. № 4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text.

су та інші носії інформації (у тому числі комп'ютерні дані)» (п. 1 ч. 2 ст. 99 КПК)[1] і *«носії інформації, на яких за допомогою технічних засобів зафіксовано процесуальні дії»* (п. 3 ч. 2 ст. 99 КПК)[2]. Оригіналом електронного документа зазначено *«його відображення, якому надається таке ж значення, як документу»* (ч. 3 ст. 99 КПК)[3]. Дублікати документів та копії інформації у цифровій формі, виготовлені *«слідчим, прокурором із залученням спеціаліста, визнаються судом як оригінал документа»* (ч. 4 ст. 99 КПК)[4].

Документами як цифровими доказами є не лише текстові документи, малюнки, фотознімки, аудіо- та відеозаписи, а й комп'ютерні програми та бази даних. Вони різняться не лише за формою та змістом, а й за джерелом походження. Частину документів створює людина, інші виникають внаслідок роботи електронних пристроїв і систем та не залежать від дій людини (інформація з навігаційно-моніторингових систем, електронний цифровий підпис, інформація мобільних операторів, мережева технологічна інформація тощо).

У ст. 237 КПК регламентовано огляд комп'ютерних даних, який *«проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі)»* (абз. 2 ч. 2)[5]. Утім, там бракує обов'язкового переліку інформації для фіксації цифрових доказів.

Останніми роками в судах України все частіше предметом дослідження стають цифрові докази, однак під час розгляду справ у судах різних юрисдикцій у суддів виникають певні труднощі щодо визнання інформації в цифровій формі допустимими й достовірними доказами. Часто адвокати заявляють клопотання про недопустимість цифрового доказу через те, що спочатку з телефона інформацію копіювали на комп'ютер і лише згодом – на оптичний диск, який потім

[1] Кримінальний процесуальний кодекс України від 13.04.2012 р. №4651-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/4651–17#Text.

[2] Там само.

[3] Там само.

[4] Там само.

[5] Там само.

надали до суду як процесуальний носій доказу. Захисники вважають, що така копія не відповідає оригіналу тому, що в разі зміни носіїв інформації змінюється формат файлу[1]. Це твердження є хибним, оскільки одна з основних ознак інформації в цифровій формі – це ідентичність оригіналові (цілковитий збіг за всіма ознаками, включно з форматом файлу) усіх його копій, зафіксованих на різних носіях. Незважаючи на це, ВС України в ухвалі за справою № 397/2588/13-к підтримав рішення судів першої та апеляційної інстанцій і визнав недопустимим доказом виконаний під час проведення оперативно-розшукових заходів відео- й аудіозапис факту давання хабаря судді у його робочому кабінеті. Суд ухвалив, що записи є копіями і, як наслідок, визнав недопустимими доказами протоколи про здійснення негласних слідчих (розшукових) дій (далі – *НСРД*), додатком до яких є цей цифровий доказ, протокол огляду запису, де слідчий навів текст розмов щодо давання хабаря, висновки трьох судових експертиз, оскільки вони є похідними від цього запису. Обвинуваченого виправдали[2].

У Постанові ВС України від 18.12.2019 р. у справі № 588/1199/16-к суд визнав недопустимими протокол аудіо-, відеоконтролю особи із додатками, протоколом огляду отриманих під час проведення НСРД носіїв інформації та постановою про визнання їх речовими доказами. Підставою такого рішення стало клопотання сторони захисту про невідкриття їй стороною обвинувачення в порядку ст. 290 КПК доручення на проведення НСРД, під час якої здійснено відеозапис. Цього разу службову особу, підозрювану в хабарництві, також виправдали[3].

ВС України у Постанові за справою № 426/12149/17 щодо наркотичних засобів наголосив на тому, що *«відсутність у матеріалах кримінального провадження саме оригіналів технічних носіїв інфор-*

[1] Судді ККС ВС обговорили проблемні питання допустимості електронних доказів під час судового розгляду. 28.10.2021 / ВСУ. URL: https://supreme.court.gov.ua/supreme/pres-centr/news/1202347/.

[2] Ухвала ВСУ від 29.05.2018 р. Справа № 397/2588/13-к. Провадження № 51-3650км18 / Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/74475933

[3] Постанова ВСУ від 18.12.2019 р. Справа № 588/1199/16-к. Провадження № 51-3127км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/86505861.

мації, на які фіксувалась процесуальна дія, за практикою Верховного Суду, є підставою визнавати такі докази (відеофонограми) недопустимими <...> обов'язковість наявності оригіналів відеозаписів, здійснених під час негласних слідчих (розшукових) дій, зокрема контролю за вчиненням злочину, покликана забезпечити можливість експертним шляхом встановити достовірність інформації, відображеної у відеозаписі»[1].

У справі №675/1046/18 (ч. 3 ст. 369 Кримінального кодексу України – надання неправомірної вигоди службовій особі[2]) ВС України, навпаки, відмовив стороні захисту в клопотанні про призначення експертизи відео- та звукозапису на предмет монтажу цифрового відеозапису НСРД, а дослідив запис самостійно і не знайшов підстав для призначення експертизи[3].

Розглядаючи справи про хабарництво, ВС України в окремих випадках *«не вбачає жодних перепон у можливості надання до суду дублікатів протоколів процесуальних дій, а також матеріалів фотозйомки, звукозапису, відеозапису та інших носіїв інформації (у тому числі електронних), виготовлених слідчим, прокурором із залученням спеціаліста, які визнаються судом як оригінал документа»*[4].

У справі про зловживання владою під час розгону акцій протесту поліцією ВС України визнав цифрові відеозаписи подій допустимим доказом навіть без зазначення того, хто їх здійснював і як їх залучено до кримінального провадження. Цей доказ став підґрунтям для обвинувального вироку службовій особі[5].

ВС України також визнав копії цифрових відеозаписів розбійного нападу на ломбард із камер відеоспостереження (на *DVD*-дисках) до-

---

[1] Постанова ВСУ від 17.03.2020 р. Справа №426/12149/17. Провадження №51-112км20 / ЄДРСР. URL: http://www.reyestr.court.gov.ua/Review/88401663.

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

[3] Постанова ВСУ від 18.12.2019 р. Справа №675/1046/18. Провадження №51-3942км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/86505906.

[4] Див., наприклад: Постанова ВСУ від 15.01.2020 р. Справа №161/5306/16-к. Провадження №51-3498км19 / ЄДРСР. URL: http://www.reyestr.court.gov.ua/Review/87053591.

[5] Постанова ВСУ від 20.02.2018 р. Справа №750/4139/15-к. Провадження №51-36км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72460327

пустимим доказом, хоча в Постанові не зазначено, у який спосіб слідство отримало копії цих записів. Висновок судової експертизи щодо ідентифікації особи за цим відеозаписом став підставою для обвинувального вироку[1]. В іншій справі щодо грабежу копія відеозапису з камери відеоспостереження (на *DWD-RW*-диску), добровільно видана співробітником ломбарду, суд також визнав допустимим доказом, незважаючи на заперечення сторони захисту. Суд зазначив, що матеріали провадження містять запит на видачу відеозапису, супровідний лист до *DVD*-диска та протокол його огляду, за яким диск визнано речовим доказом (на думку суда – *«у передбачений КПК спосіб»*)[2].

У справі щодо незаконного обігу наркотичних засобів цивільні особи передали слідству зроблений ними відеозапис правопорушення. Слідчий оформив протокол огляду відеозапису, продемонструвавши запис обвинуваченому, його захиснику та понятим. Таке процесуальне оформлення дало суду змогу визнати відеозапис допустимим доказом[3].

В одному з випадків відеозапис із двох камер відеоспостереження суд визнав належним доказом у справі про порушення правил безпеки дорожнього руху, хоча не було встановлено технічних характеристик пристроїв, на які здійснено відеозаписи, їх сертифікацію та порядок передання відомостей на сервер [4]. В іншому випадку копію запису камери відеоспостереження й автотехнічну експертизу, проведену на її підставі, суд визнав недопустимими доказами через те, що *«за копією встановити технологічні властивості відеограми за відсутності оригіналу та оригінального пристрою неможливо»* і висновок експерта *«ґрунтується на неправильних даних, здобутих з копії відеозапису»*[5].

---

[1] Постанова ВСУ від 27.02.2018 р. Справа № 759/8643/16-к. Провадження № 51-1031км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72642168.

[2] Постанова ВСУ від 02.10.2019 р. Справа № 159/2377/17. Провадження № 51-4466км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/84788575

[3] Постанова ВСУ від 15.03.2018 р. Справа № 760/11451/15-к. Провадження № 51-727км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/72909394

[4] Ухвала ВС від 25.03.2019 р. Справа № 754/2178/18. Провадження № 51-920ск19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/80716282

[5] Постанова ВСУ від 31.10.2019 р. Справа № 404/700/17. Провадження № 51-4451км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/85390646

У кримінальному провадженні щодо крадіжки суд визнав копію (на *DVD*-диску) відеозапису події недопустимим доказом через те, що без ухвали слідчого судді слідство отримало її від потерпілої[1]. Не визнав суд допустимим доказом і копію відеозапису крадіжки з камери відеоспостереження через те, що в матеріалах кримінального провадження відсутні запит про витребування цього відеозапису й відомості про особу, яка їх отримала[2]. Недопустимим доказом суд також визнав копію відеозапису з камери відеоспостереження щодо іншої крадіжки через те, що вони не є оригіналами[3].

Тобто за однакових умов донедавна судді ухвалювали протилежні рішення. В одних випадках вони визнавали копії цифрових записів допустимими доказами, в інших – недопустимими (особливо щодо корупційних злочинів). Утім, останнім часом судді намагаються підвищити свій рівень обізнаності щодо технічних характеристик цифрових доказів для уникнення судових помилок. Зокрема, суддя ККС ВС України Надія Стефанів наголошує на тому, що *«судді відповідають за підвищення власних професійних знань стосовно використання електронних доказів. Суддя сам має дбати про те, щоб бути в курсі всіх останніх новин щодо документів і стандартів та застосовувати їх відповідно до чинного процесуального законодавства»*[4].

Останнім часом судді всіх юрисдикцій намагаються дотримуватися у своїй роботі Керівних принципів Комітету Міністрів Ради Європи щодо електронних доказів у цивільних та адміністративних провадженнях[5]. Суди в Україні все частіше відхиляють клопотання

---

[1] Постанова ВСУ від 12.04.2018 р. Справа № 366/1400/15-к. Провадження № 51-1528км18 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/73438093

[2] Постанова ВСУ від 04.09.2019 р. Справа № 369/3713/18. Провадження № 51-3536км19 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/84120855

[3] Постанова ВСУ від 15.11.2018 р. Справа № 140/2668/15-к. Провадження № 51-624км17 / ЄДРСР. URL: http://reyestr.court.gov.ua/Review/78110946

[4] Стефанів Н. Матеріальний носій – лише спосіб збереження інформації, який має значення тільки тоді, коли Е-документ виступає речовим доказом / Інформагентство «ADVOKAT POST». 02.11.2021. URL: https://advokatpost.com/materialnyj-nosij-lyshe-sposib-zberezhennia-informatsii-iakyj-maie-znachennia-tilky-todi-koly-e-dokument-vystupaie-rechovym-dokazom-suddia-stefaniv/

[5] Керівні принципи Комітету Міністрів Ради Європи CM(2018)169-add1final щодо електронних доказів у цивільних та адміністративних провадженнях : прийнято Ком.

сторони захисту щодо невизнання допустимими й достовірними копій цифрових доказів, протоколів їх огляду та висновків судових експертиз під час розгляду справ різних категорій. Судді докладно оцінюють достовірність висновків експерта й досліджують цифрові докази безпосередньо (зокрема інформацію з мобільних телефонів)[1].

Судові рішення останніх 2–3 років відрізняються від попередніх більш докладним розглядом і поясненням технічних характеристик цифрових доказів, що надає більше шансів для визнання допустимим доказом копії інформації у цифровій формі. Зокрема, у справі №677/2040/16-к касаційну скаргу захисника щодо невизнання копій відеозаписів допустимим доказом суд залишив без задоволення та зазначив:

«Відповідно до ст. 7 Закону України «Про електронні документи та електронний документообіг» від 22 травня 2003 року №851-IV, у випадку зберігання інформації на кількох електронних носіях кожний з електронних примірників вважається оригіналом електронного документа.

Матеріальний носій – лише спосіб збереження інформації, який має значення, тільки коли електронний документ є речовим доказом. Головною особливістю електронного документа є відсутність жорсткої прив'язки до конкретного матеріального носія. Один і той же електронний документ (відеозапис) може існувати на різних носіях. Всі ідентичні за своїм змістом примірники електронного документа можуть розглядатися як оригінали та відрізнятися один від одного тільки часом та датою створення»[2].

