Національна академія правових наук України

Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса
Національної академії правових наук України

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У КРИМІНАЛІСТИЦІ ТА СУДОВІЙ ЕКСПЕРТИЗІ

Збірник матеріалів міжнародного
науково-практичного "круглого столу",
м. Харків, 11 грудня 2023 р.

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

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У КРИМІНАЛІСТИЦІ ТА СУДОВІЙ ЕКСПЕРТИЗІ

Збірник матеріалів міжнародного науково-практичного круглого столу

м. Харків, 11 грудня 2023 року

Електронне наукове видання

Харків
«Право»
2024

УДК [343.1+343.98]:004(061)
В43

Редакційна колегія:
В. Ю. Шепітько, Г. К. Авдєєва

Рекомендовано до опублікування та поширення через мережу Інтернет вченою радою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України (протокол № 1 від 31 січня 2024 р.)

Використання цифрових технологій у криміналістиці та судовій
В43 експертизі : матеріали міжнар. наук.-практ. круглого столу, м. Харків, 11 груд. 2023 р. : електрон. наук. вид. / [редкол.: В. Ю. Шепітько, Г. К. Авдєєва] ; Нац. акад. прав. наук України ; НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса НАПрН України. – Харків : Право, 2024. – 144 с.

ISBN 978-617-8411-50-3

Видання містить матеріали міжнародного науково-практичного «круглого столу», присвяченого найбільш важливим і сучасним проблемам використання цифрової інформації в криміналістиці, судовій експертизі і кримінальному процесі. викладені матеріали обговорень таких наукових і практичних проблем: формування цифрової криміналістики та її роль в розслідуванні кримінальних правопорушень; впровадження інноваційних методів та застосування цифрових технологій в криміналістиці та судовій експертизі; цифрова інформація у розслідуванні кримінальних правопорушень; місце цифрових доказів у розслідуванні воєнних злочинів; проблеми використання цифрової інформації у кримінальному провадженні.

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

УДК [343.1+343.98]:004(061)

Матеріали викладено в авторській редакції з незначними коректорськими правками. Відповідальність за їхню якість, достовірність, а також відсутність у них відомостей, що становлять державну таємницю та інформацію для службового користування, несуть автори.

Видання в електронному вигляді розміщується у відкритому доступі на сайті НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України в розділі «Збірники матеріалів наукових заходів» (https://surl.li/kixgu) вкладки «Інфопідтримка». Для опису видання чи посилання на нього слід використовувати пряме посилання на збірник.

© Науково-дослідний інститут вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, 2024

ISBN 978-617-8411-50-3

ЗМІСТ

Батиргареєва В. С.
Вітальне слово учасникам «круглого столу» 6

НАУКОВІ ДОПОВІДІ ТА ПОВІДОМЛЕННЯ

Broniecka Rossana
Digital tools in criminal proceedings – 3D scanning of the crime scene 9

Błaszczak Bartosz
Społeczne postrzeganie przestępczości ubezpieczeniowej (Public perception of insurance crime; Суспільне сприйняття страхової злочинності) 13

Żywucka – Kozłowska Elżbieta, Kozlowsky Gabriela
Digital technology in post mortem research 18

Kąkol Andrzej
Policyjny system informatyczny wspierający dokumentowanie czynności dochodzeniowo-śledczych (Police IT system supporting the documentation of investigative activities; IT-система поліції, яка підтримує документування слідчих дій) 23

Kozlowsky Gabriela, Żywucka – Kozłowska Elżbieta
Computed tomography in the diagnosis of the head as a result of events subject to criminal law 29

Malinowska Irena
Komparatystyka wybranych kategorii oszustw na rynku ubezpieczeń społecznych w Polsce (Comparative analysis of selected categories of fraud in the social security market in Poland; Порівняльний аналіз окремих категорій шахрайства на ринку соціального забезпечення в Польщі) 33

Авдєєва Г. К.
Використання цифрових технологій в судово-експертній діяльності 36

Алексик Н. В.
Проблемні питання використання штучного інтелекту під час досудового розслідування 40

Білоус В. В.
Особливості проведення емпіричних досліджень при написанні дисертацій з криміналістики в умовах воєнного стану 45
Брендель О. І.
Сучасні можливості застосування судової експертизи у протидії кібернетичній злочинності 51
Брендель О. І.
Дослідження автентичності цифрових відео- та звукозаписів 56
Ващук О. П.
Штучний інтелект для швидкості обробки даних у розслідуванні злочинів 61
Глинська Н. В.
Ризики переведення документообігу в царині кримінального провадження в електронну форму: ідентифікація та керування 65
Дунаєва Т. Є.
Використання передових технологій у розслідуванні кіберзлочинів 71
Журавель В. А.
Програмування як засіб підвищення якості розслідування 75
Капустіна М. В.
Можливості сучасних інформаційних систем у судовому провадженні 79
Коваленко А. В.
Метадані як джерело криміналістично значущої інформації..... 82
Кожевніков О. А.
Питання сутності та форм використання спеціальнх знань на окремих етапах OSINT розслідувань..... 86
Колодіна А. С.
Інноваційні техніко-криміналістичні технології у практиці розслідування злочинів 89
Ляшевська Л. І.
Сутність цифрових доказів у кримінальному провадженні 93
Мороз Ю. В., Ясенок А. А.
Проблеми формування і розвитку цифрової криміналістики 97

Негребецький В. В.
Можливості цифрових біометричних технологій
в правоохоронній діяльності: досвід Великобрітанії 102
Неділько Я. В.
Особливості використання можливостей штучного інтелекту
під час розслідування кримінальних кіберправопорушень..... 107
Рєпіна Ю. С.
Ризики використання технологій штучного інтелекту
в кримінальній юстиції в Україні.....111
Сушко Р. О.
Проблеми впровадження систем автоматичного
розпізнавання облич в Україні 115
Тарнавська Л. М.
Науково-технічні засоби криміналістики: сутність та зміст 119
Тіщенко В. В.
Технологічні та евристичні аспекти у розслідуванні
кримінальних правопорушень..... 122
Фурман Я. В.
Особливості використання безпілотних літальних апаратів
під час огляду місця події 126
Чабанюк О. М.
Напрями використання цифрових технологій в судовій
економічній експертизі..... 129
Шевчук В. М.
Цифрові технології та європейський вектор розвитку
криміналістики під час війни 133
Шепітько В. Ю.
Використання інноваційних засобів та цифрових
технологій у кримінальному провадженні..... 137
Яремчук В. О.
Дослідження цифрової інформації при розслідуванні
кіберзлочинів 142

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

ВІТАЛЬНЕ СЛОВО УЧАСНИКАМ «КРУГЛОГО СТОЛУ»

Первою жертвою війни стає правда.
Джонсон Хайрам, американський політик кінця XIX –
першої половини XX ст.

Стало вже доброю традицією на базі творчого криміналістичного осередку нашого Інституту проводити наукові диспути з приводу сучасності й майбутніх абрисів науки криміналістики, яка дійсно перебуває на передньому краї боротьби зі злочинністю. І до неї, як до доцентрової складової, тяжіють інші науки, що роблять й свій внесок у викриття злочинів та запобігання їм.

Черговий рік надій і сподівань тільки-но розпочнеться, але в нас, учених, вже є чимало «старих» і «нових» зобов'язань, звітувати по яких невдовзі прийдеться перед юридичною громадою, суспільством, державою. Слова «війна», «агресія», «випробування», «виклики», відігравши свою трагічну пригнічуючу роль, згодом виявилися своєрідними тригерами наукових дисциплін у сфері права. Адже рефлексія з боку правових наук – це насамперед намагання відновити спаплюжену правду. А що ж криміналістика? Що ріднить криміналістику з правдою? Відповідь цілком очевидна – її ріднить із правдою правда і тільки правда. Адже поклик і призначення криміналістики – встановлювати цю саму правду, по крупицях, наполегливо, не звертаючи увагу а ні на що…

На долю українських криміналістів випали тяжкі випробування – не лише намагатися взяти верх над внутрішньою злочинністю, а й всьому світу завдяки своїй кропіткій праці викрити і довести злочинність дій російських загарбників. Останній факт, втрутившись в логіку процесів «планової» діджиталізації буття, так само має виявитися «полігоном» для демонстрації надможливостей штучного інтелекту, що покликаний

посилити конгітивні здібності людини. Отже, йдеться про Криміналістику Майбутнього з гірким «присмаком» війни…

Для себе я визначила 2024-й рік, що наступить, Роком Криміналістики. Напевно, таке визначення навіяне тією роллю та місцем, котре посідає ця наука в легіоні Добра, що веде непримириму боротьбу зі злом, ім'я якому злочинність. Саме криміналістична наука, послуговуючись результатами власних наукових досліджень, пропонує органам кримінальної юстиції теоретично обґрунтовані та перевірені на практиці методики розкриття злочинів, розслідування та судового розгляду кримінальних проваджень.

На перетині загального руху наукової думки у парадигмі діджиталізації соціуму та необхідності виборювати щодня й щоночі українським народом свою незалежність і свободу у криміналістиці визначаються принаймні кілька ключових напрямів, що можуть відіграти роль «повороту ключа» у замковій свердловині поки що зачинених дверей, за якими ховається новий рівень Всесвіту з невідомими до цього часу можливостями. Одним із таких маркерів майбутнього, безумовно, є народження кіберкриміналістики, що виявляється відповіддю на кіберзлочини, з одного боку, та необхідністю забезпечити надійний захист цифрових даних, із другого. Тому тісний коннект зі спеціалістами у сфері інформаційної безпеки має стати дороговказом на цьому шляху. До того ж з огляду на те, що з кожним днем збільшується обсяг цифрової інформації, криміналістам важливо розвивати методи аналізу великих обсягів даних для виявлення злочинних проявів, реалізації прогностичної функції криміналістики та здійснення кримінального профілювання. Крім того, використання автоматизації і штучного інтелекту може значно полегшити процеси аналізу доказів, виявлення злочинів та відновлення подій, що сталися.

Ще один архіважливий напрям у криміналістичній науці одержав назву аерокриміналістики. Цей напрям покликаний розкрити премудрості здійснення аерозйомки із застосуванням безпілотних літальних апаратів і використання геоінформаційних систем, заснованих на знімках із космосу, під час провадження широкого переліку процесуальних та інших дій. Водночас в умовах потенційного та реального ризику для життя та здоров'я фахівців, пов'язаного зі збройною агресією, цей напрям криміналістичної науки, як бачимо, здатний убезпечити останніх під час

виявлення й фіксації ними великих обсягів криміналістично значущих геопросторових даних.

Війна, без сумніву, дала потужний поштовх для розвитку біотехнологій та генетичної криміналістики. У 2022 році прийнято Закон України «Про державну реєстрацію геномної інформації людини», яким закріплено правові засади обробки геномної інформації людини з метою ідентифікації осіб, які вчинили кримінальне правопорушення, розшуку осіб, зниклих безвісти, та ін. Отже, застосування біотехнологій у криміналістиці може допомогти в розкритті злочинів, ідентифікації злочинців та використанні генетичних даних під час розслідувань.

Колись з американських детективних кінострічок ми дізналися, що є такі незвичайні для нашої криміналістичної мови фахівці, як профайлери. Саме ці фахівці є носіями важливого знання при дослідженні поведінки та психологічних мотивів злочинців. Уявляється, що із цим знанням пов'язується важливіший напрям розвитку криміналістики, адже розуміння мотивів дає можливість більш ефективно профілювати злочинців та запобігати їх злочинам.

У зв'язку із глобалізаційними процесами, що відбуваються у світі, та зростанням транскордонної злочинності все більшої популярності набуватиме міжнародне співробітництво і створення міжнародних стандартів у галузі криміналістики. Тому і в цьому плані образ криміналістики майбутнього бачиться як цифровий каркас знання, що зможе поєднати технології, аналітику та спеціалізовані знання задля виявлення та непримиримої боротьби з різними видами злочинності. Отже, сьогодні саме криміналістика може розв'язати завдання щодо генерації найсучаснішого та найпродуктивнішого інструментарію встановлення Правди….

Від імені найпотужнішого колективу нашого Інституту та від себе особисто бажаю всім учасникам наукового форуму плідної дискусії, творчого натхнення, відповідей на складні запитання та віри в те, що Перемога вже не за горами!

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

DIGITAL TOOLS IN CRIMINAL PROCEEDINGS – 3d SCANNING OF THE CRIME SCENE

Examination is one of the procedural activities used to obtain as much information as possible about the crime, enable reconstruction of events, allow identification of the perpetrator (perpetrators) of the event, allow collection of material evidence in the form of revealed and secured forensic traces, which in the further activities of detectors enable to prove the degree of participation in the crime of the perpetrator (perpetrators) [1, p.204].

It should be remembered that examinations are a unique enterprise, poorly performed may deprive you of evidence, often not obtainable by other sources of evidence. J. Mazepa rightly stated that the inspections «are the foundation of the whole case. The time of their conduct, the professionalism with which they were carried out, the scope of the activities carried out are of decisive importance for the fate of the preparatory proceedings (investigation-investigation)» [2, p.16].

Inspections should be carried out only after the formal initiation of proceedings. In urgent cases, as well as in cases necessary to protect evidence against loss or distortion, inspections may be carried out before the formal opening of proceedings.

Pursuant to Art. 308 § 1 of the Code of Criminal Procedure [3]. Within the limits necessary to protect the traces and evidence of a crime against their loss, distortion or destruction, the public prosecutor or the Police may in any case, in urgent cases, before issuing an order to initiate an investigation or investigation, carry out procedural measures to the extent necessary, and in particular carry out inspections, if necessary with the assistance of an expert, searches or the actions listed in Article 74 § 2, point (a) of the Code of Criminal Procedure.

1 k.p.k. in relation to the suspect, as well as to undertake other necessary actions towards him, not excluding the collection of blood, hair and body secretions. After these steps have been taken, in cases where investigation

by the prosecutor is mandatory, the prosecutor shall immediately refer the case to the prosecutor. Article 207 of the Code of Criminal Procedure lists three types of inspection: inspection of the place, person and property. For the purposes of this article, I will deal only with site visits.

In the Code of Criminal Procedure we find the term «site inspection». P. Horoszowski defines «place of inspection» as any area where any evidence can be found» [4, p.10–11]. During the site inspection, the site and all the things located in that particular part of the space are inspected. [5, p.89]. Inspection of a place is an activity that involves thoroughly familiarizing yourself with a specific space, as well as searching for and securing important traces that may be related to a crime.

From the content of art. 205 § 1 of the Code of Criminal Procedure it follows that if «conducting an inspection, interrogation using technical means enabling this activity to be carried out at a distance, an experiment, an expert opinion, the seizure of things or a search requires technical activities, in particular such as taking measurements, calculations, photos, recording traces, you may participate in them call specialists.» [3]. In this provision, the legislator used the term «in particular, such as measurements, calculations, photographs, recording of traces» , these are activities of an auxiliary and purely technical nature. The Code of Criminal Procedure did not mention technical activities, equipment, technologies, the use of which is permissible during inspections.

Article 147 § 5 of the Code of Criminal Procedure and the Regulation of the Minister of Justice of 14 September 2012 on the type of equipment and technical means used to record video or sound for trial purposes and on the method of storing, reproducing and copying recordings [6]. This regulation regulates issues related to records and storage of media, but does not contain any technical requirements that must be met during the inspection.

As the above-mentioned provisions indicate, thanks to the open catalog of technical and forensic activities that can be performed during an inspection at the scene of the incident, the legislator has created the possibility of carrying out visual inspection using a 3D scanner – as stated in Art. 205 §1 of the Code of Criminal Procedure «performing calculations, taking photos, recording traces».[7, p.10]

The method was developed thanks to advances in forensic techniques, which make it possible to use ground-based 3D scanning for surveillance activities at the scene of an incident. 3D scanning is a modern and dynamically

developing technology, which is used mainly in such specializations as: «construction and architecture, industrial engineering, geodesy, preservation of monuments and archaeology» [8, p.341]. 3D scanners allow for fairly fast acquisition of detailed data about the environment (this technique is often used in the United States and Australia).

3D scanning enables precise and efficient measurements of the designated area or the building as an event location, streamlines the work of the police, prosecutor's office and courts. 3D scanners allow researchers to create a full 360-degree image of a scene within minutes. There are two main technologies that are used in 3D laser scanners. These are: flight time and phase shift technology. These methods are used to precisely determine the position of a given object relative to the position of the scanner [9].

The 3D scanner allows access to most data from the scene at any time in the form of a 3D image. The value of using 3D scanners to investigate crimes is that evidence can be documented, analyzed and processed later if necessary [10].

The first attempt in Poland to explore the possibilities of using 3D laser scanning systems when conducting procedural inspections at the scene of a criminal incident and documenting them was undertaken by the Police School in Piła together with the 3D Scanning and Modeling Laboratory located at the Institute of the History of Architecture, Art and Technology of the Wrocław University of Science and Technology. Leica Geosystems. As part of practical workshops with the participation of a representative of Leica Geosystems, Waldemar Kubisz, and the head of the 3D Scanning and Modeling Laboratory and a lecturer from the Department of Forensic Science of the Police School in Piła, Jacek Kościuk [11]. A forensic examination of two simulated incident sites was carried out: a road accident and the place where a body was found. Investigative activities at the scene of the incident were carried out in accordance with the provisions of the Code of Criminal Procedure and the rules for carrying out such activities at the scene of a criminal incident [12]. During the inspection, traditional digital photogrammetry and a Leica ScanStation 2 scanner were used.

Currently, more and more police stations are equipped with 3D scanners – in 2017, police officers of the Poznań City Police Headquarters received such a 3D scanner, which is used at the scene of various types of crimes or road accidents [13]. In 2022, police technicians from the Podlachia garrison received the most modern equipment to work on the scene of disasters,

murders or other events of a criminal nature. The Z+F IMAGER 5016 scanner is designed for 3D laser scanning [14]. The same scanner was also received by the capital's technicians [15].

Bibliography :

1. Goc M., Oględziny [w:] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008.
2. Mazepa J., *Oględziny* [w:] Vademecum technika kryminalistyki, Pod red. J. Mazepy, Oficyna a Wolters Kluwer business, Warszawa 2009.
3. Ustawa z dnia 6 czerwca 1997 r. – Kodeks postepowania karnego, Dz.U.2022.0.1375
4. Horoszowski P., *Śledcze oględziny miejsca*, Warszawa 1959.
5. Kędzierska G., *Polskie prawo i kryminalistyka o oględzinach*, «Jurisprudencija» 2000, t. 18 (10).
6. ROZPORZĄDZENIE MINISTRA SPRAWIEDLIWOŚCI z dnia 14 września 2012 r. w sprawie rodzaju urządzeń i środków technicznych służących do utrwalania obrazu lub dźwięku dla celów procesowych oraz sposobu przechowywania, odtwarzania i kopiowania zapisów, poz. 1090.
7. Wieczorek T., Mączka K., Szymczak M., *Analiza możliwości wykorzystania skanów 3D z miejsca zdarzenia jako materiału dowodowego w postępowaniu sądowym w warunkach prawnych obowiązujących w Polsce*, «Przegląd Policyjny» 2018, nr 2(130).
8. Hołyst B., *Kryminalistyka*, Warszawa 2018.
9. Kowbuz D., *How 3D scanning rebuilds crime scenes for courtrooms?*, «Gim International» 2020, s. 1, www.gim-international.com/content/article/how-3d-scanning-rebuilds-crime-scenes-for-courtrooms.
10. T. Dees, How 3D scanning puts the crime scene in the courtroom, www.police1.com/police-products/3d-laser-scanners/articles/how-3d-scanning-puts-the-crime-scene-in-the-courtroomgHvPQrWHyMMSL3xC
11. Ebos, *Uwaga! Polska policja skanuje*, www.ebos.pl/artykul/uwaga_policja_skanuje
12. Szkoła Policji w Pile, *Krok w przyszłość kryminalistyki*, http://pila.szkolapolicji.gov.pl/spp/aktualnosci/2009–1/1825
13. https://www.policja.pl/pol/aktualnosci/150842,Nowoczesny-skaner-na-wyposazeniu-poznanskiej-Policji.html
14. https://podlaska.policja.gov.pl/pod/aktualnosci/83267,PODLASCY-POLICJANCI-KORZYSTAJA-JUZ-Z-NAJNOWOCZESNIEJSZEGO-SKANERA-3D.html
15. https://magazyn-ksp.policja.gov.pl/mag/wyposazenie/109505,Skaner-3D.html