Міністр. 30.01.2019 р. на 1335-му засід. заст. міністр. / Мін'юст України. URL: https://minjust.gov.ua/m/rekomendatsii-parlamentskoi-asamblei-ta-komitetu-ministriv-radi-evropi

[1] Див., напр.: Вирок Дзержинського райсуду м. Харкова від 21.06.2019 р. Справа №638/5928/18. Провадження №1-кп/638/585/19. URL: https://zakononline.com.ua/court-decisions/show/82552131; Вирок Вищого антикорупційного суду від 17.02.2022 р. Справа №991/4996/20. Провадження №1-кп/991/53/20. URL: http://iplex.com.ua/doc.php?regnum=103409303&red=1000033ab78a5efaf99e232b33e4b495c626d6&d=5#:~:text=%D0%B7%D0%B0%20%D1%87.,%D0%B2%D0%B8%D0%BA%D0%BE%D

[2] Постанова ККС ВСУ від 22.10.2020 р. Справа №677/2040/16-к. Провадження №51-5738км19. URL: http://iplex.com.ua/doc.php?regnum=92458395&red=1000035e35a331e82f61d9818795df8ecd0762&d=5

Таке саме рішення містить і Постанова ККС ВС від 25.01.2021 р. у справі № 236/4268/18[1] та ухвала ККС ВС від 19.08.2021 р. у справі № 756/8124/19[2], у яких суд відмовив у задоволенні скарг захисників щодо недопустимості копій цифрової інформації як доказів.

За результатами узагальнення практики суду касаційної інстанції з питань проведення й оцінювання результатів НСРД у кримінальному провадженні з'ясовано, що найчастіше причинами невизнання судом допустимими доказами цифрових аудіо- та відеозаписів, здійснених під час їх проведення, є такі: надання до суду копій цифрової інформації, а не оригіналів; проведення НСРД співробітниками оперативного підрозділу без доручення на те слідчого, прокурора та без ухвали слідчого судді; невідкриття стороні захисту в порядку ст. 290 КПК доручення на проведення НСРД; відсутність процесуального оформлення рішення слідчого або прокурора про залучення до проведення НСРД «іншої особи»; невиконання вимог ч. 4 ст. 271 КПК щодо негайного складання протоколу за результатами проведення контролю за скоєнням злочину в присутності особи, щодо якої проведено НСРД, одразу після відкритого фіксування під час завершальної стадії контролю за скоєнням злочину з фактичним її затриманням[3].

У законодавстві США питання використання цифрових доказів є менш «зарегульованим». Ще наприкінці XX ст. цифрові докази у США виокремили у групу доказів у зв'язку з особливостями їх створення, зберігання, виявлення, дослідження й оцінки їх допустимості та достовірності. 1995 р. спільними зусиллями правоохоронні органи США, Канади й деяких країн Європи створили міжнародну організацію з комп'ютерних доказів (англ. *International Organization*

---

[1] Постанова ККС ВСУ від 25.01.2021 р. Справа № 236/4268/18. Провадження № 51-3124км20. URL: http://iplex.com.ua/doc.php?regnum=94905297&red=10000347f1960a9ea9dcf00a1e2414ca33651f&d=5

[2] Ухвала ККС ВСУ від 19.08.2021 р. Справа № 756/8124/19. Провадження № 51-601ск21. URL: http://iplex.com.ua/doc.php?regnum=94874011&red=1000037c6dddd0bd0c253b026e82724e953e47&d=5

[3] Узагальнення практики суду касаційної інстанції з питань проведення та оцінювання результатів НСРД у кримінальному провадженні (*оновлено*). Тренінговий центр прокурорів України. 2021. С. 51. URL: https://ptcu.gp.gov.ua/wp-content/uploads/2021/11/uzagalnennya_praktyky_sudu_po_nsrd_z_qrkodamy_1.pdf

on Computer Evidence, IOCE)[1], а 1998 р. – Наукову робочу групу з дослідження цифрових доказів (англ. *Scientific Working Group on Digital Evidence*, далі – *SWGDE*)[2], яка об'єднала роботу правоохоронних, академічних і комерційних організацій у галузі цифрової криміналістики з метою розроблення міждисциплінарних посібників і стандартів щодо відновлення, збереження й дослідження цифрових доказів. Група *SWGDE* розробила основні стандарти та принципи роботи з цифровими доказами, що забезпечує належність і допустимість цих доказів у судочинстві. Особливу увагу приділили процесуальній фіксації всіх операцій з такими доказами, забезпеченню доступу до них усіх учасників процесу, допущенню до дослідження цифрових доказів лише кваліфікованих *IT*-спеціалістів із метою максимального збереження їх цілісності[3].

До *FRE USA*[4], які прийнято ще 1975 р. та які регулюють роботу з доказами у цивільному і кримінальному процесах у федеральних судах США, неодноразово вносили зміни й доповнення щодо цифрових доказів з урахуванням розроблених науковцями стандартів і методологічних підходів до збирання, збереження й аналізу цифрових доказів[5] та останніх судових рішень, у яких вони фігурували. Зокрема, до Правила 902[6] *FRE USA* додали п. 13 і 14 щодо процедури визначення справжності певних цифрових доказів (окрім показань свідка) та надання сторонам у справі можливості встановлювати (оскаржувати) достовірність сертифікованих записів, створених за допомогою електронних систем і даних та скопійованих з електронного пристрою або носія. У поясненнях до цих пунктів зауважено, що для оскарження справжності цифрових доказів може знадобитися

---

[1] International Organization on Computer Evidence (IOCE) / UIA. Global Civil Society Database. URL: https://uia.org/s/or/en/1100029648

[2] Scientific Working Group on Digital Evidence **(SWGDE)**. URL: https://www.swgde.org/

[3] Kessler G. C. Judges' Awareness, Understanding, and Application of Digital Evidence. *Journal of Digital Forensics, Security and Law.* 2011. Vol. 6. No. 1. Art. 4. Pp. 54–72. DOI: 10.15394/jdfsl.2011.1088.

[4] Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre

[5] Протокол Берклі … . URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

[6] Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre

технічна інформація, здобута шляхом залучення судового експерта або спеціаліста в *IT*-сфері. До того ж у Правилі 702 обумовлено, що експертами можна залучати не лише осіб, які мають знання й навички в техніці та науці і певну освіту, а й тих, хто має досвід роботи в певних галузях (лікарів, банкірів, архітекторів, фізиків та ін.). Водночас показання та висновки експертів мають бути достовірними (відповідати *Daubert standard*[1]) і допустимими згідно з принципами Правила 104(a)[2] *FRE USA*.

Суди США встановлюють автентичність (справжність, достовірність) цифрових доказів згідно з Правилом 901[3] *FRE USA*. Зокрема, суд перевіряє інформацію про те, що цифрові докази *«були отримані з конкретного комп'ютера або іншого електронного пристрою, чи було зафіксовано повну та точну їх копію і вони залишилися незмінними з моменту їх фіксації»*[4]. Достовірність значного масиву даних у цифровому вигляді часто потребує дослідження повної копії даних електронного пристрою, яку створює спеціально залучений судовий експерт або спеціаліст. Така копія зберігає логічну структуру накопичувача інформації й навіть видалені файли. Це дає змогу надалі провести додаткову або повторну експертизу[5].

Справжність окремого файлу, його частини або групи файлів перевіряють за їхнім хеш-кодом (унікальним кодом для кожного такого об'єкта). Однакові значення хеш-коду для оригіналу файлу (зокрема з точної копії диску) і файлу, який перевіряють, свідчать про їх ідентичність [6]. Для порівняння файлів за хеш-кодом залучають

---

[1] *Daubert standard* сформовано на основі трьох судових справ – Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U. S. 579 (1993). URL: https://supreme.justia.com/cases/federal/us/509/579/; General Electric Co. v. Joiner, 522 U. S. 136 (1997). URL: https://supreme.justia.com/cases/federal/us/522/136/ та Kumho Tire Co. v. Carmichael, 526 U. S. 137 (1999). URL: https://supreme.justia.com/cases/federal/us/526/137/ – і призначено для встановлення достовірності показань і висновків експерта.

[2] Federal Rules of Evidence … . URL: https://www.law.cornell.edu/rules/fre

[3] Ibid.

[4] United States v. Budziak, 697 F.3d 1105 (2012) / Caselaw Access Project. URL: https://cite.case.law/f3d/697/1105/

[5] United States v. Burdulis, 753 F.3d 255 (1st Cir. 2014). URL: https://casetext.com/case/united-states-v-burdulis

[6] United States v. R. Burke. 633 F.3d 984 (10th Cir. 2011). URL: https://casetext.com/case/united-states-v-r-burke

судового експерта або *IT*-спеціаліста, а достовірність показань або висновків експерта перевіряють за *Daubert standard* (Правилом 702).

Суд може визначити справжність цифрових доказів також за допомогою показань свідків навіть за відсутності в матеріалах справи або протоколах відповідних даних[1]. Такими свідками, зокрема, можуть бути співробітники правоохоронних органів, які вилучали електронні пристрої або фіксували (копіювали) інформацію в цифровій формі[2].

Науковці Національного інституту юстиції США наголошують на важливості докладного протоколювання процесів автентифікації (визначення справжності) і всіх інших дій із цифровими доказами (вилучення з докладним описом електронного пристрою, зазначенням його власника й осіб, які мали до нього доступ, способів і засобів вилучення інформації, копіювання на зовнішній носій, дослідження з описом задіяних методів і засобів тощо). Це дає змогу довести факт зберігання інформації в первісному вигляді[3]. Сторона обвинувачення також зобов'язана своєчасно відкрити стороні захисту цифрові докази, інакше суд поверне матеріали на дослідування.

З метою запобігання помилкам під час роботи з цифровими доказами поліцейські академії США розширили навчальну програму з цифрових доказів на підставі настанов щодо роботи з такими доказами[4]. Автори настанов наголошують на тому, що цифрові докази марні без визначення їх достовірності й докладної фіксації «ланцюжка зберігання доказів», тому вони розробили алгоритм протоколювання дій із цифровими доказами та навели перелік питань, які потрібно зазначити в протоколах[5].

---

[1] United States v. Bush. 727 F.3d 1308 (11th Cir. 2013). URL: https://casetext.com/case/united-states-v-bush-30

[2] Goodison S. E., Davis R. C., Jackson B. A. Digital Evidence and the U. S. Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence. RAND Corporation, 2015. P. 11. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

[3] Ibid. P. 13.

[4] Hagy D. W. Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors. U. S. Department of Justice. Office of Justice Programs. National Institute of Justice. Washington, Jan 2007. 81 p. URL: https://www.ojp.gov/ncjrs/virtual-library/abstracts/digital-evidence-courtroom-guide-law-enforcement-and-prosecutors

[5] Ibid. Pp. 15–17.

Окрему увагу автори настанов приділяють таким питанням: необхідності підвищення кваліфікації слідчих і прокурорів щодо технічних аспектів цифрових доказів[1]; порадам щодо перевірки справжності електронних листів[2]; процесуальному значенню роздруківок інформації з комп'ютера, поясненню понять «оригінал», «копія» і «дублікат» цифрової інформації[3]; порядку визначення справжності цифрових фотознімків та ін.[4]

До 2014 р. співробітники правоохоронних органів США під час арешту осіб вилучали в них мобільні телефони й досліджували вміщену там інформацію. Утім, ВС США постановив, що обшук і вилучення цифрової інформації з телефона без відповідного ордера протирічить Конституції США й порушує права громадян[5]. Додатково ситуацію з отриманням інформації з мобільних телефонів ускладнили відмови представників компаній *Apple* та *Google* надавати доступ до інформації про користувачів навіть за офіційними запитами правоохоронних органів. Це спонукає сторони у справі приділяти більше уваги цифровим слідам, залишеним мобільними пристроями в інтернеті. Завданням суб'єктів доказування є ретельна фіксація фіксування таких цифрових доказів, аналізування їх повноти, справжності й надійності, а також оцінка допустимості та достовірності.

Дослідники Національного інституту юстиції США шляхом опитування співробітників правозастосовних органів з'ясували, що респонденти стикаються з безліччю проблем під час роботи з цифровими доказами. Зокрема, їм не вистачає знань про технічні характеристики цифрової інформації, правила її вилучення та зберігання. Слідчі потребують комплектів науково-технічних засобів для роботи з цифровими доказами, зокрема сумок Фарадея для ізолювання електронних пристроїв. На тлі швидкого розвитку технологій цифрових пристроїв і способів вилучення з них цифрової інформації виникають значні труднощі з оцінкою цифрового доказу за критерієм достовір-

[1] Ibid. P. 23.
[2] Ibid. P. 31.
[3] Ibid. P. 33.
[4] Ibid. P. 50.
[5] Riley v. California, 573 U. S. 373 (2014). URL: https://supreme.justia.com/cases/federal/us/573/373/

ності (його відповідності *Daubert standard*)[1]. Дослідники стверджують, що прокурори (через недостатню обізнаність із технічними характеристиками цифрових доказів) намагаються вилучити більше інформації, аніж це необхідно, і перевантажують судових експертів непотрібною роботою, а деяким суддям бракує знань про методи оброблення та вилучення цифрових доказів. Поліцейські й детективи часто не знають, як фіксувати та зберігати цифрові докази, а судові експерти потребують сучасних методик їх дослідження. Ці проблеми ми пропонуємо розв'язати розробленням настанов для роботи з цифровими доказами (для кожного відомства – окремо) і підвищенням кваліфікації всіх співробітників правозастосовних органів, які у своїй роботі стикаються з цифровими доказами[2].

Отже, слідчі, судді, прокурори, оперативні співробітники й судові експерти у США під час роботи із цифровими доказами певною мірою стикаються з тими самими проблемами, які виникають у відповідних співробітників усіх рівнів кримінального правосуддя України. Водночас, на відміну від КПК, *FRE USA* містять розгалужену систему поправок, які стосуються порядку вилучення цифрових доказів, їх фіксації, зберігання, автентифікації (перевірки справжності), оцінки допустимості й достовірності тощо. Достовірність цифрових доказів, наукових показань спеціалістів і висновків експертів щодо них у США визначають за *Daubert standard*. Співробітники всіх рівнів кримінального правосуддя США в роботі з цифровими доказами керуються Протоколом Берклі й Настановами щодо використання цифрових доказів.

У КПК України відсутнє визначення терміна «цифрові докази», не наведено докладного порядку їх вилучення, огляду, фіксації та зберігання. Це може спричинити помилки в роботі із цифрової інформацією й невизнання її допустимим і достовірним доказом у суді.

Викладене вище свідчить про те, що судочинство США має більше можливостей для ефективного використання цифрових доказів, аніж судочинство України.

---

[1] Goodison S. E., Davis R. C., Jackson B. A. Op. cit. P. 16. URL: https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

[2] Ibid. P. 25.

2.4. Цифрові джерела інформації – об'єкт дослідження судового експерта

Глобальний розвиток цифрових технологій розповсюджується на всі сфери життєдіяльності людини і функціонування держави, що не оминає і судово-експертну діяльність, появу нових об'єктів дослідження, як то цифрові джерела інформації, і нових завдань. Суттєво це стосується актуальної лінгвістичної експертизи, її об'єктів дослідження – інтернет-форумів, постів, смс-повідомлень, e-mail листування тощо, які стають засобами скоєння злочинів у резонансних справах, а також у справах про захист честі, гідності, ділової репутації у зв'язку з наклепами та образами, щодо майнових спорів, конфліктів, пов'язаних з рекламою, передвиборчими технологіями тощо. Під час порушення кримінальних проваджень щодо корупційних злочинів, погроз, закликів, спрямованих на розпалювання національної ворожнечі, насильницьку зміну чи повалення конституційного ладу, релігійних питань тощо, слідчі мають потребу у перевірці версій у ході розслідування справ та звертаються до експертних установ з метою встановлення необхідної інформації шляхом дослідження вилучених об'єктів.

Останнім часом науковцями звертається увага на те, що під час розгляду справ виникають певні труднощі щодо допустимості та достовірності як доказу інформації в цифровій формі через неналежне вилучення, фіксування, зберігання, що недостатньо закріплено в чинному законодавстві[1]. З приводу цього слід зазначити, що, керуючись експертною практикою, можна відмітити позитивні кроки при призначенні судових експертиз, об'єктами дослідження яких є цифрові джерела інформації. У співпраці слідчих і суддів з експертами визначилися певні напрями у дослідженні, як то комплексний підхід. Наприклад, якщо необхідно встановити, чи є у тексті виступу певної особи, який було записано на відео, заклики до порушення територі-

[1] Авдєєва Г., Живуцька-Козловська Е. Проблеми використання цифрових доказів у кримінальному судочинстві України і США. *Теорія та практика судової експертизи і криміналістики*. Вип. 1 (30). С. 126–143.

альної цілісності України, слідчий призначає комплексну експертизу, в якій експертами певних галузей знань вирішуються завдання в межах їх компетенції, і надає носії інформації, які містять запис виступу. На дослідження можуть бути надані диск, флеш-носій інформації, системний блок, телефон тощо, які стають об'єктом дослідження експерта а галузі комп'ютерних досліджень та відео-звукозапису, який виявлену інформацію на зазначених носіях надає експерту іншої галузі знань для вирішення поставленого завдання слідчим (суддею).

Під компетентністю розуміється чітке коло завдань, які може вирішувати експерт певної спеціальності з урахуванням його спеціальних знань. Науковцями зазначається, що правильніше розмежовувати «об'єктивно-науковий» та «суб'єктивний» рівні компетенції експерта. Під науковим рівнем компетенції експерта розуміють об'єм спеціальних знань, що є достатнім для вирішення певного кола завдань, і який складає зміст певного роду, виду (підвиду) судової експертизи. А суб'єктивний рівень компетентності вказує на ступінь володіння експертом теорією й методикою експертизи певного роду або виду, що залежить від його досвіду, обсягу знань про традиційні методики, розуміння нових методик і методів, орієнтування на методичну або предметно-об'єктно-методичну підготовку.

Для вирішення лінгвістичних завдань важливі обидва зазначених рівня компетенції експерта, що мають значення для дотримання таких принципів судово-експертної діяльності, як законність та достовірність.

Через необхідність задовольнити нагальні потреби суду, слідства, фізичних та юридичних осіб у справах, які внаслідок суспільно-політичних змін у країні почали оновлюватися і зростати, виникає необхідність у подальшому розвитку всіх видів експертиз, в яких об'єктами дослідження є цифрові носії доказової інформації, з урахуванням сучасних потреб дійсності. Саме таке визначення об'єктів дослідження І. О. Крицькою, на наш погляд, є більш влучним, оскільки містить «характерні властивості… які обґрунтовують їх особливий процесуальний статус»[1].

[1] Крицька І. О. Речові докази та цифрова інформація : поняття та співвідношення. *Часопис Київського університету права*. № 1. 2016. С. 304.

Запитання для самоконтролю

1. Що таке цифрова інформація і цифрові докази?
2. Що таке цифрова криміналістика і в яких напрямках відбувається її розвиток?
3. Яким чином використовується цифрова інформація під час проведення оперативно-розшукових заходів та негласних слідчих (розшукових) дій?
4. Які існують проблеми у використанні цифрової інформації (цифрових доказів) у кримінальному провадженні?
5. Чи існують особливості у проведенні огляду комп'ютерних даних?
6. Які особливості використання цифрової інформації у практиці судових органів США?
7. Чи можуть бути об'єктом судової експертизи джерела цифрової інформації?

Розділ 3

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ У ПРАВОЗАСТОСОВНІЙ ПРАКТИЦІ

3.1. Криміналістичне забезпечення розслідування кримінальних правопорушень в умовах цифрових технологій

Сьогодні застосування цифрової інформації та сучасних інформаційних технологій – це не просто новітній технологічний тренд чи модне захоплення – це фактично нова цифрова реальність, яка заснована на соціальних інноваціях та передових технологіях цифровізації[1]. Очевидно, що в сучасних умовах процеси цифровізації виступають, як важливий *стратегічний напрямок* перспективного розвитку передових держав Європи, світу, у тому числі й України, яка обрала європейський вектор розвитку.

Надання Україні статусу кандидата в члени ЄС створило додатковий імпульс для гармонізування підходів та активізації перетворень у цифровій сфері. У цьому плані важливою подією стало те, що Україна долучилася до Програми «Цифрова Європа» до 2027 р., метою цієї програми є активізація відновлення економіки та цифрової трансформації України[2]. Тому формування єдиного цифрового ринку

[1] Заславська Л. В. Цифрова ера: нові можливості та нові виклики для людини і суспільства. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : матеріали Всеукр. на- ук.-практ. конф., м. Київ, 2 грудня 2021 р. Київ-Одеса : Фенікс, 2021. С.101–104.

[2] Україна долучилася до Програми «Цифрова Європа»: що це означає | Кабінет Міністрів України. https://www.kmu.gov.ua/news/ukraina-doluchylasia-do-prohramy-tsyfrova-ievropa-shcho-tse-oznachaie

з ЄС та наближення цифрового сектора України до європейського стало пріоритетним напрямом державної політики цифрових перетворень в умовах війни[1]. За таких умов цифровізація стала не лише сучасним трендом розвитку суспільства, але й стає визначним фактором економічного, соціального, політичного та міжнародного зростання держави.

Сучасні процеси активізації цифровізації усіх сфер діяльності держави в свою чергу обумовлюють необхідність удосконалення системи органів правопорядку і прокуратури, судових органів. Відбувається перехід існуючої традиційної системи до нової реальності – цифрової, у якій цифрова інформація є невід'ємниим атрибутом, як в роботі органів кримінальної юстиції, з одного боку, й сучасної злочинної діяльності, з іншого[2]. Це у свою чергу визначає сучасні тенденції та перспективи розвитку юридичної науки, у тому числі й криміналістики, яка знаходиться на передньому краю боротьби із злочинністю.

Очевидно, що цифрова реальність сьогодення нині тісно пов'язана із появою нових форм злочинності – кіберзлочинів, інформаційного шахрайства, великою кількістю кібератак на підприємства та установи, в тому числі, й державні бази даних[3]. Безумовно, що такі загрози потребують розроблення новітніх підходів протидії злочинності, модернізації та оновлення системи органів кримінальної юстиції до сучасних умов та глобальних загроз XXI століття[4]. Це зумовлює

---

[1] Шевчук В. М. Європейський вектор розвитку сучасної криміналістики. *Адаптація правової системи України до права Європейського союзу: теоретичні та практичні аспекти* : матеріали VI Всеукр. наук.-практ. конф. (м. Полтава, 29.09.2022 року). Полтава: Полтавський юридичний інститут, 2022. С. 325–327.

[2] Shevchuk V. M., Konovalova V. O., Sokolenko M. O. Digital criminalistics: formation and role in the fight against crime in wartime conditions in Ukraine. *Використання цифрової інформації в розслідуванні кримінальних правопорушень* : матеріали міжнар. наук.-практ. круглого столу, м. Харків, 12 груд. 2022 р. / електрон. наук. вид., редкол.: В. Ю. Шепітько (голова), В. М. Шевчук, Г. К. Авдєєва, М. О. Соколенко ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. Харків : Право, 2022. С. 97–102.

[3] Тимошенко, Ю., Кисленко, Д. Правоохоронна система в епоху діджиталізації. *Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*, (1 (59), 2022. С. 41.

[4] Orlovskyi R., Us O., Shevchuk V. Committing a Criminal Offence by an Organized Criminal Group. *Pakistan Journal of Criminology.* Vol.14. №2. April-June 2022. Pp. 33–46.

активізацію застосування та поширення цифрових технологій у слідчій, судовій та експертній діяльності.

Крім цього, серед нових викликів і загроз безпрецедентним та шокуючим стала воєнна агресія РФ і повномасштабне вторгнення російських окупаційних військ на територію України 24 лютого 2022 року. Збройна агресія РФ та запровадження воєнного стану в Україні суттєво вплинуло на усі сфери нашого життя.

За таких умов виклики та загрози сьогодення обумовлюють необхідність формування та запровадження інноваційних підходів у криміналістичному забезпеченні протидії військовим кримінальним правопорушенням та воєнним злочинам. Такі виклики сьогодні визначають сучасні тенденції розвитку юридичної науки, у тому числі й криміналістики, яка знаходиться на передньому краю боротьби із злочинністю. Тому особливої актуальності та значимості набувають проблеми дослідження криміналістичного забезпечення розслідування військовим кримінальним правопорушенням, воєнним злочинам в умовах війни та сучасних реаліях значного поширення цифрових технологій у слідчій, судовій та експертній діяльності.

В таких реаліях сьогодення однією із найважливіших тенденцій сучасної криміналістики є інтеграція знань, створення та пропонування інноваційних розробок науки, спрямованих на вирішення завдань протидії злочинності в умовах війни щодо ефективного формування доказів, які в додальшому можуть бути використанні як в національних, так і міжнародних судах. Інноваційним напрямом у розвитку криміналістики є розроблення та впровадження в практику криміналістичного забезпечення протидії сучасній злочинності, у тому числі й військовим кримінальним правопорушенням та воєнним злочинам. Це потребує активізації розроблення та впровадження прогресивних технологій, які ґрунтуються на застосуванні сучасних криміналістичних знань, дотримуючись стандартів доказування у кримінальному провадженні та широкого застосування цифрових технологій і штучного інтелекту[1].

[1] Шевчук В. М. Цифрова криміналістика: воєнні виклики сьогодення та нові завдання у сучасних умовах. *Правові виклики сучасності* : матеріали всеукраїнського круглого столу (м. Харків, 20 грудня 2022 р.). Харків: Державний біотехнологічний університет, 2022. С. 35–39.