Bartosz Błaszczak
PhD, *University of Vocational Training in Wrocław, Poland*

SPOŁECZNE POSTRZEGANIE PRZESTĘPCZOŚCI UBEZPIECZENIOWEJ

PUBLIC PERCEPTION OF INSURANCE CRIME

Abstract: *Insurance crime is defined as actions aimed at obtaining compensation (redress) in an amount higher than the actual loss or attempting to obtain compensation when no loss has occurred at all. The author cited public perceptions of insurance crime. The article covers the definition issues, the scale and magnitude of the phenomenon, legal methods of counteracting insurance crime , indicating the scope of meaning of the term and described the causes of the crime, its manifestations and social consequences as well as the tasks of institutions responsible for this category of crime.*

Key words: *insurance, crime, insurance market, law.*

Wyłudzenie odszkodowania jest czynem karalnym. W świetle kodeksu karnego, osoba, która w celu uzyskania odszkodowania z tytułu umowy ubezpieczenia, przyczynia się do zdarzenia będącego podstawą wypłaty świadczenia, podlega karze pozbawienia wolności od 3 miesięcy do 5 lat. Co ważne, karze podlega nie tylko osoba, która dopuści się takiego czynu, ale także każdy, kto jej w tym pomaga [1]. Przestępczość ubezpieczeniową definiuje się jako działania mające na celu uzyskanie odszkodowania (zadośćuczynienia) w kwocie wyższej, niż faktycznie wynosi szkoda lub próbę uzyskania odszkodowania w sytuacji, gdy szkoda nie wystąpiła w ogóle. Osoby, które chcą w ten sposób się wzbogacić, najczęściej: wprowadzają ubezpieczyciela w błąd, np. co do wartości i pochodzenia mienia czy stanu zdrowia, zatajenia faktów (np. stan mienia, przebyte choroby), podają fikcyjne danych osobowych, umyślnie niszczą mienie lub ingerują w systemy bezpieczeństwa (np. antypożarowe), samookaleczają się, podają nieprawdziwe okoliczności zaistnienia szkody, podają się za uprawnionego do odbioru odszkodowania. Podobnie jak w przypadku wielu innych działów gospodarki, tak i branża ubezpieczeniowa cierpi z powodu wyłudzeń, usiłowań i innych nielegalnych działań klientów, które zbiorczo określa się mianem

przestępczości ubezpieczeniowych. Jakie konsekwencje wiążą się z tego typu próbami? Jaka często do nich dochodzi? [2]. Zjawisko przestępczości ubezpieczeniowej, podobnie jak wszystkie inne zjawiska wchodzące w skład tak zwanej «szarej strefy», nie jest możliwe do zmierzenia w sposób bezpośredni. Nie każdy sprawca incydentu polegającego na próbie wyłudzenia odszkodowania, zostaje doprowadzony przed oblicze wymiaru sprawiedliwości. Różnorodność metod przestępczych stosowanych przez sprawców powoduje, że przestępczość ubezpieczeniowa wymyka się ścisłej klasyfikacji. Zwykle przy osądzaniu sprawców zastosowanie mają art. 286 i art. 298 k.k [3]. Zauważa się, że transformacje polityczne oraz gospodarcze w Polsce w latach dziewięćdziesiątych przyczyniły się do uwolnienia sektorów ubezpieczeń. Z jednej strony skupiono się na odpowiednim podjęciu dyskusji nad koniecznością kompleksowych reform zwłaszcza ubezpieczenia społecznego skupionego do tej pory w sposób monopolistyczny w jednym Zakładzie Ubezpieczeń Społecznych, natomiast z drugiej strony o wiele częściej podmiot gospodarczy jak również osoba fizyczna dostrzegała potrzebę do tego, aby ochronić ubezpieczeniową komplementarność związaną z prawidłowym rozwojem prywatnych przedsiębiorczości, ryzykiem finansowym jak również stanem posiadania społeczeństwa. Bardzo ważna tutaj jest funkcja związana z prawidłową ochroną, która to jest pełniona poprzez różnorodne ubezpieczenia gospodarcze, a mowa tutaj o majątkowych oraz osobowych, które co ważne są oferowane poprzez zakłady oraz towarzystwa ubezpieczeniowe, która przede wszystkim działają na normalnej zasadzie ekonomicznej zgodnie z obowiązującym prawem oraz warunkami wolnej gry rynkowej. Proces związany z dynamicznym rozwojem ubezpieczenia gospodarczego był zapoczątkowany poprzez Ustawę o działalności ubezpieczeniowej jej nowelami oraz Rozporządzeniem Ministrów Finansów. Aczkolwiek postrzega się też, że ubezpieczenie się jest bardzo mocno powiązane z rozwojem gospodarczym. Im dochodzi do większego rozwoju gospodarki, a to bowiem przyczynia się do wyższego standardu życia członków społeczeństwa, w tym też jest większa potrzeba na to, aby ubezpieczyć życie, zdrowie, czy też mienie. Przyczyną chęci ubezpieczenia jest fakt, że może dojść do jakiegoś zdarzenia, które to przede wszystkim spowoduje szkodę w mieniu, bądź utracenie zdrowia, czy też życia osoby, która miała zamiar się ubezpieczyć. Wyzwania instytucji ubezpieczeń są określone w ustawie o ubezpieczeniach, jak też w krajowych i międzynarodowych przepisach karnych. Aby obywatel mógł prawidłowo

funkcjonować w coraz to nowszym społeczeństwie ważne jest to, aby posiadał wiedzę o możliwych ubezpieczeniach jak również jego formach. Tego typu jest w dużej mierze niezbędna do wybierania określonych rodzajów ubezpieczeń. W dzisiejszych czasach w naszym kraju firmy ubezpieczeniowe w swojej ofercie posiadają mnóstwo istotnych rodzajów ubezpieczeń, które to bardzo często są o takiej samej nazwie. Ubezpieczenie należy do procesu ekonomicznego jak również społecznego. Szczególnym zjawiskiem w tej przestrzeni jest niemal powszechne, iż w ubezpieczeniu dochodzi do alokacji środka finansowego między ubezpieczycielem, a ubezpieczonym w sytuacjach ściśle określonej umowie ubezpieczenia. Alokacja tychże środków jest przede wszystkim uzależniona od ram prawnych, które mają regulować działania podmiotów ubezpieczeniowych. Prawidłowe funkcjonowanie ubezpieczenia na danym rynku powiązane jest z działalnościami marketingowymi zakładów ubezpieczeń oraz pośredników ubezpieczeniowych. Należy zwrócić uwagę na to, że ich działalność jest bardzo mocno zróżnicowana oraz co istotne jest mocno uzależniona od normy prawnej określonej w akcie legislacyjnym. W momencie wybierania zakładu ubezpieczeń przez daną osobę ważne jest to, aby dokonała ona odpowiedniej analizy zwłaszcza tej wskaźnikowej. Jeśli chodzi o proces ubezpieczenia się to należy on do procesu społecznego, gdzie mamy do czynienia z interakcją między przedstawicielem zakładu ubezpieczeń, a ubezpieczającym. Wszelkie możliwe elementy związane z funkcjonowaniem ubezpieczenia gospodarczego powiązane są z takimi mechanizmami jak: ekonomiczne, społeczne, prawne. Zakłada się, że źródło przestępczości ubezpieczeniowej można wyjaśniać poprzez grunt dorobku naukowego ekonomii behawioralnej, która to przyczynia się do zbadania wpływów emocji, wartości jak również instynktu ludzi za różnorodne zachowania oraz próbuje je w sposób odpowiedni wyjaśnić oraz zrozumieć. Prawidłowe zgłębienie motywu oraz podstawy działania przestępcy pozwala na określanie metody związanej ze skutecznym przeciwdziałaniem [4]. Stwierdzić należy, że przyzwolenie do nadużycia może należeć do udziału przeciętnego obywatela, która uchodzi za praworządnego w oczach własnych oraz innych osób. Obok zakresów licznych nadużyć, które to należą do znaczącego wyznacznika moralnych kondycji społeczeństwa bardzo podobny, ale również ważny wskaźnik to nic innego jak sam poziom akceptacji dla naruszenia normy, odwzorowujący społeczne przyzwolenia dla nadużycia. Przyzwolenie ma bowiem stworzyć odpowiednie środowisko dla tego typu nadużyć z tego względu, że osoba, które je popełnia w żaden sposób nie musi obawiać się

społecznych ostracyzmów, a co ważne może liczyć na akceptację ze strony środowiska [5]. Problem *misselingu* na rynku ubezpieczeniowym to zagadnienie złożone jak również dość często realizowane w ramach grupy przestępczej, organizowanej przede wszystkim poprzez pośredników ubezpieczeniowych, w których to uczestniczą zakłady ubezpieczeń zainteresowane sprzedawaniem produktów oraz pośrednicy, którzy utrzymują się tylko i wyłącznie z prowizji, która jest uzyskiwana w związku z fraudami, które to w celu zarobkowym sprzedają zupełnie niepotrzebne produkty ubezpieczeniowe. Osoby, które biorą udział w takim oto procesie uważane są za uczciwych obywateli, którzy akcentują system wartości, który został ukształtowany poprzez wyznawaną religię, rodzinę, czy też grupę społeczno-zawodową [6]. Źródła przestępczości można połączyć z trzema istotnymi zjawiskami takimi jak [7]: asymetria informacji, negatywna selekcja, hazard moralny, czyli pokusa nadużyć. Biorąc pod uwagę raport Polskiej Izby Ubezpieczeń, który odnosi się do przestępczości ubezpieczeniowej należy wywnioskować, że w 2022 roku w Polsce wykryto prawie 32 tysiące przypadków wyłudzeń odszkodowań. Ponad 8,6 tys. przypadków dotyczyło ubezpieczeń na życie, większość, bo ponad 23 tys. ubezpieczeń majątkowych. Udaremniono nienależne wypłaty na kwotę 409 mln złotych – 51,7 mln w ubezpieczeniach na życie oraz 357,3 mln zł w ubezpieczeniach majątkowych. W porównaniu z 2021 rokiem o ponad 25% wzrosła liczba przestępstw ubezpieczeniowych. Całkowita wartość przestępstw obniżyła się o 7%, jednak odnotowano duży wzrost wartości przestępstw w ubezpieczeniach na życie. Struktura przestępczości w Polsce cały czas się zmienia. Zwiększa się liczba popełnianych przestępstw gospodarczych, a zmniejsza liczba przestępstw kryminalnych. Sytuacja ta zapewne nie ulegnie w dalszym ciągu zmianie, a to oznacza, że również będzie przybywać przestępstw ubezpieczeniowych. Coraz większe znaczenie będą odgrywać zorganizowane grupy przestępcze, w tym grupy o zasięgu międzynarodowym. W rozumieniu współczesnym, łączącym badania naukowe z działalnością ubezpieczeń stwierdza się, iż w zarówno w ubezpieczeniach komunikacyjnych jak i ubezpieczeniach na życie i zdrowie będzie przybywać wyłudzeń odszkodowań związanych głównie ze szkodami osobowymi, przed szkodami majątkowymi. Dziać się tak będzie głównie ze względu na dużą łatwość w uzyskaniu takiego odszkodowania i fakt, że zakłady ubezpieczeń nie przyzwyczajone do takich roszczeń nie mają wypracowanych skutecznych mechanizmów obronnych przed nadużyciami w tym zakresie [8].