Сьогодні в умовах воєнного стану та сучасних євроінтеграційних процесів криміналістика потребує активізації наукових досліджень практичної спрямованності, що пов'язане передусім із появою нових викликів перед системою кримінальної юстиції та необхідністю вирішення першочергових завдань в умовах війни, формування криміналістичних знань відповідно до сучасних потреб практики. У таких умовах криміналістика покликана розроблювати інноваційні криміналістичні продукти, засоби, прийоми та методи, спрямовані на протидію злочинності, пов'язаною із військовою агресією РФ проти України й вирішення інших важливих завдань.

Крім цього, перед системою органів досудового розслідування, кримінальної юстиції постають нові виклики, пов'язані із необхідністю швидкого, всебічного та якісного документування, збирання доказів масових кримінальних порушень міжнародного гуманітарного права, що вчиняються військовими РФ. Фактично можна констатувати: саме сьогодні формується новий науковий криміналістичний напрям – воєнна криміналістика [1].

Варто зауважити, що в історії криміналістики були спроби сформувати ідею «воєнно-польової криміналістики» (наприклад, Г. М. Григорян)[2], «військово-прикладна криміналістики», «військова криміналістики»[3] та ін. , На нашу думку, запропоновані терміни дещо звужують розуміння предмета, системи й завдань воєнної криміналістики. Так, наприклад, сам термін «польова криміналістика» є дискусійним, оскільки під ним доволі умовно розуміють техніко-криміналістичні засоби й методи роботи з доказами, які використовуються або можуть бути використані не в кабінеті слідчого або в лабораторії експерта, а безпосередньо на місці події під час його огляду, чи під час

[1] Shevchuk V. The role of criminalistics in improving the efficiency of the investigation of war crimes committed by the military of the RF in Ukraine. *Scientific Collection «InterConf»*. 2022. Vol. 122. Pp. 187–195. URL: https://archive.interconf.center/index.php/conference-proceeding/article/view/1208 (дата звернення: 20.02.2023).

[2] Григорян Г. М. Международно-правовые и организационные основы расследования военных преступлений, совершаемых противоборствующими сторонами вооруженного конфликта : автореф. дис. … д-ра юрид. наук. Ереван, 2021. 41 с.

[3] Шевчук В. М. Воєнна криміналістика : проблеми формування та роль у сучасних умовах. *Реалізації прав людини у діяльності правоохоронних органів в умовах окупації українських територій* : V Всеукр. наук.-практ. конф. (м. Кривий Ріг, 30 вересня 2022 р.). Кривий Ріг : ДонДУВС, 2022. С. 136–140 .

провадження на цьому місці інших слідчих дій або дослідницьких експертних операцій. Як бачимо, ці питання далеко не вичерпують проблематики воєнної криміналістики. Значний інтерес як у науковому, так і в практичному плані становлять аналізування й вирішення інших проблем, що потребують дослідження у цій специфічній галузі знань.

На наш погляд, *зміст* наукової концепції воєнної криміналістики мають скласти ідеї та теоретичні положення про об'єкт дослідження, система знань, зміст її окремих елементів, місце в системі наукового знання, значення для теорії та практики слідчої роботи, завдання подальшого наукового дослідження. *Об'єктом* вивчення воєнної криміналістики виступають закономірності збирання, дослідження та використання доказової інформації, формування криміналістичного забезпечення розслідування воєнних злочинів та військових кримінальних правопорушень, що вчиняються в умовах війни, в районах воєнних дій, проведення бойових операцій та воєнної агресії.

Вбачається, що об'єкт воєнної криміналістики певною мірою зумовлює її *систему*, що містить науково обґрунтовані й апробовані на практиці криміналістичні положення та рекомендації щодо організації виявлення, документування і розслідування воєнних злочинів та кримінальних правопорушень, вчинених у районах активних бойових дій або збройного конфлікту. Також положеннями цієї системи зумовлено розроблення і використання теоретико-методологічних основ, вибору та застосування засобів, методів та прийомів криміналістичної техніки, тактики і методики розслідування з урахуванням специфічних умов діяльності – *в умовах воєнного стану, війни* та активних бойових дій на певній території держави.

Головними *завданнями* воєнної криміналістики є розроблення, формування й застосування системи засобів, методів, прийомів і заходів криміналістичного забезпечення протидії скоєнню воєнних злочинів та військових кримінальних правопорушень. Оскільки воєнна криміналістика має комплексний характер, то має охоплювати теоретико-методологічний, техніко-, тактико- і методико-криміналістичний напрями досліджень[1].

[1] Shevchuk V. Current Issues of Criminalistics in Context of War and Global Threats. *Theory and Practice of Forensic Science and Criminalistics*. Issue 3 (28). 2022. P. 11–27. DOI: 10.32353/ khrife.3.2022.02.

Теоретико-методологічні основи воєнної криміналістики містять загально-наукову проблематику, пов'язану із розробленням поняття, предмета, системи й завдань воєнної криміналістики, її місця в системі криміналістичної науки. Важливими напрямами наукових досліджень може стати розроблення таких наукознавчих проблем, як методологія воєнної криміналістики, системи курсу воєнної криміналістики, інновації у криміналістичній дидактиці під час викладання воєнної криміналістики та ін. У цьому разі можна говорити про воєнну криміналістику як новий науковий напрям у криміналістичній доктрині, який має значні перспективи та потребує подальших наукових досліджень.

У напрямі *техніко-криміналістичного забезпечення* воєнної криміналістики слід актуалізувати наукові розробки й дослідження щодо створення та впровадження інноваційних криміналістичних продуктів, спрямованих на оптимізацію боротьби зі злочинністю у військовій сфері, документування та розслідування виявлених злочинів, пов'язаних із військовою агресією РФ проти України. Серед таких інноваційних продуктів можна назвати новітні (новостворені або пристосовані до завдань і потреб протидії воєнній злочинності й іншим кримінальним виявленням в умовах війни) техніко-криміналістичні засоби, сучасні інформаційні технології, електронні бази знань, методи фіксування, аналізування, оцінювання та збирання доказової інформації. Крім цього, для потреб воєнної криміналістики можна застосувати сучасні ідентифікаційні біометричні системи за ознаками людини (за відбитками пальців рук, ознаками зовнішності, малюнком райдужної оболонки ока, ДНК, ознаками ходи або почерку та ін.). Актуальним є використання можливостей безпілотних літальних апаратів, систем спостереження й відеоконтролю, електронного контролю за пересуванням осіб у просторі та повітрі, ідентифікаційні системи розпізнавання осіб за обличчями тощо. Також необхідно активізувати роботу із застосування штучного інтелекту для забезпечення розглядуваних видів діяльності й розв'язання практичних завдань як у правозастосовній сфері, так і в боротьбі зі злочинністю в умовах війни.

У *тактико-криміналістичному забезпеченні* воєнної криміналістики перспективними напрямами досліджень має стати розроблення

тактичних основ проведення процесуальних дій і криміналістичних рекомендацій щодо їх проведення в умовах війни. Вони можуть бути пов'язані зі специфікою тактики проведення окремих слідчих (розшукових) і негласних слідчих (розшукових) дій в умовах воєнного стану або бойових дій. Така ситуація зумовлює потребу в розробленні нових тактичних прийомів, перегляд можливостей тактичних комбінацій і тактичних операцій, алгоритмів слідчих (розшукових) дій та ін. Важливо розробити окремі тактики проведення дій, у яких учасниками (підозрюваними, свідками, потерпілими та ін.) є особи з тимчасово окупованих територій або з районів активних бойових дій, а також військовополонені.

Методико-криміналістичне забезпечення воєнної криміналістики тісно пов'язане зі зміною кримінального та кримінального процесуального законодавства, оскільки такі зміни вимагають удосконалення наявних методик розслідування кримінальних правопорушень і розроблення нових криміналістичних методик[1]. Інноваційні розробки у цій галузі криміналістики мають бути спрямовані на створення методик розслідування нових видів кримінальних правопорушень, тактичних операцій, алгоритмів слідчих (розшукових) дій, перевірки типових слідчих версій, розроблення криміналістичної характеристики кримінальних правопорушень та ін.[2] Реалії війни в Україні потребують нагального вдосконалення, розроблення та впровадження у практику системи криміналістичних методик розслідування окремих видів злочинів, скоєних військовослужбовцями у районах збройного конфлікту (зокрема, розслідування самовільного залишення військової частини (місця служби) і дезертирства; ухилення від військової служби шляхом членоушкодження; злочинів, скоєних військовослужбовцями щодо цивільного населення; розкрадань військовослужбовцями зброї та боєприпасів; перевищення командирами військових частин посадових повноважень та ін.).

---

[1] Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів: монографія. Вінниця, 2017. 492 с.

[2] Konovalova V. O., Shevchuk V. M. Prospective directions of research of innovations of separate criminalistic methodics. *Scientific practice: modern and classical research methods:* Collection of scientific papers «ΛΌГОΣ». Boston; Vinnitsa, 2021. Vol. 1. Pp. 81–85. DOI: 10.36074/logos-26.02. 2021.v1. (дата звернення: 20.02.2023)

Досить актуальним сьогодні є створення системи військової юстиції, зокрема, це питання формування військової поліції, військової прокуратури та військових судів (спеціалізованих колегій) із врахуванням передового зарубіжного досвіду, європейських та міжнародних стандартів щодо протидії злочинності. Створення органів військової юстиції в реаліях воєнного сьогодення є необхідним кроком задля забезпечення якісного та ефективного виявлення, фіксації розслідування воєнних злочинів, що вчиняються російськими військовими на території України. Вирішення цього питання потребує відповідного законодавчого регулювання та розроблення *концепції криміналістичного забезпечення діяльності органів військової юстиції,* що визначає новий науковий напрямок досліджень у криміналістиці.

У сучасних реаліях воєнного стану в Україні важливим є забезпечення дотримання міжнародних принципів і стандартів у протидії корупції, враховуючи досвід європейських і світових практик, беручи до уваги традиції, звичаї і менталітет українських громадян, адже характер корупції в нашій державі відрізняється від корупційних проявів в інших країнах. Україна відіграє ключову роль в процесі міжвідомчої координації міжнародного співробітництва у сфері протидії та запобігання корупції. Крім цього, на наш погляд, за таких умов постає проблема забезпечення діяльності системи цих органів необхідними ресурсами, засобами й навчання, у тому числі й криміналістичного та кримінально-процесуального спрямування.

В реаліях сьогодення сучасна криміналістика покликана розроблювати та запроваджувати в практику інноваційні засоби, прийоми та методи, спрямовані на протидію воєнних злочинів, що вчиняються військовими РФ на території України та криміналістичного забезпечення розслідування кримінальних правопорушень в умовах воєнного стану. Окремим напрямом у криміналістиці має бути розроблення системи криміналістичних методик розслідування, активізація розробок техніко-криміналістичного забезпечення, застосування спеціальних знань, захист інформаційних джерел і проблеми інформаційної безпеки. Відтак, проблема криміналістичного забезпечення та практика застосування криміналістичних знань для збирання доказової інформації під час війни є досить актуальною та значимою.

Таким чином, в реаліях сьогодення особливої значимості та актуальності набуває проблематика формування та реалізації криміналістичного забезпечення розслідування воєнних злочинів та військових кримінальних правопорушень із врахуванням сучасних викликів та загроз. Вбачається, що побудова ефективного криміналістичного забезпечення розслідування та судового розгляду має охоплювати теоретико-методологічний, техніко-криміналістичний, методико-криміналістичний напрями, включаючи супроводження і забезпечення засобами криміналістики й судовий розгляд таких воєнних злочинів.

3.2. Системи штучного інтелекту у правозастосовній діяльності

Термін «штучний інтелект» (ШІ) уперше запропонований американським ученим-математиком Джоном Макарті у середині 50-х р.р. минулого століття як новий напрям інформатики і був визначений як «наука і техніка створення інтелектуальних машин»[1]. На сьогодні єдиного загальновизнаного визначення цього терміна не існує, оскільки це міждисциплінарна наука, яка поєднує багато її галузей (інформатика, математика, соціологія, психологія, право та ін.).

Європейською етичною хартією про використання штучного інтелекту в судових системах та їх оточення (2018 р.) ШІ визначається як сукупність наукових методів, теорій та технік, мета яких – відтворити машиною когнітивні здібності людини[2].

У Державному стандарті України ДСТУ 2938–94 («Системи оброблення інформації») штучний інтелект визначається як «здатність систем оброблення даних виконувати функції, що асоціюються з ін-

[1] John McCarthy (2007). «What is Artificial Intelligence». Society for the Study of Artificial Intelligence and Simulation of Behavior, Computer Science Department, Stanford University. URL : http://jmc.stanford.edu/articles/whatisai/ whatisai.pdf

[2] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (Council of Europe, 3–4 December 2018). URL : https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artifi cial-intelligence-ai-in-judicial-systems-and-their-environment

телектом людини – логічне мислення, навчання та самовдосконалення»[1]. Учені в галузі комп'ютерних наук під штучним інтелектом (ШІ) також розуміють «властивість автоматичних систем брати на себе окремі функції інтелекту людини, наприклад, вибирати й ухвалювати оптимальні рішення на основі раніше одержаного досвіду й раціонального аналізу зовнішніх дій»[2].

Проблемам визначення напрямів використання ШІ у правозастосовній діяльності і їх правового регулювання присвячені публікації багатьох закордонних дослідників, а саме: Джованні Сартора та Карла Брантинга (1998)[3], Крістофера Рігано (2019)[4], Асми Іддер та Стефана Куло (2021)[5], Алі Фагірі Кабола (2022)[6] та ін. Останнім часом до проблем дослідження ШІ зверталися й українські дослідники.

О. Баранов визначає ШІ як «деяку сукупність методів, способів і засобів, зокрема, апаратних, та комп'ютерних програм, які реалізують одну, кілька або всі когнітивні функції (КФ) достатньою мірою еквівалентні когнітивним функціям людини»[7]. Є. Мічурин при всьому наголошує на тому, що ШІ є результатом творчої діяльності людини і являє собою пристрій або комп'ютерну програму щодо здо-

---

[1] ДСТУ 2938–94. Системи оброблення інформації. Основні поняття. Терміни та визначення (ISO 2382–1:1993, NEQ). URL : http://online.budstandart. com/ua/catalog/doc-page.html?id_doc=77434

[2] Методи та системи штучного інтелекту: Навчальний посібник для студентів напряму підготовки «Комп'ютерні науки» / Уклад. : А. С. Савченко, О. О. Синельніков. Київ : НАУ, 2017. С. 9.

[3] Sartor, G., Branting, L. K. (1998). Introduction: Judicial Applications of Artificial Intelligence. In: Sartor, G., Branting, K. (eds) Judicial Applications of Artificial Intelligence. Springer, Dordrecht. DOI : https://doi.org/10.1007/978-94-015-9010-5_1

[4] Christopher Rigano. Using Artificial Intelligence to Address Cri minal Justice Needs. NIJ Journal 280, January 2019. URL : https://www.nij.gov/journals/ 280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.Aspx

[5] Asma Idder, Stephane Coulaux. Artificial intelligence in criminal justice: invasion or revolution? 13 December 2021. International Bar Association : website. URL : https://www.ibanet.org/dec-21-ai-criminal-justice

[6] Ali Faghiri Kabol. The Use Of Artificial Intelligence In The Criminal Justice System (A Comparative Study). Article in Webology November 2022. URL : https://www.researchgate.net/publication/365027297_The_Use_Of_Artificial_Intelligence_ In_ The_Criminal_Justice_System_A_Comparative_Study

[7] Баранов О. А. Інтернет речей : регулювання надання послуг роботами зі штучним інтелектом. *Інформація і право*. №4(27)/2018. С. 47. URL : http://ippi.org.ua/sites/default/files/7_10.pdf

буття, обробки та застосування інформації і формування «умінь», що подібні до дій, які свідомо виконує людина[1]. Тобто, у загальному розумінні системами штучного інтелекту (ШІ) є комп'ютерні системи, що не лише виконують певні завдання за заздалегідь заданим алгоритмом, а й вирішують творчі завдання на основі аналізу значної за обсягом різноманітної інформації та імітують такі процеси мислення людини, як навчання, прогнозування, оцінка ризиків, робота з неповними даними та ін.[2]

Учені визначили такі види систем штучного інтелекту: системи, які «думають» як люди (зокрема, штучні нейронні мережі); системи, які діють як люди (наприклад, роботи); та системи, які постійно навчаються і генерують нові знання (наприклад, експертні системи)[3].

У сучасному світі системи ШІ активно використовуються в системах комунікації, промисловості, сільському господарстві, медицині, транспорті, освіті, науці, побуті та ін. Військове застосування штучного інтелекту та машинного навчання охоплює спостереження, розвідку, аналіз інформації та пропонування певних оптимальних рішень щодо нанесення бойових ударів, надання гуманітарної допомоги, ліквідації наслідків надзвичайних ситуації, прийняття управлінських або логістичних рішень військовим командуванням тощо[4]. Системи протиповітряної оборони, які Україна отримала від закордонних країн, найбільш складні функції виконують за допомогою ШІ[5].

---

[1] Мічурін Є. Правова природа штучного інтелекту. *Forum Prava*. 2020. № 64 (5). С. 68

[2] Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 6.

[3] Pablo Lázaro. Artificial Intelligence in Criminal Investigation. Agenda for International Development : website. URL : https://www.a-id.org/artificial-intellige nce-in-criminal-investigation

[4] Авдєєва Г. К. Євроінтеграціні напрями формування законодавства України у галузі використання систем штучного інтелекту у правозастосовній діяльності. *Сучасний розвиток державотворення та правотворення в Україні: проблеми теорії та практики*: матеріали XI Міжнародної науково-практичної конференції (26 червня 2023 року, м. Київ): Зб. тез наук. праць / за заг. редакцією М. В. Трофименко. Київ: МДУ, 2023. С. 8.

[5] Київ захищають системи ППО зі штучним інтелектом – МВС. Слово і діло : аналітичний портал. URL : https://www.slovoidilo.ua/2022/06/17/novyna/ bezpeka/ kyyiv-zaxyshhayut-systemy-ppo-shtuchnym-intelektom-mvs

Навіть для розшуку депортованих у РФ дітей з окупованих територій України використовують системи ШІ[1].

У правозастосовній діяльності такі системи також показали свою ефективність. Зокрема, системи безпеки дорожнього руху з елементами ШІ допомагають збирати доказову інформацію при розслідуванні дорожньо-транспортних подій. Вони виявляють порушення правил дорожнього руху, допомагають ідентифікувати транспортні засоби та осіб в несприятливих умовах (низька роздільна здатність фото- або відеокамери, темрява, снігопад, дощ тощо). Спеціальні системи ШІ, які здатні прогнозувати зростання злочинності в окремих регіонах, дозволяють підвищити ефективність заходів її попередження. Зокрема, в Апараті РНБО України використовується сучасна багатофункціональна інформаційно-аналітична система з елементами ШІ «СОТА», яка слугує інструментом аналізу та управління ризиками у сфері національної безпеки й оборони України[2].

Незважаючи на активне використання систем ШІ у правозастосовній діяльності, визначення поняття «штучний інтелект» в законодавстві України відсутнє, не охарактеризовані види ШІ, принципи їх використання, межі, умови, порядок застосування тощо. Ці питання є вкрай актуальними і мають досліджуватись науковцями.

Системи ШІ показали свою ефективність у роботі правозастосовних органів багатьох країн. Крістофер Рігано стверджує, що, завдяки їх використанню, покращилися результати роботи правоохоронних органів, зменшився рівень злочинності, скоротилися строки розслідування злочинів[3].

Система ШІ ePOOLICE (early Pursuit against Organized crime using environmental scanning, the Law and IntelligenCE systems) з 2013 р.

---

[1] Депортованих із Криму до РФ дітей-сиріт шукають за допомогою штучного інтелекту – прокурор АРК. URL : https://ua.krymr.com/a/news-prokuror-ark-dity-syroty-krym/32327860.html

[2] В Апараті РНБО України розроблено та введено в експлуатацію сучасну інформаційно-аналітичну систему «СОТА». РНБО: офіц. сайт. URL : https://www.rnbo.gov.ua/ua/Diialnist/5011.html

[3] Christopher Rigano. Using Artificial Intelligence to Address Cri minal Justice Needs. NIJ Journal 280, January 2019. URL : https://www.nij.gov/journals/ 280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.Aspx

успішно використовується в країнах-членах ЄС[1]. Вона вивчає сторінки сайтів, електронне листування, поліцейську інформацію для пошуку інформації про діяльність організованих злочинних груп та здійснює оцінку ризику появи кримінальної активності[2].

У Великій Британії система штучного інтелекту HART (Harm Assessment Risk Tool) показала ефективність при прогнозуванні низького ризику на 89,8%, однак ефективність при високому ризику рецидиву злочину щодо раніше засуджених осіб становила 78,8%[3].

У Сполучених Штатах Америки для оцінки ймовірності скоєння підсудним рецидиву злочинів та аналізу попередніх проступків використовуються такі системи ШІ: Watson/Ross – IBM (аналітика), Lex Machina – LexisNexis (аналітика), COMPAS – Correctional Offender Management Profiling for Alternative[4].

О. Плахотнік справедливо вважає, що системи ШІ COMPAS та HART «здатні оцінювати ризики рецидиву злочинів і з успішністю можуть бути використані під час підготовки досудової доповіді у кримінальному провадженні, а також у наглядовій та пенітенціарній пробації в Україні»[5].

---

[1] Early Pursuit against Organized crime using envirOnmental scanning, the Law and IntelligenCE systems. European Commission : website. URL : https://cordis. europa.eu/project/id/312651

[2] Авдєєва Г. К., Коновалова В. О., Соколенко М. О. Перспективи використання систем штучного інтелекту у правозастосовній діяльності. *Перспективні напрями розвитку кримінальної юстиції в цифрову еру* : матеріали Всеукр. заоч. наук.-практ. конф. (м. Харків, 24 лип. 2023 р.) : електрон. наук. вид. / редкол.: В. С. Батиргареєва (голова), Н. В. Глинська, Д. П. Євтєєва ; [уклад.: Н. В. Глинська, Д. І. Клепка]. ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Від. дослідж. проблем кримін. процесу та судоустрою. Харків : Право, 2023. С. 7.

[3] AI can predict reoffending, university study finds. Durham Constabulary. 24 January 2022. URL : https://www.durham.police.uk/News/News-Articles/2022/January/AI-can-predict-reoffending-university-study-finds.aspx

[4] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (Council of Europe, 3–4 December 2018). URL : https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artifi cial-intelligence-ai-in-judicial-systems-and-their-environment

[5] Плахотнік О. В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. № 4/2019. С. 54. DOI : https://doi.org/10.17721/2413–5372.2019.4/45–57

Міністерство Юстиції України до Єдиного реєстру засуджених осіб підключило аналітичну систему з елементами ШІ «Касандра», яка аналізує різноманітну інформацію про засуджених осіб та виявляє ризики повторного кримінального правопорушення[1].

Системи ШІ в усьому світі використовуються під час розслідування злочинів для отримання інформації про осіб та їхні дії, різноманітні об'єкти і явища, з метою виявлення і попередження шахрайських дій, для ідентифікації осіб і предметів (у т.ч., зброї) за їх слідами та ін.[2] В. Шевчук зазначає, що під час аналізу соціальних мереж «штучний інтелект може допомогти виявити зв'язки між підозрюваними, які можуть бути пов'язані з воєнними злочинами, та ідентифікувати осіб, які можуть бути свідками воєнних злочинів або мати інформацію про них»[3].

При розслідуванні воєнних злочинів, скоєних військовими РФ в Україні, системи ШІ ефективно вирішують завдання щодо ідентифікації осіб за фотознімками, відеозаписами та пробами ДНК. Зокрема, за допомогою американської системи розпізнавання осіб Clearview AI, яка використовує базу даних з 30 млрд фотопортретів із соціальних мереж та стрічок новин[4], встановлено особи окремих

---

[1] Оценивать опасность преступников будет «Кассандра» : Денис Малюська сообщил, что КМУ внес проект в Раду. Судебно-юридическая газета. 13 апреля 2021. URL : https://sud.ua/ru/news/publication/198879-otsenivat-opasnost-prestupnikov-budet-kassandra-denis-malyuska-soobschil-chto-kmu-vnes-proekt-v-radu

[2] Christopher Rigano. Using Artificial Intelligence to Address Cri minal Justice Needs. NIJ Journal 280, January 2019. URL : https://www.nij.gov/journals/ 280/Pages/using-artificialintelligence-to-address-criminal-justice-needs.Aspx

[3] Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки*: практики ефективного реагування : матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Харків : Право, 2019. С. 143.

[4] Авдєєва Г. К., Коновалова В. О. Штучний інтелект у боротьбі зі злочинністю: напрями використання та проблеми законодавчого врегулювання. *Цифрова трансформація кримінального провадження в умовах воєнного стану* : матеріали круглого столу, присвяч. Всеукр. тижню права (м. Харків, 23 груд. 2022 р.) : електрон. наук. вид. / [редкол.: Н. В. Глинська (голов. ред.), Д. І. Клепка, А. А. Барабаш] ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України, Від. дослідж. Проблем крим. проц. та судоустрою. Харків : Право, 2022. С. 37. DOI: https://doi.org/10.31359/9789669984395

злочинців-військових РФ за їхніми фотознімками. Ця система дозволила ідентифіковати понад 1 000 осіб (живих і загиблих) та встановити особи окремих громадян РФ, які скоїли злочини на території нашої держави та/або розповсюджують дезінформацію від імені громадян України. Система показала свою ефективність навіть при аналізі зображень понівечених тіл[1].