Bibliografia :

1. Ubezpieczenia, https://beesafe.pl/abc-ubezpieczen/wyludzenie-ubezpieczenia/, [dostęp: 24.11.2023].

2. Czym jest przestępczość ubezpieczeniowa, https://eurofinance.info.pl/blog/ubezpieczenia-wiedza/czym-jest-przestepczosc-ubezpieczeniowa/, [dostęp: 24.11.2023].

3. Majewski P., Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń, Warszawa 2018, s.6, https://piu.org.pl/wp-content/uploads/2018/11/PIU_analiza_przestepstw-2017.pdf, [dostęp: 24.11.2023].

4. T. Tyszka, Decyzje. Perspektywa psychologiczna i ekonomiczna, Warszawa 2010, s. 127.

5. M. Romanowska, *Leksykon zarządzania*, Warszawa 2004, s. 501.

6. S. Messner, R. Rosenfeld, Markets, *Morality and an Institutional Anomie Theory od Crime*, (w:) The Future od Anomic Theory, Boston 1997, s. 5.

7. Polska Izba Ubezpieczeń, https://piu.org.pl/analiza-przestepczosc-ubezpieczeniowa-w-2022-r-2/, [dostęp: 24.11.2023].

8. Miksiewicz D., Charakterystyka przestępczości ubezpieczeniowej w Polsce, Studenckie Zeszyty Naukowe, 2015, file:///C:/Users/imalinowska/Downloads/2106-5059-1-SM.pdf, [dostęp: 24.11.2023], s.17.

Elżbieta Żywucka – Kozłowska
Phd. hab. dr of law, assoc. prof., University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Criminal Procedure and Executive Criminal Law, Olsztyn city, Poland

Gabriela Kozlowsky
5th year student of medicine, Faculty of Medicine, Ivano-Frankivsk National Medical University, Ivano-Frankivsk city, Ukraine

DIGITAL TECHNOLOGY IN POST MORTEM RESEARCH

Digital technology has become a permanent part of many fields of modern science. Today, no one is surprised by digital X-rays, not to mention computed tomography or magnetic resonance imaging [1]. In the 1970s, CT was used for the first time to examine human cadavers [2]. It is debatable whether the examination of a human mummy is equivalent to the examination of a human corpse, given the fact that the mummy does not have internal organs extracted from the cavities of the body during the embalming process. The literature on the subject emphasizes that post-mortem examinations with the use of CT allow a broader diagnosis of the cause of death [3]. While in the last century this technique was rare, nowadays it is increasingly used before classical autopsy, which obviously results in greater accuracy [1]. Forensic practice is currently using a high-resolution 3D scanner for imaging objects According to Krzysztof Maksymowicz, Magdalena Kobielarz and Tomasz Jurek, it is a non-contact and non-destructive method that allows observation and data collection using a laser beam. What is particularly important – it leaves the evidence intact, and this is important from the point of view of criminal proceedings, because the examined object remains intact, and what is obvious is extremely important from the point of view of the evidential value of the examined object. This technique allows parallel archiving of levies, fast remote transfer. The authors emphasize the possibility of comparing evidence secured in this way with data collected in law enforcement databases. Another attribute, according to the cited authors, is the low cost of 3D scanning, as well as the very simple operation and the possibility of cooperation, as they say, with all tools operating in digital technology [4]. The medical literature indicates the usefulness of digital radiology techniques in the process of individual identification. Dorota Lorkiewicz-Muszyńska, Adrian Rajczyk, Agnieszka

Cugier and Marzena Łabęcka underline that «skeletal elements such as the skull or extracranial skeletal elements may show significant usefulness in identification studies. Long bones, vertebrae, complete skull, or surviving parts of the skull comprising important structures exhibiting high interpersonal variability, e.g. the temporal mammary appendage, paranasal sinuses, maxillary sinuses, and, finally, the frontal sinus, may show significant usefulness in the process of individual identification. A wide range of population studies allow to know inter-individual, inter-sex and inter-population differences, and the observed variability indicates the uniqueness of the morphological structure of the frontal sinus» [5]. The authors cited draw attention to an important detail, namely that «the frontal bay is characterized by a great diversity of structure and is a structure which, after obtaining its final shape, around the age of 20 years, usually remains unchanged» [5]. It is clear that this structure can change as a result of mechanical injury, cancerous changes and aging-related changes. Digital radiology is the field that allows precise determination of the structure of the examined area of the body, in this case the frontal sinus [6], [7]. The cited authors emphasize that the frontal sinuses can be compared to fingerprint lines, due to the uniqueness (individuality) of features, which results from both the literature and the experiences of these authors. Computed tomography is increasingly used in postmortem examinations (in cases of significant destruction of the corpse). Such cases are not uncommon in the practice of forensic physicians (railway accidents, burnt corpses, dismembered corpses). Krzysztof Woźniak, Artur Moskała, Andrzej Urbanik and Małgorzata Kłys described cases of postmortem examinations of human corpses after mechanical injuries (with significant energy), causing destruction and erasure of the anatomical order [8]. According to these researchers, «the post-mortem CT scan with 3D reconstruction should be the procedure of choice in the future in the thanatological diagnosis of victims of accidents with significant trauma energy» [8]. It is difficult to disagree with such a thesis, especially in the case of air and rail accidents. The accuracy of the 3D diagnostic method removes doubts that were previously impossible to assess due to limited exploratory capabilities of a cognitive nature. The literature on the subject emphasizes that digital technologies – computed tomography and magnetic resonance imaging, until recently used in clinical practice, have been successfully adapted to postmortem examinations [9], [10], [11]. Rafał Skowronek and Czesław Chowaniec, analyzing the dissection techniques, report: «Thali, Dirnhofer and Vock from the University of Bern developed an original technique at the end of the 20th

century, which they named Virtopsy® (Virtual Autopsy).It involves the use of data collected through laser scanning of cadavers, 3D photogrammetry, computed tomography (CT), magnetic resonance imaging (MRI) and spectroscopy» [12]. They emphasize that this technique is non-invasive, which is important in both medical and forensic practice. It is also worth adding that other diagnostic techniques, present in clinical procedures, are used in postmortem examinations. The literature indicates ultrasonography, which is not as accurate and precise as computed tomography or magnetic resonance imaging, which is natural, but significantly broadens the cognitive perspective [13]. Jerzy Gąsiorowski, describing new technologies in forensic science, emphasizes the importance of postmortem examinations performed in the technique of computed tomography. The cited author writes that «computed tomography in postmortem examination offers a number of possibilities, such as: 1) accurate analysis of bone structure in terms of possible injuries (fractures), individual features, with their subsequent visual 3D reconstruction, easier to accept than «classic» photographic photographs of «bloody» preparations with soft tissues or previously prepared and macerated bones, 2) definition of space which makes it possible to demonstrate post-traumatic lesions that are difficult to verify in the classical autopsy technique leading to death – e.g. air embolism of the heart or to indicate the course of wound ducts, e.g. in gunfire, especially in cases with damage to bone structures, 3) visualize the level of fluids – e.g. presence of blood in the pleural cavities or fluid in the sinuses of the nose in cases of drowning 4) evaluation of soft tissues, including musculoskeletal organs – it should be noted, however, that without the use of a contrast agent, the scope of evaluation is limited, 5) image recording 6) the use of a CT examination in a screening system in cases where there is no obvious indication for a forensic autopsy of the corpse» [14]. It is impossible not to add that it is possible to combine digital techniques with other types of tests, such as thin-needle biopsy. Many of the latest diagnostic methods in clinical medicine can also be successfully used in forensic medicine in post-mortem examinations [15], [16]. The literature on the subject emphasizes that radiological (post-mortem) examinations should be mandatory in case of mass events. The Commission for Forensic Imaging Research at the Polish Society of Forensic Medicine and Criminology indicates that the method of first choice in such cases is computed tomography [17].

Digital (post-mortem) research enables precise determination of the cause of death of a person. In the context of the position of the Forensic Imaging

Commission operating at the Polish Society of Forensic Medicine and Criminology operating in Poland are those that can be used in cases of war crimes (murder) of a mass nature, air or rail disasters. The usefulness of computed tomography in forensic medicine is unique, as is the 3D scanning of the scene in forensics [18].

The reporting framework, does not allow describe mentioned test methods from a technical perspective. The clue is the usefulness of digital technologies in each field of medicine, including forensic medicine, what was previously impossible to determine is now a known fact.

Bibliography :

1. Urbanik A., Chrzan R. (2013). Zastosowanie badania tomografii komputerowej (TK) dla potrzeb medycyny sądowej.Przegląd Lekarski, 70(5).

2. Harwood-Nash D. C., Computed tomography of ancient Egyptian mummies. JCAT1978, 3, 768

3. Hayakawa M., Yamamoto S., Motani H. et al.: Does imaging technology overcome problems of conventional postmortem examination? A trial of computed tomography imaging for postmortem examination. Int. J. Legal Med. 2006,120, 24.

4. Maksymowicz K., Kobielarz M., Jurek T. (2009). Skanowanie 3D jako metoda obrazowania złożonych i rozległych relacji przestrzennych dla potrzeb medycyny sądowej i kryminalistyki-ocena przydatności. *Wiadomości Konserwatorskie*, (26), 689–695.

5. Lorkiewicz-Muszyńska D., Rajczyk A., Cugier A., Łabęcka M., Znaczenie zmienności międzyosobniczej budowy morfologicznej zatoki czołowej w identyfikacji pośmiertnej przy użyciu metod radiografii cyfrowej. (w:) Nauki Przyrodnicze i Medyczne: Najnowsze doniesienia dotyczące nauk medycznych i biotechnologicznych, Lublin 2018, s.69.