Спецслужбами РФ для проведення інформаційно-психологічних атак використовуються фейкові (підроблені) новини, які супроводжуються фальшивими фотознімками та відеозаписами, у т.ч. створеними за допомогою нейронних мереж, алгоритм роботи яких імітує роботу мозку людини (ШІ). Останнім часом найбільш відомими недостовірними світлинами, згенерованими системами штучного інтелекту, є зображення хлопчика, який вижив під час ракетного удару в Дніпрі, та фейкове звернення В. Зеленського про капітуляцію, яке з'явилося в інформаційному просторі в березні 2022 р.[2]

ШІ здатен автоматично аналізувати велику кількість даних з різних джерел з метою виявлення неправдивої інформації та встановлення її джерел, розпізнавання змінених або підроблених зображень шляхом порівняння їх з оригінальними, встановлення схем і способів поширення дезінформації та її блокування.

Центр стратегічних комунікацій та інформаційної безпеки України використовує автоматизовану систему SemanticForce, яка дозволяє аналізувати певні неприйнятні або шкідливі інформаційні потоки і зображення та реакцію на них користувачів, відрізняти хибні акаунти від реальних користувачів тощо[3]. Аналітичні алгоритми вітчизняного сервісу Attack Index дозволяють виявляти певні інформаційні

---

[1] Джеймс Клейтон. Як штучний інтелект допомагає ідентифікувати загиблих в Україні. BBC News Україна. URL : https://www.bbc.com/ukrainian/ features-61105661

[2] Авдєєва Г. К. Системи штучного інтелекту як засоби протидії інформаційній війні в Україні. *Національна безпека України в умовах інформатизації та глобалізації суспільних процесів: сучасні загрози та кримінально-правове регулювання* : матеріали VII Міжнар. наук.-практ. конф. (м. Харків, 11 трав. 2023 р.) / редкол.: Л. М . Демидова (голов. ред.), Н. В . Шульженко, Д. О. Куковинець, О. С. Попович ; Нац. юрид. ун-т ім. Ярослава Мудрого ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса Нац. акад. прав. наук України ; Громад. орг. «Всеукр. асоц. кримін. права». Харків : Право, 2023. С. 281. DOI: https://doi.org/10.31359/9789669985552

[3] SemanticForce media and e-commerce intelligence. URL : https://semant icforce.ai/en

операції та їх ознаки (час, інтенсивність, масштабність, ініціатор операції, мережа розповсюдження інформації) та пропонує сценарії протидії інформаційним загрозам[1].

Попри ефективну роботу з великими масивами інформації, системи ШІ мають певні недоліки і викликають занепокоєння в усьому світі. Зокрема, через недосконаліть біометричних систем, велику кількість помилок у їх роботі та можливі порушення прав людини парламент ЄС нещодавно запропонував заборонити збирання фотозображень осіб до приватних систем розпізнавання (у т.ч., Clearview)[2].

У США з 2013 по 2016 рр. в поліції проходила тестування система Watson компанії IBM, яка автоматично складала стандартні звіти і процесуальні документи після усного повідомлення інформації електронному помічникові. Через низьку якість отриманих документів та, як наслідок, суттєве зниження якості роботи поліцейські надали негативну оцінку системі Watson та припинили її використання[3].

За результатами дослідження, проведеного аналітичним центром NewsGuard у січні 2023 р., встановлено, що дуже популярна та загальнодоступна в усьому світі система штучного інтелекту ChatGPT (Generative Pre-trained Transformer), розроблена компанією OpenAI для роботи в діалоговому режимі, здатна генерувати неправдиві тексти з елементами інформації про реальні події[4]. Система за певним запитом може згенерувати дезінформаційне повідомлення, у т. ч. засноване на «кремлівській» пропаганді. При тому навіть суддя окружного суду м. Картахена (Колумбія) під час судового розгляду справи використовував систему ШІ GPT для постановки юридичних питань щодо справи та включив отримані

---

[1] Attack Index : website. URL : https://attackindex.com/uk/golovna

[2] Європарламент закликав заборонити системи розпізнавання осіб. Європейська правда : веб-сайт. 06.10.2021. URL : https://www.eurointegration. com.ua/news/2021/10/6/7128684

[3] Авдєєва Г. К. Проблеми використання систем штучного інтелекту в роботі органів кримінальної юстиції. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 8.

[4] Misinformation Monitor: January 2023. NewsGuard. URL : https://www.newsguardtech.com/misinformation-monitor/jan-2023

від ШІ відповіді у своє рішення. Про це він зазначив у своєму Рішенні від 30 січня 2023 р.[1]

Члени міжнародної асоціації юристів попереджають про можливі помилкові результати роботи систем ШІ через похибки людини під час формування баз даних і формулювання варіантів підсумкових рішень, які аналізує ШІ, а також через погрішності в програмному коді ШІ, який також створюється людиною[2].

Очільник Tesla та SpaceX Ілон Маск, один із засновників Apple Стів Возняк й більше тисячі експертів у галузі IT-технологій підписали відкритий лист із закликом припинити розробку просунутого штучного інтелекту та тимчасово призупинити навчання більш потужних систем, ніж GPT-4 від компанії OpenAI. Автори листа вважають, що навіть творці «потужних цифрових розумів» не можуть їх контролювати, а сучасні системи штучного інтелекту починають конкурувати з людиною та здатні зруйнувати ринок праці, вплинувши на 300 млн робочих місць[3].

З метою запобігання дискримінації і порушення основних прав і свобод під час використання систем ШІ у правоохоронних органах до парламенту ЄС поданий проєкт «Закону про штучний інтелект», у якому запропоновано при використанні таких систем застосовувати високі рівні підзвітності, справедливості та прозорості[4]. У документі наголошено на тому, що системи ШІ мають бути юридично, етично та технічно надійними, повинні відповідати демократичним цінностям, правам людини та верховенству закону. Науковці попереджають,

---

[1] Колумбійський суддя використав штучний інтелект ChatGPT для вирішення справи. Юридична Газета. URL : https://yur-gazeta.com/golovna/kolumbiyskiy-suddya-vikoristav-shtuchniy-intelekt-chatgpt-dlya-virishennya-spravi.html

[2] Asma Idder, Stephane Coulaux. Artificial intelligence in criminal justice: invasion or revolution? 13 December 2021. International Bar Association : website. URL : https://www.ibanet.org/dec-21-ai-criminal-justice

[3] Маск, Возняк та понад тисячу експертів закликали припинити розробку штучного інтелекту. [Електронний ресурс] 30 березня, 2023 р. URL : https://espreso.tv/mask-voznyak-ta-ponad-tisyachu-ekspertiv-zaklikali-pripiniti-rozrobku-shtuchnogo-intelektu

[4] Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. An official website of the European Union. Brussels, 21.4.2021. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX%3A52021PC0206

що «існує ризик використання штучного інтелекту для переслідування політичних опонентів або некоректного відображення даних через певні алгоритмічні недосконалості. Крім того, важливо враховувати законодавчі обмеження щодо застосування штучного інтелекту в розслідуванні злочинів, зокрема заборони на використання деяких видів даних, які можуть порушувати права людини»[1].

Завдання розвитку технологій ШІ в Україні є одним з пріоритетних напрямів у сфері науково-технологічних досліджень. У «Концепції розвитку штучного інтелекту в Україні» (далі – Концепція) основою державної політики у сфері правового регулювання галузі штучного інтелекту проголошено захист прав та свобод учасників відносин у галузі штучного інтелекту, розроблення та використання технологій штучного інтелекту з дотриманням етичних стандартів[2]. На жаль, у «Плані заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки» не містяться конкретні заходи щодо законодавчого регулювання процесів використання ШІ у правозастосовній діяльності, а заплановано лише «запровадження правового регулювання з питань формування державної політики в галузі штучного інтелекту» та «впровадження технологій штучного інтелекту в національну систему кібербезпеки»[3].

Стрімкий розвиток і широке розповсюдження систем ШІ випереджають процеси створення умов і засобів ефективної протидії недоброчесному і зловмисному їх використанню. Для вирішення цього питання на засіданні групи семи розвинутих країн (G7), яке відбулося в Японії 29 квітня 2023 р, міністри цифрових технологій узгодили п'ять таких принципів розвитку ШІ: верховенство права, дотримання

---

[1] Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. Цифрова трансформація кримінального провадження в умовах воєнного стану : мат-ли Всеукр. круглого столу (Харків, 16.12.2022). Харків, 2022. С. 139.

[2] Концепція розвитку штучного інтелекту в Україні. Схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL : https://zakon.rada.gov.ua/laws/show/1556–2020-%D1%80#Text

[3] План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2021–2024 роки. Затверджено розпорядженням Кабінету Міністрів України від 12 травня 2021 р. № 438-р. URL : https://zakon.rada.gov.ua/laws/show/ 438–2021-%D1%80#n10

законної процедури, демократія, повага до прав людини і використання можливостей для інновацій[1]. На майбутніх засіданнях групи G7 планується розглянути питання щодо управління системами ШІ, захисту авторського права та боротьби з дезінформацією.

У вересні 2022 р. Європейська комісія підписала Угоду про приєднання України до програми «Цифрова Європа» та надала можливість нашій країні скористатися фінансуванням і підтримкою програми щодо розширення можливостей використання систем ШІ в різних галузях (у т.ч., у правозастосовній діяльності). Така можливість може бути реалізована лише за умови імплементації норм, закріплених у «Рекомендаціях щодо штучного інтелекту», що прийняті в червні 2019 року Організацією економічного співробітництва та розвитку[2], та за умови дотримання етичних стандартів, передбачених у Рекомендаціях CM/Rec (2020)1 Комітету Міністрів державам-членам щодо впливу алгоритмічних систем на права людини, схвалених 8 квітня 2020 р.[3] , у законодавство України. Оскільки 23 червня 2022 р. Україна набула статусу країни-кандидата на вступ до Європейського Союзу, законодавство нашої країни, у т.ч. у частині використання систем ШІ в інформаційній війні з РФ, має бути поступово адаптовано до законодавства ЄС. Тобто, Україна під час розроблення власного законодавства щодо регулювання процесів використання систем ШІ у правозастосовній діяльності може використати численні нормативно-правові акти і рекомендації, прийняті різними інституціями ЄС та Ради Європи. Одним із найважливіших таких документів є схвалена ще у 2018 р. Європейською комісією з питань ефективності правосуддя «Етична хартія про використання штучного інтелекту

[1] G7 should adopt 'risk-based' AI regulation, ministers say. Reuters. April 30, 2023. URL : https://www.reuters.com/markets/europe/g7-should-adopt-risk-based-ai-regulation-ministers-say-2023-04-30/

[2] Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments. (OECD/LEGAL/0449). Adopted on: 22/05/2019. URL : https://legal instruments.oecd.org/en/instruments/oecd-legal-0449

[3] Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impacts of algorithmic systems (Adopted by the Committee of Ministers on 8 April 2020 at the 1373rd meeting of the Ministers' Deputies). URL : https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016809e1154

в судових системах та їх середовищі»[1], яка закріплює принципи використання систем ШІ під час здійснення правосуддя, а саме: дотримання основних прав людини при використанні ШІ; запобігання будь-якої дискримінації між окремими особами чи групами осіб; якість та безпека при обробленні судових рішень і даних, що мають міститися в безпечному технологічному середовищі; прозорість, неупередженість та справедливість.