6. Marques JAM, Musse JO, Gois BC, Galvão LCC, Paranhos LR.: Cone-beam computed tomography analysis of the frontal sinus in forensic investigation. Int. J. Morphol. 2014; 32(2): 660–665. doi.org/10.4067/S0717–95022014000200046

7. Patil N, Karjodkar FR, Sontakke S, Sansare K, Salvi R.: Uniqueness of radiographic patterns of the frontal sinus for personal identification. Imaging Sci Dent. 2012; 42(4):213–217. doi: 10.5624/isd.2012.42.4.213.

8. Woźniak K., Moskała A., Urbanik A., Kłys M. (2010). Wartość pośmiertnych badań TK w przypadkach urazów mechanicznych powodujących znacznego stopnia destrukcję zwłok. Archiwum Medycyny Sądowej i Kryminologii, 60(1).

9. Woźniak K. J., Moskała A., Kluza P., Romaszko K., Lopatin O., Rzepecka-Woźniak E., Whole body post-mortem computed tomography angiography of a new born revealing transposition of great arteries, Int J .Legal Med., November 2015, Volume 129 Issue 6 , 1253–1258.

10. Ampanozia G., Hatcha G. M., Rudera T., Flacha P. M. Germerotta T., T ali M. J., Eberta L. C.. Post- mortem virtual estimati on of free abdominal blood , volume, Eur. J. Radiol. 81 (2012), 2133–2136.

11. Maksymowicz K. (2016). Zastosowanie technologii obrazowania 3D w opiniowaniu medyczno-sądowym. Uniwersytet Medyczny im. Piastów Śląskich we Wrocławiu.

12. Skowronek R., Chowaniec C., (2010). Ewolucja techniki sekcyjnej – od Virchowa do Virtopsy®. *Arch. Med. Sad. Krym., 2010l LX*, 48–54.

13. Fariña J., Millana C., Jesús Fdez-Aceñero M., Furió V., Aragoncillo P., Martín V. G., Buencuerpo J., Ultrasonographic autopsy (echopsy): a new autopsy technique. Virchows Arch, 2002, 440, 635–639.

14. Gąsiorowski J., Nowoczesne technologie w kryminalistyce. Kultura Bezpieczeństwa. Nauka –Praktyka –Refleksje 21 (2018); 73–114.

15. Woźniak K., Moskała A., Urbanik A., Kłys M., Pośmiertne badania obrazowe TK z rekonstrukcją 3D u ofiar wypadków drogowych, Archiwum Medycyny Sądowej i Kryminologii, 2009, t. 59, nr 2.

16. Woźniak K., Urbanik A., Moskała A., Chrzan R., Kamieniecka B., Konfrontacja klinicznego obrazu tK złamań kości czaszki z wynikami badania sekcyjnego, Archiwum Medycyny Sądowej i Kryminologii, 2008, LVIII.

17. Borowska – Solonynko, A., Dąbkowska A., Moskała A., Teresiński G., Woźniak K. (2018). Radiological examination of mass disaster victims – position statement of the Forensic Imaging Examinations Commission at the Polish Society of Forensic Medicine and Criminology. Archiwum Medycyny Sądowej i Kryminologii/Archives of Forensic Medicine and Criminology, 68(3), 201–207.

18. Juszka K., Skanowanie 3D w realizacji zasad efektywnego przeprowadzania oględzin w sprawach zabójstw, [w:] Oblicza współczesnej kryminalistyki. Księga jubileuszowa Profesora Huberta Kołeckiego, E. Gruza (red.), Warszawa 2013.

Andrzej Kąkol
asystent w Collegium Balticum – Akademia Nauk Stosowanych w Szczecinie, Polska

POLICYJNY SYSTEM INFORMATYCZNY WSPIERAJĄCY DOKUMENTOWANIE CZYNNOŚCI DOCHODZENIOWO-ŚLEDCZYCH

Elektroniczny Rejestr Czynności Dochodzeniowo-Śledczych powstał w celu usprawnienia pracy policjantów prowadzących postępowania przygotowawcze [1]. Potrzeba opracowania takiego rozwiązania (narzędzia) była niejednokrotnie sugerowana przez policjantów wykonujących i nadzorujących czynności dochodzeniowo-śledcze. Idea wprowadzenia w jednostkach organizacyjnych Policji odpowiedniego narzędzia informatycznego, wspierającego takie czynności narodziła się w listopadzie 2014 r. Wymagała też tego nowela przepisów postępowania karnego, która weszła w życie z dniem 1 lipca 2015 roku.

Jak wskazywała praktyka dotychczas w części jednostek użytkowane były aplikacje lokalne, zbudowane na bazie arkuszy kalkulacyjnych lub wykorzystujące proste bazy danych. Część garnizonów wypracowała rozwiązania, bardziej lub mniej zaawansowane, które wykorzystywały pracę w sieci. Funkcjonalność tych aplikacji była bardzo zróżnicowana i niejednokrotnie ograniczała się do realizacji podstawowych czynności ewidencyjnych. Kierując się potrzebą jego stworzenia Komendant Główny Policji wydał decyzję nr 20 Komendanta Głównego Policji z 17 stycznia 2014 r. w sprawie powołania zespołu do opracowania studium wykonalności narzędzia informatycznego wspierającego dokumentowanie czynności dochodzeniowo-śledczych oraz czynności rejestracyjnych w ramach prowadzonych postępowań przygotowawczych, którego zadaniem było wskazanie możliwych do zautomatyzowania czynności realizowanych przez Policję w toku prowadzonych postępowań przygotowawczych i wyszukanie rozwiązań wspierających powyższe procesy poprzez zastosowanie narzędzi informatycznych. W wyniku powyższych prac sformułowano założenia budowy systemu zastępującego tradycyjną ewidencję prowadzoną w formie papierowej. Z uwagi na fakt, że Policja nie posiadała centralnej aplikacji umożliwiającej wspomaganie funkcjonariuszy w czynnościach rejestracyjnych

podjęto decyzję o budowie systemu w architekturze rozproszonej z wykorzystaniem narzędzia informatycznego, które funkcjonowało już w jednym z garnizonów Policji. ERCDŚ został wdrożony i produkcyjnie uruchomiony 1 stycznia 2015 r. we wszystkich jednostkach Policji i CBŚP.

Prowadzenie ERCDŚ i przetwarzanie w nim danych w formie elektronicznej odbywa się w celu wykonywania czynności dochodzeniowo-śledczych i techniczno-kryminalistycznych oraz realizacji wszelkich obowiązków ustawowych wynikających z przepisów ustaw wymienionych w § 1 Zarządzenia Nr 4 Komendanta Głównego Policji w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych Policji oraz przechowywania przez Policję dowodów rzeczowych uzyskanych w postępowaniu karnym z dnia 9 lutego 2017 r. [2], tj.:

a) ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego [3];

b) ustawy z dnia 10 września 1999 r. – Kodekskarny skarbowy [4];

c) ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich [5].

Zgodnie z § 1 Zarządzenia nr 31 Komendanta Głównego Policji z dnia 6 października 2020 r. w sprawie funkcjonowania Elektronicznego Rejestru

Czynności Dochodzeniowo-Śledczych [6] ERCDŚ prowadzi się w Komendzie Głównej Policji w systemach teleinformatycznych Policji, jako system służący do przetwarzania w formie elektronicznej, w sposób zautomatyzowany, informacji i danych osobowych gromadzonych przez Policję w urządzeniach ewidencyjnych w ramach prowadzonych postępowań karnych, karnych skarbowych i w sprawach nieletnich.

Rejestracja prowadzonych przez Policję postępowań oraz związanych z nimi czynności procesowych prowadzona jest w urządzeniach ewidencyjnych w ERCDŚ. Urządzenia ewidencyjne ERCDŚ funkcjonują w oparciu o bazę danych w wersji MySQL 5.6.10, serwer Apache/PHP 5.3.3 oraz system operacyjny CENTOS LINUX 6.4 (lub nowszy). Przetwarzanie danych odbywa się w oparciu o platformę klient-serwer w obrębie PSTD. Aplikacja działa w formie witryny internetowej Web 2.0. Dostęp do programu jest możliwy tylko poprzez przeglądarkę internetową. Wspierane są wszystkie najnowsze wydania najpopularniejszych przeglądarek – Firefox 18+, Chrome 30+. Wszystkie żądania do aplikacji są przesyłane za pomocą szyfrowanej wersji protokołu HTTP – czyli HTTPS. Blokowanie dostępu do aplikacji realizowane jest z poziomu aplikacji poprzez odebranie użytkownikowi prawa logowania do aplikacji. Dostęp do systemu operacyjnego serwera posiada administrator

techniczny oraz osoby przez niego wyznaczone. Dostęp do danych osobowych przetwarzanych w ERCDŚ może mieć miejsce wyłącznie po uwierzytelnieniu uprawnionego użytkownika aplikacji w systemie operacyjnym. Ponadto system jest regulowany poprzez przypisanie użytkowników do odpowiednich poziomów dostępu oraz aktywowanie konta użytkownika. Zarządzanie użytkownikami możliwe jest z poziomu aplikacji tylko dla użytkownika z odpowiednimi uprawnieniami.

W ERCDŚ prowadzi się następujące urządzenia ewidencyjne :

1. rejestr śledztw i dochodzeń (e-RSD);
2. rejestr postępowań sprawdzających (e-RPS);
3. rejestr czynności zleconych do wykonania przez jednostki Policji albo inne organy uprawnione do prowadzenia postępowania przygotowawczego (e-RPP);
4. księgę dowodów rzeczowych (e-KDRz);
5. rejestr wystąpień sądu lub prokuratora, o których mowa w art. 20 § 2 k.p.k. [3] i 326 § 4 k.p.k. [3] (e-RW);
6. rejestr wydanych postanowień o dopuszczeniu dowodu z opinii biegłego i wykonanych badań specjalistycznych (e-RPB);
7. rejestr podejrzanych, wobec których zastosowano środek zapobiegawczy w postaci dozoru Policji (eDozory);
8. rejestr czynności techniczno-kryminalistycznych (e-RCTK);
9. rejestr badań kryminalistycznych (e-RBK);
10. rejestr pozytywnych wyników sprawdzeń uzyskanych z krajowych lub zagranicznych baz śladów biologicznych albo daktyloskopijnych (e-RPWS);
11. wykaz biegłych sądowych i tłumaczy przysięgłych (e-WBiT);
12. skorowidz podejrzanych;
13. skorowidz zawiadamiających/pokrzywdzonych.

Na podstawie danych ERCDŚ można generować formularze procesowe lub rejestracyjno-statystyczne. Rejestry są prowadzone dla każdego roku kalendarzowego, z zachowaniem kolejności wpisów postępowań w ciągu roku. ERCDŚ umożliwia zautomatyzowaną lub częściowo zautomatyzowaną wymianę informacji z innymi systemami policyjnymi i pozapolicyjnymi.

W ERCDŚ stosuje się następujące operacje przetwarzania informacji, w tym danych osobowych:

1. wprowadzanie – polegające na dodawaniu informacji, w tym danych osobowych, po raz pierwszy do urządzenia ewidencyjnego;

2. odczytywanie – polegające na zapoznaniu się z informacjami, w tym danymi osobowymi, znajdującymi się w urządzeniach ewidencyjnych;

3. modyfikowanie – polegające na zmianie zawartości informacji, w tym danych osobowych, znajdujących się w urządzeniu ewidencyjnym, w tym zmianie zarejestrowanych informacji lub ich uzupełnieniu;

4. weryfikowanie – polegające na sprawdzaniu poprawności, kompletności i prawidłowości zarejestrowanych informacji, w tym danych osobowych, lub na dokonywaniu oceny przydatności lub niezbędności tych informacji do dalszego ich przetwarzania;

5. udostępnianie – polegające na udostępnieniu informacji, w tym danych osobowych, ze zbioru danych innemu uprawnionemu podmiotowi, bez względu na formę tej czynności;

6. przekazywanie – polegające na przekazywaniu informacji, w tym danych osobowych w obrębie ERCDŚ innej jednostce lub komórce organizacyjnej Policji, w szczególności w wyniku podjętej decyzji procesowej lub organizacyjnej;

7. usuwanie – polegające na zniszczeniu lub deformacji informacji, w tym danych osobowych, w sposób uniemożliwiający dalsze ich odtworzenie;

8. wykorzystywanie – polegające na korzystaniu lub użyciu informacji, w tym danych osobowych, uzyskanych w wyniku sprawdzenia w celu realizacji ustawowych zadań Policji;

9. koordynowanie – polegające na wyszukiwaniu i wskazywaniu informacji zapisanych w urządzeniach ewidencyjnych służących realizacji celów określonych w art. 297 k.p.k. [3], a także ustaleniu czy zachodzą przesłanki określone w art. 17 § 1 pkt 7 k.p.k. [3];

10. pseudonimizowanie – polegające na przetworzeniu danych osobowych w taki sposób, aby nie można było ich już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

Dokumentami stanowiącymi podstawę do wprowadzania do urządzeń ewidencyjnych informacji i danych osobowych są:

1. zawiadomienie o przestępstwie;

2. materiały postępowania w niezbędnym zakresie, o których mowa w art. 308 k.p.k. [3];

3. materiały zebrane w trybie art. 32e § 1 u.p.n. [5] z odpowiednimi dekretacjami kierownika jednostki organizacyjnej Policji lub osoby przez niego upoważnionej;

4. postanowienie o wszczęciu dochodzenia lub śledztwa;

5. zarządzenie prokuratora o powierzeniu śledztwa Policji;

6. postanowienie lub zarządzenie wydane w toku postępowania przez policjanta, prokuratora lub sąd;

7. protokół z czynności procesowej;

8. inny dokument zawierający podlegające wprowadzeniu informacje lub dane.

W odniesieniu do danych ERCDŚ, w celu zapewnienia zgodności trybu gromadzenia informacji z celem ich wprowadzania, zapewnienia integralności i bezpieczeństwa informacji, monitorowania danych wprowadzonych w ERCDŚ oraz w celu weryfikacji poprawności i zgodności z prawem, a także jako jeden ze środków ochrony, o której mowa w art. 39 pkt 3–7 UDODO [7], wykonuje się czynności kontroli i nadzoru służbowego obejmujące:

1. dostęp do danych ERCDŚ;

2. przetwarzanie danych ERCDŚ;

3. uprawnienia do przetwarzania danych ERCDŚ.

Niewątpliwe system ten jest jednym z kluczowych narzędzi informatycznych wspomagających pracę policji, w szczególności pionu kryminalnego. Zastąpienie rejestrami elektronicznymi papierowych ewidencji w obrębie prowadzonych postępowań przygotowawczych spowodowało uporządkowanie i usystematyzowanie wykonywanych zadań przez policję na każdym jej szczeblu organizacyjnym.

Aplikacja stale się rozwija, uzyskując coraz większe możliwości. Rozwój nowych technologii informatycznych nie tylko podnosi profesjonalizm wykonywanych czynności przez funkcjonariuszy i pracowników policji, ale daje także impuls do szukania nowych rozwiązań w zakresie wdrażania kolejnych oraz doskonalenia już posiadanych funkcjonalności systemu. Wydaje się, że ERCDŚ jest narzędziem ściśle dostosowanym do specyfiki funkcjonowania policji, a jego rozwój gwarantuje usprawnienie i rozwiązanie napotkanych problemów. Aplikacja stale się rozwija, uzyskując coraz większe możliwości. Rozwój nowych technologii informatycznych nie tylko podnosi profesjonalizm wykonywanych czynności przez funkcjonariuszy i pracowników policji, ale daje także impuls do szukania nowych rozwiązań w zakresie wdrażania kolejnych oraz doskonalenia już posiadanych

funkcjonalności systemu. Wydaje się, że ERCDŚ jest narzędziem ściśle dostosowanym do specyfiki funkcjonowania policji, a jego rozwój gwarantuje usprawnienie i rozwiązanie napotkanych problemów [8, p.28].

Bibliografia :

1. Zarządzenie nr 31 Komendanta Głównego Policji z dn. 6 października 2020 r. w sprawie funkcjonowania Elektronicznego Rejestru Czynności Dochodzeniowo-Śledczych (Dz. Urz. KGP z 2020 r. poz. 53.), zwany dalej ERCDŚ.
2. Zarządzenie Komendanta Głównego Policji w sprawie niektórych form organizacji i ewidencji czynności dochodzeniowo-śledczych Policji oraz przechowywania przez Policję dowodów rzeczowych uzyskanych w postępowaniu karnym z dnia 9 lutego 2017 r. (Dz. Urz. KGP z 2017 r. poz. 9.)
3. Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (Dz. U. z 1997 r., nr 89, poz. 555 z późn. zm.).
4. Ustawa z dnia 10 września 1999 r. – Kodeks karny skarbowy (Dz. U. z 1999 r., nr 83, poz. 930 z późn. zm.).
5. Ustawa z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich (Dz. U. z 1982 r., nr 35, poz. 228 z późn. zm.).
6. Zarządzenie nr 31 Komendanta Głównego Policji z dn. 6 października 2020 r. w sprawie funkcjonowania Elektronicznego Rejestru Czynności Dochodzeniowo-Śledczych (Dz. Urz. KGP z 2020 r. poz. 53).
7. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
8. M. Bałęcki, Kierunki rozwoju policyjnego systemu informatycznego wspierającego dokumentowanie czynności dochodzeniowo-śledczych i techniczno-kryminalistycznych (Problemy Kryminalistyki 291(1), 2016.

Gabriela Kozlowsky
5th year student of medicine, Faculty of Medicine,
Ivano-Frankivsk National Medical University, Ivano-Frankivsk city, Ukraine

Elżbieta Żywucka – Kozłowska
Phd. hab. dr of law, assoc. prof., University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration, Department of Criminal Procedure and Executive Criminal Law, Olsztyn city, Poland

COMPUTED TOMOGRAPHY IN THE DIAGNOSIS OF THE HEAD AS A RESULT OF EVENTS SUBJECT TO CRIMINAL LAW

Since time immemorial, people have suffered injuries, whether not in wars, then in everyday life. Head injuries occur as a result of various events, such as accidents, mass disasters, gunshots and intentionally inflicted blows. The clinical picture of just those mentioned above varies, among others, due to the extent, damage to bone structures and soft tissues, etc. The most common injuries include: cuts to the eyebrows, fractures of the nasal bones, fractures of the zygomatic bones, fractures of the mandible, fractures of the scales of the frontal bone, cracks (fractures) of the bones of the upper jaw, tooth fractures, cuts to the lips of the mouth, concussions, bleeding into the cerebral ventricles, tearing of the cerebellar tentorium. Each of the above-mentioned injuries may occur as a single injury or may occur together. In addition to those mentioned above, there are bloody spots (usually in the form of eye bruises), but also in other areas of the face and brain. In some cases, intracranial bleeding is diagnosed, often requiring surgical intervention [1, p.357]. Bone fractures (in the broadest sense) are a consequence of the tool acting on the bone with significant force. The continuity of the bone tissue is interrupted, which is not the case in cases of fractures, where the morphological structure is disrupted without interruption of the tissue continuity [2. p. 362]. Injuries to the central nervous system – the brain – are considered the most dangerous and can lead to a threat to life or death [3. p. 27]. Head injuries, of course, have different consequences, from quickly healing abrasions of the epidermis, minor cuts and contusions, to life-threatening ones (post-traumatic brain edema, intracranial bleeding). The ultimate result of head injuries is death. Computed tomography has become a permanent part of clinical diagnostics, including

traumatology. It is a precise method of assessing the effects of injuries suffered as a result of various events, including those subject to legal and criminal assessment (assault, murder, road accident, railway accident, plane accident, abuse, attempted murder) [4], [5]. This research method could be called universal, if only because not only bone structures but also soft tissues can be examined. It is equally well used in neurosurgical, neurological, internal medicine, oncological, pulmonological and gynecological diagnostics as well as in forensic medicine, including post-mortem examinations. It can be said that CT has entered diagnostic practice in cases of severe head injuries (gunshots, post-explosion effects or other origins)[6]. The literature on the subject indicates that head injuries are primarily concussions. According to Andrzej Żyluk, Agnieszka Mazur and Bernard Piotuch, «textbooks do not provide precise instructions on the diagnostic and treatment procedures for the so-called concussion or minor head injury, when there are no abnormalities in the neurological examination and there is only a temporary loss of consciousness (or even not) as a result of the injury – in an interview collected most often from the patient (not from witnesses). The most common practice is radiological diagnosis and 2–3 days of hospital observation.» [7]. Most often, the consequences indicated by the cited authors occur in traffic accidents, beatings, attempted murders, and abuse. Each of the above is subject to legal and criminal assessment. If bodily injuries result in disorder and impairment of bodily functions for more than seven days, they constitute the basis for initiating criminal proceedings, the purpose of which is to determine the circumstances of the event and the persons who may be its perpetrators. It is worth emphasizing here that in forensic medicine the term «really life-threatening disease» is understood as a condition that may result in the death of a person (it may, but does not have to). Computed tomography in the assessment of the effects of injuries (in the legal and criminal aspect) is of particular importance for the legal classification of the act. Agnieszka P. Jurczyk, Janusz Wendorff, Agata Michalska, Krzysztof Rybka and Jarosław Berent described cases of hypoxic-ischemic encephalopathy as a specific form of head injury complication in the battered child syndrome. The authors emphasize the diagnostic value of computed tomography, especially in therapy, but also emphasize the criminal nature of the uprising [8]. It is also worth noting that CT is a useful diagnostic method in cases of cut and stab injuries to the head (although the latter are rare).[9]. The results of tests performed using digital technology are valuable in medicine, but also constitute the basis for the