Національною асоціацією адвокатів України (НААУ) створено Робочу групу з питань правового регулювання ШІ та напрацювання рекомендацій до національного законодавства в цій сфері. Організатори робочої групи впевнені, що це дозволить забезпечити прозорість та належне правове регулювання штучного інтелекту, захист від можливих кібератак та інших загроз, а також запобігти їх недоречному використанню. Ключовим завданням Робочої групи є забезпечення належного захисту прав людини під час розробки, впровадження та використання систем ШІ[2]. Однак, окрім окреслених робочою групою питань, є безліч інших, які слугують предметом активних дискусій науковців у галузі права. Зокрема, О. Радутний вважає ШІ електронною особою (особистістю), пропонує визнати його суб'єктом правовідносин і застосовувати до нього заходи кримінально-правового характеру[3]. Т. Каткова також пропонує внести зміни в кримінальне законодавство з метою «визначення кримінальної відповідальності ШІ»[4]. В. Грига вважає можливим навіть визнавати ШІ потерпілим від злочину[5]. З такими пропозиціями погодитися

---

[1] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (Council of Europe, 3–4 December 2018). URL : https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artifi cial-intelligence-ai-in-judicial-systems-and-their-environment

[2] Голова НААУ, РАУ створила Робочу групу з правового регулювання штучного інтелекту та рекомендацій до законодавства | НААУ. НААУ. 08.03.23. URL : https://unba.org.ua/news/7940-golova-naau-rau-stvorila-robochu-grupu-z-pra vovogo-regulyuvannya-shtuchnogo-intelektu-ta-rekomendacij-do-zakonodavstva. html

[3] Радутний О. Є. Кримінальна відповідальність штучного інтелекту. Інформація і право. №2(21)/2017. С. 131. URL : http://ippi.org.ua/sites/default/ files/14_5.pdf

[4] Каткова Т. Штучний інтелект в Україні: правові аспекти. Право і суспільство. 2020. № 6. С. 53. URL : http://pravoisuspilstvo.org.ua/archive/2020/ 6_2020/10.pdf

[5] Грига В. Штучний інтелект як потерпілий від злочину. Молодий вчений. 2019. №5 (69). С. 191. URL : https://doi.org/10.32839/2304–5809/2019-5-69-41

не можна, особливо в разі настання цивільно-правової відповідальності. Досвідчений фахівець аналітичного центру з міжнародного розвитку в галузі кібербезпеки Пабло Лазаро справедливо зазначає, що «робот не може нести відповідальність за дії або бездіяльність, які можуть завдати шкоди третім особам. Судді судять людей, а не роботів, не кажучи вже про алгоритми»[1]. Тобто, для отримання якісного нормативно-правового акту, який регулюватиме порядок використання ШІ у правозастосовній діяльності, до його розроблення мають долучатися науковці в галузі права, судді, слідчі, адвокати та інші співробітники правозастосовної сфери.

В Україні доцільно прийняти єдиний нормативно-правовий акт у формі закону, який розв'язав би всі можливі проблеми використання ШІ у правозастосовній діяльності. Під час розроблення цього документу слід враховувати, що процедура доказування у процесуальній діяльності є тривалим процесом, який являє собою всебічний аналіз і зіставлення лише об'єктивної доказової інформації. Вона відрізняється від автоматичного аналізу даних системою ШІ, що здатна враховувати недостовірні або підроблені дані, неправдиві показання свідка або потерпілого, помилкові висновки експерта та ін. Це може вплинути на правильність висновку штучного інтелекту і призвести до порушення таких фундаментальних принципів судочинства, як верховенство права, недискримінація, неупередженість, справедливість та ін. Тому повністю автоматизувати процеси прийняття процесуальних рішень в Україні поки що зарано.

3.3. Можливості та перспективи використання технологій штучного інтелекту в розслідуванні кримінальних правопорушень

На сьогоднішній день застосування та впровадження технологій штучного інтелекту у правоохоронну діяльність багато в чому обу-

[1] Pablo Lázaro. Artificial Intelligence in Criminal Investigation. Agenda for International Development : website. URL : https://www.a-id.org/artificial-intelligence-in-criminal-investigation.

мовлено необхідністю протистояти злочинному світу, який дедалі бере на озброєння найсучасніші інноваційні технології. Злочинці достатньо активно використовують останні досягнення четвертої промислової революції: технології блокчейну, дрони, робототехніку, штучний інтелект. Технології штучного інтелекту сьогодні є провідною галуззю у сфері цифрових технологій та цифрових телекомунікацій. Тому використання можливостей штучного інтелекту у роботі органів правопорядку та юстиції є насьогодні достатньо актуальними та затребуваними практикою.

Системи на основі технологій штучного інтелекту знаходять активне застосування і в криміналістиці, будучи логічним продовженням процесу програмування та алгоритмізації у розслідуванні кримінальних правопорушень, у тому числі й розслідуванні воєнних злочинів в Україні. Водночас, нині існує низка дискусійних питань щодо застосування технологій штучного інтелекту у криміналістиці, від самого розуміння ролі штучного інтелекту, поняття, співвідношення із інтелектом людини, зокрема слідчого, із криміналістичним мисленням і до важливих інших проблем. Більше того, останнім часом ставиться питання про створення штучного інтелекту, який має відтворювати особливості криміналістичного мислення, який базується на таких технологіях, що потребують наукових розробок та впровадження на практиці.

Сучасний стан злочинності в Україні та її динаміка під час війни значно вплинули на зміну пріоритетів завдань криміналістики та особливості формування і застосування криміналістичних знань. Інформатизація соціального середовища призвела до «технологізації» криміналістики, розроблення і впровадження інформаційних, цифрових, телекомунікаційних та інших технологій[1]. За таких обставин у воєнних реаліях сьогодення нині гостро постає питання про підвищення ефективності розслідування воєнних злочинів за допомогою технологій штучного інтелекту та активізації використання спеціальних знань, як важливих напрямків удосконалення криміналістичної методики розслідування цих злочинів.

[1] Шепітько В. Ю. Формування доктрини криміналістики та судової експертизи в Україні – шлях до єдиного європейського криміналістичного простору. *Право України.* 2022. №2. С. 76–90. С. 83.

Практика показує, що за допомогою технологій штучного інтелекту можна ідентифікувати російських військових за соціальними мережами й записами камер відеоспостереження[1]. Достатньо активно застосовуються технології розпізнавання обличчя *Clearview AI* для боротьби з дезінформацією, розпізнавання й ідентифікації загиблих і воєнних злочинців[2]. Використання технологій штучного інтелекту допомагає руйнувати міфи про нібито невмируших солдатів так званої «спецоперації», розпізнаючи обличчя трупів російських військових окупантів, відшукуючи їх у соціальних мережах і за допомогою автодозвонів повідомляючи родичів про їхню смерть. В реаліях російської військової агресії інструменти штучного інтелекту істотно сприяють виявленню, розкриттю та розслідуванню воєнних злочинів, злочинів проти людяності та геноциду[3].

В сьогоднішніх реаліях штучний інтелект використовується щоденно у повсякденній діяльності людини, наприклад, для перекладу текстів, створення субтитрів для відео або блокування електронних листів (спаму). При цьому штучний інтелект розглядається як сукупність методів, способів, технологій і засобів (зокрема, апаратних), комп'ютерних програм, які реалізують одну, кілька або всі когнітивні функції, еквівалентні когнітивним функціям людини[4]; це сконструйований людиною пристрій або комп'ютерна програма зі здобування, оброблення й застосування інформації та формування вмінь, подібних до дій, свідомо виконуваних людиною[5].

---

[1] Латиш К. Цифрова криміналістика у період війни в Україні: можливості використання спеціальних знань у сфері інформаційних технологій. *Kriminalistikairteismo ekspertologija* : *mokslas, studijos, praktika.* 2022. Т. 18. С. 32.

[2] Федоров М. Технології з розпізнавання облич та штучний інтелект дозволяють знайти кожного / SUNDRIES. 09.04.2022. URL: https://sundries.com.ua/tekhnolohii-z-rozpiznavannia-oblych-ta-shtuchnyi-intelekt-dozvoliaiut-znaity (дата звернення: 12.10.2022).

[3] Мамедов Г. Цифрова криміналістика. Як це допомогло зібрати докази злочинів у Бучі? / New Voice. 08.06.2022. URL: https://nv.ua/ukr/opinion/viyna-v-ukrajini-yak-cifrova-kriminalistika-vikrivaye-zlochini-rf-v-ukrajini-novini-ukrajini-50248411.html (дата звернення: 12.10.2022).

[4] Баранов О. Ідентифікація робота зі штучним інтелектом як суб'єкта права. *Інтернет речей: проблеми правового регулювання та впровадження* : мат-ли друг. наук.-практ. конф. (Київ, 29.11.2018). Київ, 2018. С. 9. URL: http://ippi.org.ua/sites/default/files/zbirnik_tez_19.12.2018-maket_3-converted.pdf (дата звернення: 19.10.2022).

[5] Мічурін Є. О. Правова природа штучного інтелекту. *Форум Права.* 2020. №64 (5). С. 67–75. DOI: 10.5281/zenodo.4300624 (дата звернення: 19.10.2022).

Системи штучного інтелекту можуть бути заснованими виключно на програмному забезпеченні та працювати у віртуальному світі (наприклад, голосові синтезатори, програмне забезпечення для аналізу відеозаписів, пошукові системи, системи розпізнавання мовлення й обличчя) або можуть бути інтегрованими в апаратне забезпечення (наприклад, робототехніка, безпілотні транспортні засоби, дрони чи об'єкти мережі «Інтернету речей» (англ. *Internet of Things, IoT*)) тощо.

Попри всі позитивні можливості й потенціал штучного інтелекту, останнім часом такими технологіями дедалі частіше послуговуються злочинці, винаходячи нові способи злочинної діяльності і з використанням новітніх технологій штучного інтелекту. До того ж криміногенні чинники застосування штучного інтелекту спричиняють нові загрози та виклики охоронюваним законом інтересам як окремих громадян, так і держави й суспільства загалом, потребуючи адекватних засобів протидії таким кримінально-правовим[1] і криміналістичним засобам[2]. Тому штучний інтелект як останнє наукове досягнення потребує нових криміналістичних ідей і методів, пов'язаних із його використанням у боротьбі зі злочинністю[3].

Визначаючи межі, напрями та сфери застосування штучного інтелекту у криміналістиці, необхідно виходити із визначення предмету та об'єктів криміналістики. Відомо, що криміналістика – це наука про закономірності злочинної діяльності та її відображення в джерелах інформації, які слугують основою для розробки засобів, прийомів і методів збирання, дослідження, оцінки і використання доказів з метою розкриття, розслідування, судового розгляду та запобігання кримінальним правопорушенням[4]. Злочинна поведінка від-

---

[1] Radutniy O. E. Novel Criminal Delicts Related to Digital Human Being. *Вісник Асоціації кримінального права України.* 2020. Т. 1. № 13. С. 16–28. URL: http://vakp.nlu.edu.ua/issue/view/12594 (дата звернення: 17.10.2022).

[2] Konovalova V. O., Shevchuk V. M. Modern criminalistics in the conditions of war: problems of adaptation and reload. *Modern research in world science* : Proceedings of the 5th International scientific and practical conference (August 7–9, 2022). Lviv, 2022. Pp. 896–903.

[3] Jackson C. Artificial Intelligence Changing the World of Forensics Science. EasyChair Preprint. 2021. No. 5815. 3 p. URL: https://easychair.org/publications/preprint/1Fmk (дата звернення: 17.10.2022).

[4] Textbook of criminalistics. Vol. 1: General theory. / Hendryk Malevski, Valery Shepitko. Kharkiv: Apostille Publishing House, 2016. 488 p. P. 46–53.

бивається в різних слідах, які можуть стати у встановленому законом порядку джерелом доказів[1]. Тому важливим елементом предмета криміналістики є процеси збирання, дослідження, оцінки та використання доказів[2].

У таких процесах особливого значення набуває механізм та сліди злочинної діяльності із застосуванням штучного інтелекту, а також їх наслідки[3]. Мова йде про цифрові сліди та особливості збирання, дослідження, оцінки та використання цифрових доказів у кримінальному провадженні. Більше того, враховуючи двуєдиний об'єкт криміналістики – з одного боку злочинна діяльність, з іншого – діяльність спеціальних суб'єктів стосовно виявлення, розкриття, розслідування та профілактики кримінальних правопорушень необхідно розуміти, що у даному випадку мова йде про застосування штучного інтелекту, як у злочинній діяльності, так і у діяльності органів правопорядку та суду під час виявлення, розкриття, розслідування та профілактики кримінальних правопорушень, при вчиненні яких нині досить активно застосовуються інноваційні засоби та технології, у тому числі й технології штучного інтелекту.

З огляду на викладене, можна виокремити такі *основні напрямки застосування штучного інтелекту*, зокрема: використання штучного інтелекту злочинцями під час вчинення ними протиправної діяльності (кібершахрайство, кібертероризм, технології дипфейку та ін.); застосування штучного інтелекту у діяльності органів правопорядку та суду; у правоохоронній діяльності та у судочинстві; у судово-експертному забезпеченні; у науково-дослідницькій діяльності у сфері протидії сучасній злочинності[4] та ін.

---

[1] Zhuravel, V. A., & Kovalenko A. V. Examination of evidence in criminal proceedings as a component of the proof process. *Journal of the National Academy of Legal Sciences of Ukraine,* 2022, 29(2), 313–328.

[2] Журавель В. А. Загальна теорія криміналістики: ґенеза та сучасний стан: монографія. Харків: Право, 2021. 448 с. С. 63–91.

[3] Zhuravel, V. A. Crime mechanism as a category of criminalistics. *Yearbook of Ukrainian law: Coll. of scientific papers / responsible for the issue O. V. Petryshyn.* Kharkiv: Pravo, 2021. №13. С. 390–404.

[4] Карчевський, М. В. Протидія злочинності в україні у форматі DATA SCIENCE. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*, 2022, 2(98), 202–227.