reconstruction of the mechanism of injury, which in turn translates into a forensic version. Filip Waśniewski, Bartosz Skulimowski, Joanna Witkiewicz and Małgorzata Wierzbicka described a case of a foreign body (knife) stuck in the external auditory canal [9]. The diagnostics used, among others, computed tomography. The description suggests that it was probably an act of self-harm. If it were assumed (hypothetically) that the injury was the result of the action of a third party, then the result in the form of damage to the ear canal and peripheral facial nerve paralysis (as a consequence of the injury) would be classified as impairment of bodily functions for a period longer than 7 days. There are many similar (in terms of consequences) descriptions of head injuries in the literature on the subject. [10], [11]. [12]. Medical diagnostics in the form of digital technology is highly specialized in the criminal law assessment of events resulting in head injuries. Moreover, in judicial practice (determining the degree of disability resulting from head injuries), digital radiology tests are important evidence for the adjudicating body. The results of research in rental digital technologies are precise and accurate, and this undoubtedly increases their diagnostic value. One can only hope that they will become a permanent part of the practice of forensic medicine and thanatology.

Bibliography :

1. Critchley M .Medical aspects of boxing, particularly from a neurological standpoint.Br Med J. 1957; 1: 357–362
2. Sanz-Reig, J., Lizaur-Utrilla, A., & Verdú-Román, C. (2006). Asociación de fractura de olécranon y fractura de cabeza radial.Revista Española de Cirugía Ortopédica y Traumatología, 50(5), 361–365.
3. Grcević, N. (1988). The concept of inner cerebral trauma.Scandinavian journal of rehabilitation medicine. Supplement, 17, 25–31.
4. Aghayev E., Thali M., Jackowski C., Sonnenschein M., Yen K., Vock P., Dirnhofer R.: Virtopsy – fatal motor vehicle accident with head injury, J. Forensic Sci. 2004, 49(4), 809–813
5. Woźniak K., Urbanik A., Moskała A., Chrzan R., Kamieniecka B. (2008). Konfrontacja klinicznego obrazu TK złamań kości czaszki z wynikami badania sekcyjnego. Archiwum Medycyny Sądowej i Kryminologii, 58(4).
6. Giese A, Koops E, Lohmann F. Westphal M, Püschel K., Head injury by gunshots from blank cartridges. Surg. Neurol. 2002, 57, 268–77
7. Żyluk A., Mazur A., Piotuch B. Czy badanie tomografii komputerowej jest konieczne w każdym przypadku lekkiego urazu głowy? Analiza materiału

klinicznego i radiologicznego grupy chorych; Pom. J. Life Sci. 2015, 61, 2, 158–162

8. Jurczyk A. P., Wendorff J., Michalska A., Rybka K., Berent J. (2010). Encefalopatia niedotlenieniowo -niedokrwienna jako szczególna postać powikłania urazu głowy w zespole dziecka maltretowanego. Arch Med Sąd Krym, 60, 137–145.

9. Waśniewski F., Skulimowski B., Witkiewicz J., Wierzbicka M. (2023). Ciało obce (nóż) w przewodzie słuchowym zewnętrznym-opis przypadku. Advances in Head & Neck Surgery/Postępy w Chirurgii Głowy i Szyi, 22(1).

10. Teresiński, G. (2002). O ustalaniu okoliczności urazu głowy. Archiwum Medycyny Sądowej i Kryminologii, 52(2), 65–83.

11. Żaba C., Żaba Z., Świderski P., Klimberg A., Marcinkowski J. T., Przybylski Z. (2007). Błędy diagnostyczne w urazach głowy. Arch. Med. Sąd. Krym, 57.

12. Wierzchołowski, W. Ocena zależności morfologii obrażeń w obrazach tomografii komputerowej całego ciała od mechanizmu urazu. Poznań 2015. http://www.wbc.poznan.pl/Content/373797/PDF/index.pdf] dostępne 25.11.2023

Irena Malinowska
PhD, University of Vocational Training in Wrocław, Poland

KOMPARATYSTYKA WYBRANYCH KATEGORII OSZUSTW NA RYNKU UBEZPIECZEŃ SPOŁECZNYCH W POLSCE

COMPARATIVE ANALYSIS OF SELECTED CATEGORIES OF FRAUD IN THE SOCIAL SECURITY MARKET IN POLAND

W ostatnich latach przedmiotem szerokiego dyskursu społecznego są kierunki w ubezpieczeniach na życie i zdrowie człowieka. Epidemia COVID-19 uruchomiła wiele procesów, które mogą stanowić wyzwanie dla rynku ubezpieczeniowego w Polsce. Obywatele zaczęli myśleć inaczej o ubezpieczeniu na swoje życie i zdrowie. Natomiast inni zaczęli uciekać się do różnych metod mających na celu wyłudzenie nienależnego świadczenia. W Polsce w roku 2022 wykryto 31 985 przypadków wyłudzeń odszkodowań i świadczeń Ubezpieczeniowych [1]. Jedną z nich jest m. in. celowe spowodowanie wypadku ubezpieczeniowego, które na podstawie umowy ubezpieczenia może być podstawą do wypłacenia odszkodowania. Innym zdarzeniem, które podlega karze jest upozorowanie wypadku, czyli zgłoszenie do towarzystwa zdarzenia, które w rzeczywistości nie miało miejsca. Przykładem może być chociażby zgłoszenie kradzieży samochodu w przypadku, gdy ten został wcześniej sprzedany. Oszuści bardzo często uciekają się także do zawyżenia wartości szkody w mieniu. Z tym do czynienia mamy najczęściej w przypadku przypisywania wcześniej istniejących szkód do skutków konkretnego zdarzenia [2]. Oszustwo ubezpieczeniowe mające na celu wypłatę nienależnego odszkodowania rzekomo poszkodowanej osobie. Najczęściej polega ono na poświadczeniu nieprawdy, co wiąże się ze świadomym działaniem na szkodę ubezpieczyciela. Podstawą wyłudzenia odszkodowania może być chociażby podanie we wniosku ubezpieczeniowym informacji nie mających pokrycia w rzeczywistości czy nadużycie podczas zgłaszania szkody. Na polskim rynku od lat najpopularniejszym i najbardziej dotkliwym pod względem wartościowym przestępstwem jest wyłudzenie świadczenia za zgon osoby ubezpieczonej. Tendencja ta utrzymuje się

praktycznie od początku prowadzenia badań przez PIU. W 2022 roku często wykrywano także przypadki związane z poważnym zachorowaniem, inwalidztwem i przede wszystkim leczeniem szpitalnym. Szczególnie ten ostatni produkt zasługuje na słowo komentarza. Prosta symulacja trudno diagnozowalnych dolegliwości skutkuje kilkudniowym pobytem w szpitalu i świadczeniem na około tysiąc złotych. W roku 2022 ujawniono aż 578 takich przypadków [3]. Obok tego rodzaju przestępstwa wykryto także liczne fraudy dotyczące poważnego zachorowania oraz trwałego inwalidztwa. Od lat najczęstszym przestępstwem są wyłudzenia świadczeń za leczenie szpitalne [4]. Kiedy ma miejsce wyłudzenie odszkodowania? Oszuści ubezpieczeniowi uciekają się do różnych metod mających na celu wyłudzenie nienależnego świadczenia. Jedną z nich jest na przykład celowe spowodowanie wypadku ubezpieczeniowego, które na podstawie umowy ubezpieczenia może być podstawą do wypłacenia odszkodowania. Innym zdarzeniem, które podlega karze jest upozorowanie wypadku, czyli zgłoszenie do towarzystwa zdarzenia, które w rzeczywistości nie miało miejsca. Przykładem może być chociażby zgłoszenie kradzieży samochodu w przypadku, gdy ten został wcześniej sprzedany. Oszuści bardzo często uciekają się także do zawyżenia wartości szkody w mieniu. Z tym do czynienia mamy najczęściej w przypadku przypisywania wcześniej istniejących szkód do skutków konkretnego zdarzenia.

Przestępstwo oszustwa ubezpieczeniowego, zostało uregulowane w Art. 298. – [Wyłudzenie odszkodowania] – Kodeks karny [5]. Zwracając uwagę na oszustwa ubezpieczeniowe, zauważa się, iż fakt związany z tym, że przestępca ubezpieczeniowy jest też klientem danego zakładu ubezpieczeń znacznie utrudnia takim zakładom podejmowanie zdecydowanego działania, które by zwalczało przestępczość ubezpieczeniową z obawą, że może dojść do utracenia klientów. Pozycja ubezpieczeniowa jeśli chodzi o walkę z przestępczością ubezpieczeniową jest bardzo mocno osłabiona przez społeczne przyzwolenie dla tego rodzajów czynów, bądź też z postrzegania niskiej społecznej szkodliwości przestępstwa ubezpieczeniowego. Uogólniając wiedzę o ubezpieczeniach zauważa się, iż rynek ubezpieczeń należy do rynku zaufania publicznego, z tego też względu zjawisko przestępczości ubezpieczeniowej należy do istotnego problemu do odpowiedniego rozwiązania firmom ubezpieczeniowym oraz instytucją, które regulują owy rynek. Obok tak zwanego obywatela, który to w tym samym czasie jest sprawcą wewnętrznym i zewnętrznym przestępstwa ubezpieczeniowego,

tworzy się cała istotna grupa przestępcza jak również sieć powiązań, które wykorzystują stosunek ubezpieczenia w sposób mocno patogenny. Mając na względzie dane statystyczne Polskiej Izby Ubezpieczeń, należy stwierdzić, iż przestępczość ubezpieczeniowa jest to zjawisko trudne do wykrycia i oszacowania. Jej nieznana w pełni skala obejmuje przestępczość nieujawnioną, inaczej mówiąc – ciemną liczbę przestępstw. Są to czyny których nie udało się wykryć. Przypuszczalnie w Polsce i Europie ich szacunkowa wartość przewyższa dziesięciokrotnie dane ujęte w statystykach [6]. W niektórych istotnych przypadkach wykrytych przestępstw dochodzi do pociągania za sobą skutków cywilnoprawnych, a jeszcze inne pociągają dodatkowe skutki prawnokarne. W momencie wybieranie narzędzi do tego, aby zapobiegać jak również zwalczać przestępczość wskazane jest przede wszystkim to, aby porównać koszty związane z zastosowaniem narzędzi z korzyściami, które są możliwe do osiągnięcia.