У криміналістичній техніці технології штучного інтелекту можуть застосовуватися та надавати допомогу : при розроблені для вирішення завдань і потреб протидії злочинності новітніх техніко-криміналістичних засобів; при створенні та застосуванні сучасних інформаційних технологій; електронних баз знань; методів фіксації, аналізу, оцінки та збору доказової інформації; сучасних ідентифікаційних біометричних систем за ознаками людини та ін.[1] Інноваційними напрямками застосування штучного інтелекту в галузі криміналістичної техніки також виступають : використання безпілотних літальних апаратів; систем спостереження та відеоконтролю; електронний контроль за пересуванням осіб у просторі та повітрі; ідентифікаційні системи розпізнавання за обличчями осіб; криміналістичний ДНК-аналіз тощо.

Вбачається, що певний науковий та практичний інтерес викликають пропозиція застосування таких технологій у сучасній практиці. Так, наприклад, запропоновано систему генерації фотороботів Forensic Sketch AI-rtist на базі штучного інтелекту DALL-E 2 для створення фотороботів злочинців[2]. В іншому випадку запропоновано використання інноваційного поліграфа (детектора брехні) XXI століття – EyeDetect, який базується на застосувані технологій ШІ і немає датчиків або кабелів, підключених безпосередньо до досліджуваного[3]. Водночас, як показує практика, їх застосування має багато недоліків, які негативно впливають на прийняття рішень слідчим, детективом, судею, що потребує виваженого відношення до такого роду пропонованих новацій, які не завжди відповідають вимогам та принципам застосування криміналістичних інновацій на практиці.

Значною проблемою від використання технологій штучного інтелекту сьогодні є порушення прав людини у сфері захисту конфіденційності особистих даних в Інтернеті та проблеми втручання в при-

[1] Shepitko V. Yu., Konovalova V. O., Shevchuk V. M. et. al. Scientific and technical support of investigative activities in the context of an adversarial criminal procedure. *Issues of Crime Prevention*. Vol. 1. №. 42. 2021. Pp. 92–102.

[2] Штучний інтелект навчили ловити злочинців – NoWorries. https://noworries.news/shtuchnyj-intelekt-navchyly-lovyty-zlochynczivv/#

[3] Сучасна технологія виявлення обману – поліграф EyeDetect – науковий online журнал «Судово-психологічна експертиза» https://expertize-journal.org.ua/inshi-napryami-spetsobladnannya

ватне життя. Тому важливо не перебільшувати можливості та переваги штучного інтелекту, враховуючи і певні недоліки. Вбачається, що застосування штучного інтелекту у судочинстві та правоохоронній діяльності є можливим із обов'язковим врахуванням принципів верховенства права, дотримання основних прав людини, поваги до честі і гідності, рівності перед законом і судом, пропорційності, змагальності сторін, прозорості, неупередженості та справедливості тощо. Водночас, неможливо на сьогодні повністю замінити суддю при здійсненні судочинства на штучний інтелект, однак, ніщо не забороняє оптимізувати роботу судді та суду шляхом залучення таких технологій. Головна роль штучного інтелекту має бути визначена не як заміна судді при здійсненні судочинства, а як своєрідна допомога для здійснення правосуддя суддею.

Необхідно створити глобальне (обов'язкове) міжнародне законодавство щодо розробки та впровадження штучного інтелекту, зокрема для запобігання його нелегальному, тобто нецивілізаційному використанню. Крім того, уряди та компанії повинні знати про недосконаліть даних, на яких базується технологія штучного інтелекту, і подбати про запобігання дискримінації та порушенням прав людини. Перспективи подальших досліджень мають бути спрямованні на розроблення питань, що стосуються розвитку та використання штучного інтелекту як складової інформаційних технологій у правоохоронній діяльності та правосудді з врахуванням міжнародного досвіду та сучасної практики[1].

У сучасних умовах війни органи кримінальної юстиції достатньо активно використовують технології штучного інтелекту у різних сферах професійної діяльності, які суттєво підвищують ефективність цієї роботи, зокрема, серед основних слід виокремити: 1) розпізнавання обличчя та ідентифікація російських військових-окупантів у соціальних мережах та камерах відеозапису; 2) забезпечення безпеки на дорогах, виявлення та фіксація порушень правил дорожнього руху; 3) використання безпілотників для протидії незаконному

[1] Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану* : мат-ли Всеукр. круглого столу (Харків, 16.12.2022). Х., 2022. С. 135–140.

оббігу вогнепальної зброї, наркозлочинності, проведення військових операцій та збирання доказової інформації умовах війни і ведення активних бойових дій з метою фіксації воєнних злочинів; 4) попередження кримінальних правопорушень з використанням інтелектуальних систем безпеки з різними пристроями (датчиками) збору інформації; 5) прогнозування кримінальних правопорушень методом картографування злочинності, за допомогою якого формуються прогнози щодо місцевої злочинності та індивідуальної злочинної поведінки.

Сучасні можливості розслідування воєнних злочинів дозволяють визначити джерел цифрової інформації, які визначають напрями збирання та дослідження цифрових слідів, досить багато, але вони потребують спеціальних досліджень, особливо щодо можливостей та перспектив застосування технологій штучного інтелекту під час розслідування воєнних злочинів в Україні.

Застосування штучного інтелекту в розслідуванні воєнних злочинів в Україні може бути корисним в багатьох аспектах. Основними напрямками, в яких він може бути використаний, є такі: 1) *аналіз супутникових знімків.* Штучний інтелект може допомогти аналізувати великі обсяги супутникових знімків для виявлення змін у ландшафті, зокрема будівель, доріг, об'єктів інфраструктури, які можуть бути пов'язані з воєнними злочинами, а також допомогти в ідентифікації місць, де можуть бути поховані тіла жертв воєнних злочинів; 2) *аналіз відео- та фотоматеріалів*. Штучний інтелект може бути використано для аналізу великого обсягу відео- та фотоматеріалів, які були зняті на місцях вчинення воєнних злочинів, що, у свою чергу, може допомогти в ідентифікації підозрюваних та свідків, а також встановити, чи були зображені на них об'єкти, які можуть містити криміналістично-значущу інформацію для розслідування таких злочинів; 3) *обробка аудіоматеріалів.* За записами телефонних розмов та під час обробки аудіоматеріалів щодо розслідування воєнних злочинів штучний інтелект може допомогти в ідентифікації голосів, які містяться на таких носіях, а також визначити місця, де були здійснені ці розмови; 4) *аналіз соціальних мереж*. Аналізуючи соціальні мережі, штучний інтелект може допомогти виявити зв'язки між підозрюваними, які можуть бути пов'язані з воєнними злочинами, та ідентифікувати осіб, які можуть бути свідками воєнних злочинів

або мати інформацію про них[1]; 5) *аналіз даних з медичних закладів*. Штучний інтелект може допомогти в ідентифікації тіл жертв воєнних злочинів, встановленні причини смерті, ідентифікації військовополонених, військових злочинців та їх пошук за даними про хворобу та відомостями про їх ідентифікаційні ознаки, які допомагають встановленню конкретної особи; 6) *розпізнавання облич.* Штучний інтелект може бути використаний для розпізнавання облич на фото та відео з місць вчинення воєнних злочинів. Це може допомогти в ідентифікації підозрюваних, причетних до вчиненя таких злочинів, та встановленню свідків, які можуть повідомити важливу інформацію про розслідувану подію воєнного злочину; 7) *аналіз текстової інформації.* Аналіз штучним інтелектом текстової інформації (наприклад, повідомлень у соціальних мережах та інших джерелах), пов'язаної з воєнними злочинами, сприятиме ідентифікації підозрюваних і свідків та з'ясуванню криміналістично значущої інформації про воєнні злочини, які розслідуються[2].

Крім того, важливо враховувати законодавчі обмеження щодо застосування штучного інтелекту в розслідуванні злочинів, зокрема, заборони на використання деяких видів даних, які можуть порушувати права людини[3]. Усі ці фактори потребують ретельного аналізу та планування перед застосуванням штучного інтелекту в розслідуванні воєнних злочинів. Водночас, застосування штучного інтелекту є потужним інструментом в розслідуванні воєнних злочинів в Україні та може допомогти забезпечити справедливість та притягнути винних до відповідальності за вчинені такі воєнні злочини.

---

[1] Шевчук В. М. Використання інформації із соціальних інтернет-мереж при розслідувані кіберзлочинів: криміналістичні проблеми. *Кримінальні загрози в секторі безпеки: практики ефективного реагування*: матеріали панельної дискусії III Харків. міжнар. юридичного форуму (м. Харків, 26 вересня 2019 р.); Нац. юрид. університет ім. Ярослава Мудрого. Х.: Право, 2019. С.142–146.

[2] Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики.* Вип. 4 (29). 2022. С.12–46. С. 37.

[3] Baltrūnienė J., Shevchuk V. Artificial Intelligence Technologies in Law Enforcement and Justice: Ukrainian and European experience. *Цифрова трансформація кримінального провадження в умовах воєнного стану* : мат-ли Всеукр. круглого столу (Харків, 16.12.2022). Харків, 2022. С. 81.

Сучасні підходи до розслідування воєнних злочинів дають змогу визначити джерела цифрової інформації, якими зумовлено напрями збирання й дослідження цифрових слідів для отримання інформації: із мобільних пристроїв, вилучених в учасників кримінального провадження телефонів; із персональних комп'ютерів фізичних і юридичних осіб; із серверів та інших накопичувачів інформації в організаціях та установах; із радіочастотних ідентифікаторів, *GPS*-трекерів, датчиків, стаціонарних і мобільних вимірювальних пристроїв із використанням систем геолокації, відеоспостереження та позиціонування; із мережевих сервісів, що забезпечують голосовий і відеозв'язок між комп'ютерами через інтернет (*ICQ, Skype, WhatsApp, Viber, Telegram* та ін.); із банківських систем на цифрових носіях (*HDD, SSD*, флешкартках тощо); від стільникових операторів зв'язку щодо деталізації абонентського зв'язку й визначення місця знаходження абонента за допомогою геолокації; із записів камер відеоспостереження комерційних і державних структур; із вилучених в учасників кримінального провадження фотоапаратів і відеокамер[1].

Вбачається, що застосування технологій штучного інтелекту та процес цифровізації криміналістики є закономірним етапом розвитку й формування сучасних криміналістичних знань, який передбачає активне впровадження цифрових технологій у різні галузі криміналістики, судової експертології та юридичної практики. За таких умов в реаліях сьогодення необхідно активізувати розроблення нової галузі знань – цифрової криміналістики як стратегічного напрямку розвитку сучасної криміналістики. При цьому особливу увагу потрібно звернути на роль криміналістичної дидактики[2], зокрема, криміналістичну підготовку слідчих, судів, прокурорів, детективів, судових експертів у сфері цифрових технологій.

Час та практика показали, що в реаліях сьогодення засоби та технології штучного інтелекту сьогодні є провідною галуззю у сфері

[1] Матулєне С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: український та європейський досвід. *Теорія та практика судової експертизи і криміналістики.* Вип. 4 (29). 2022. С.12–46. С. 37.

[2] Malewski, H., Kurapka, V. E., Tamelė, I. Motivation and expectations of students-animportant factorin theimplementation of the new bachelor's degreeprogram «Law and Criminalistics. *The Criminalist of the First Printing*, 21/2021, 12–26.

цифрових технологій та цифрових телекомунікацій. Тому використання можливостей штучного інтелекту у роботі органів правопорядку та юстиції є насьогодні достатньо актуальними та затребуваними практикою.

Запитання для самоконтролю

1. Які інноваційні напрямки в криміналістиці існують на сьогодні?
2. Що є об'єктом вивчення воєнної криміналістики?
3. Що таке штучний інтелект (ШІ) та яка його роль в криміналістичній та судово-експертній діяльності?
4. Яким чином використовується ШІ у зарубіжній практиці правозастосовних органів?
5. Які основні напрямки використання ШІ в сучасних умовах?
6. Чи існують негативні тенденції у використанні ШІ?
7. Чи має використовуватися ШІ в розслідуванні воєнних злочинів?

Наукове видання

Шепітько Валерій Юрійович,
Авдєєва Галина Костянтинівна,
Коновалова Віолетта Омелянівна та ін.

ІННОВАЦІЙНІ МЕТОДИ, ЗАСОБИ ТА ТЕХНОЛОГІЇ В КРИМІНАЛІСТИЦІ ТА СУДОВІЙ ЕКСПЕРТИЗІ

Науково-практичний посібник

За редакцією академіка НАПрН України
В. Ю. Шепітька

Електронне наукове видання

Комп'ютерна верстка *А. Т. Гринченка*

Підписано до поширення через мережу Інтернет 29.12.2023.
Відповідає формату друкованого видання 60×84/16. Гарнітура Times.
Обл.-вид. арк. 5. Об'єм даних 2,9 Мб.
Вид. № 3285

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