Bibliografia :

1. Polska Izba Ubezpieczeń, *Analiza przestępczości ubezpieczeniowej*, https://piu.org.pl/wp-content/uploads/2023/09/PIU%20RAPORT%20PRZEST%C4%98PCZO%C5%9A%C4%86%202022.pdf, [dostęp: 24.11.2023].
2. https://beesafe.pl/abc-ubezpieczen/wyludzenie-ubezpieczenia/, [dostęp:24.11.2023].
3. Majewski P., *Analiza danych dotyczących przestępstw ujawnionych w 2017 roku w związku z działalnością zakładów ubezpieczeń – członków Polskiej Izby Ubezpieczeń*, Warszawa 2018, s.6, https://piu.org.pl/wp-content/uploads/2018/11/PIU_analiza_przestepstw-2017.pdf, [dostęp: 24.11.2023].
4. Analiza danych dotyczących przestępstw ubezpieczeniowych ujawnionych w 2022 roku, Warszawa 2023 dr Piotr Majewski Polska Izba Ubezpieczeń Komisja ds. przeciwdziałania przestępczości ubezpieczeniowej, https://piu.org.pl/wp-content/uploads/2023/09/PIU%20RAPORT%20PRZEST%C4%98PCZO%C5%9A%C4%86%202022.pdf, [dostęp: 24.11.2023].
5. Ustawa kodeks karny, (Dz. U.2022.1138), https://sip.lex.pl/akty-prawne/dzu-dziennik-ustaw/kodeks-karny-16798683/art-298, dostęp: 24.11.2023].
6. Analiza danych dotyczących przestępstw ubezpieczeniowych ujawnionych w 2022 roku, Warszawa 2023 dr Piotr Majewski Polska Izba Ubezpieczeń Komisja ds. przeciwdziałania przestępczości ubezpieczeniowej, https://piu.org.pl/wp-content/uploads/2023/09/PIU%20RAPORT%20PRZEST%C4%98PCZO%C5%9A%C4%86%202022.pdf, [dostęp: 24.11.2023].

Галина Авдєєва
кандидатка юридичних наук,
старша наукова співробітниця,
провідна наукова співробітниця НДІ вивчення проблем злочинності
ім. акад. В. В. Сташиса НАПрН України, м. Харків, Україна

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В СУДОВО-ЕКСПЕРТНІЙ ДІЯЛЬНОСТІ

Стрімкий розвиток інформаційних технологій призвів до глобальної інформатизації суспільства та використання в багатьох сферах діяльності людини нових автоматизованих методів накопичення, оброблення і аналізу значних обсягів інформації. Не є виключенням і судова експертиза, в якій сучасні методи і методики дослідження об'єктів передбачають використання цифрових технологій.

Застосування цифрових технологій в роботі судового експерта дозволяє частково або повністю звільнити його від безпосередньої участі в процесах одержання, перетворення, фіксації, накопичення і систематизації інформації під час дослідження матеріальних (матеріалізованих) об'єктів, явищ і процесів. Зокрема, в сучасних умовах цифрові зображення об'єктів слугують основою для створення різного роду автоматизованих інформаційно-довідкових експертних колекцій та криміналістичних обліків [1].

Цифрові технології в судовій експертизі використовуються за такими напрямами: 1) управлінська діяльність та статистичний аналіз роботи експертної установи; 2) інформаційне забезпечення експертної та наукової діяльності; 3) створення різного роду колекцій цифрових копій об'єктів та автоматизованих інформаційно-пошукових систем (АІПС); 4) автоматизація процесів отримання і оброблення результатів фізико-хімічних, біологічних, ґрунтознавчих, металографічних та ін. досліджень за допомогою методів ультрафіолетової та інфрачервоної спектроскопії, мас-спектрометрії, рідинної та газо-рідинної хроматографії, емісійного спектрального аналізу, рентгеноструктурного та атомного спектрального та ін. видів аналізу; 5) порівняльний аналіз зображень, під час вирішення діагностичних та ідентифікаційних експертних завдань щодо підписів, слідів рук, ніг і взуття, слідів інструментів, слідів каналу ствола вогнепальної зброї на снарядах, фотознімків зовнішнього вигляду

людей і предметів та ін. об'єктів судової експертизи; 6) здійснення допоміжних розрахунків за спеціальними формулами і алгоритмами та моделювання певних подій за наявними вихідними даними (моделювання дорожньо-транспортних подій, виникнення і розвитку пожежі, умов і наслідків вибуху та ін.); 7) розроблення програмних комплексів автоматизованого вирішення експертних завдань та формування тексту висновку експерта.

Автоматизація процесів вирішення експертних завдань дозволяє мінімізувати вплив суб'єктивного фактору (недостатня компетентність експерта, його фізичні, психологічні та ін. недоліки) на процеси формування висновку експерта. Тому сучасні засоби судово-балістичного, судово-трасологічного, судово-фізичного, судово-біологічного, судово-медичного та ін. досліджень створюються у вигляді автоматизованих систем, що дозволяють відповідно до певного алгоритму керувати процесом дослідження (в т.ч. роботою певних приладів) за допомогою комп'ютерної техніки, візуально спостерігати за процесом та результатами досліджень, фіксувати отримані результати та роздруковувати їх у вигляді таблиць, схем та ін. Автоматизація експертних досліджень не передбачає усунення експерта від процесу дослідження та формулювання висновку тому, що обрання мети та напрямку дослідження, методики дослідження та варіанту висновку залишається за дослідником.

Прикладами успішного використання АІПС в судово-експертних установах України є такі: «ТАІС» та «Рикошет» – в балістичній експертизі; «Взуття» та «Фара» – в трасологічній експертизі; «Марка» – в експертизі лако-фарбових матеріалів і покриттів; «Проволока» – в експертизі металів і сплавів та ін. Зокрема, за допомогою АІПС «Марка» здійснюється встановлення родової (марки) і групової (в межах марки) належності лако-фарбового покриття. Як ознаки використовуються відомості про якісні і кількісні характеристики елементного складу мінеральної частини всіх марок авто-емалей, які використовуються автозаводами України, РФ, США і країн Європи. Пошук здійснюється шляхом порівняння основних ознак невідомої авто-емалі з ознаками відомих авто-емалей (еталонів), що містяться в банку даних автоматизованої системи.

В дактилоскопічних відділах судово-експертних установ України використовується автоматизована дактилоскопічна ідентифікаційна система «Папілон», яка в автоматизованому режимі дозволяє здійснювати реєстрацію, оброблення, порівняння та ототожнення слідів рук та на-

копичувати дактилоскопічну інформацію. Система вирішує завдання щодо ідентифікації осіб за відбитками пальців і долонь рук, встановлює причетність осіб до раніше скоєних злочинів та об'єднує злочини, вчинені тією ж самою особою.

Ідентифікаційна балістична система «BALSCAN» виробництва компанії Laboratory Imaging s.r.o. (Чехія) спеціалізується на цифровій обробці й порівняльному аналізі зображень [2, С. 11]. Ця система використовується в Україні з 2019 року і на сьогодні включає більше 600 тисяч зображень куль та гільз зі слідами більше 200 тисяч одиниць зброї. Система дозволяє сканувати і порівнювати сліди вогнепальної зброї навіть на деформованих кулях і їх фрагментах з метою ідентифікації конкретного екземпляра вогнепальної зброї.

Останніми роками в межах експертизи відео- та звукозапису розроблено низку новітніх алгоритмізованих методик із встановлення автентичності цифрових сигналограм, які дозволяють виявляти сліди монтажу в цифрових фотознімках, фонограмах та відеограмах. На їх основі створено експериментальні експертно-аналітичні автоматизовані системи «Академія» та «Фрактал», які дозволяють встановлювати автентичність цифрових сигналограм, а також ідентифікувати електронний пристрій, на якому їх зафіксовано.

Дослідження електронних пристроїв, які слугують сховищем загальної і особистої інформації, відомостей щодо різного роду подій і явищ, дій окремих осіб, та ін. відомостей, здійснюється за допомогою сучасних портативних апаратно-програмних комплексів «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC Physical Analyzer». Вони дозволяють виявляти, декодувати і аналізувати цифрові дані, отримані з мобільних телефонів та ін. електронних пристроїв. Такі комплекси дозволяють: вилучати дані без введення графічного ключа, паролю чи PIN-коду з пристроїв Android, Apple та ін.; відновлювати раніше видалену інформацію; дешифрувати зашифровану базу даних історії WhatsApp; вилучати дані додатків, паролі, миттєві повідомлення (зокрема, з месенджерів Viber, WhatsApp та Telegram), контакти, SMS-повідомлення, електронні листи, аудіо- та відеофайли, журнали викликів, інформацію про місцезнаходження телефону та маршрут пересування його власника шляхом аналізу історії використання точок доступу до Wi-Fi-мереж, тощо [3, С. 71].

В судово-експертних установах України використовується АІПС управлінського характеру, яка акумулює, систематизує і аналізує статистичні дані про кількість і характер висновків судових експертиз (катего-

ричних, вірогідних, тощо), про причини розбіжності висновків повторних і первинних експертиз, тощо.

Згідно з Законом України «Про державну реєстрацію геномної інформації людини» [4] в експертній службі МВС України створено автоматизовану систему обліку генетичних ознак людини, за допомогою якої здійснюється ДНК-ідентифікація осіб.

Відповідно до наказу Міністерства Юстиції України від 28.04.2020 №1540/5 «Про затвердження Змін до Положення про Центральну експертно-кваліфікаційну комісію при Міністерстві юстиції України та атестацію судових експертів» в експертних установах МЮ України обладнано автоматизовані робочі місця для складання кваліфікаційного іспиту (тестування) на право проведення експертної діяльності.

На сьогодні триває робота з розроблення комп'ютерних систем щодо вирішення таких завдань: математичне моделювання з метою вирішення експертного завдання щодо можливості здійснення пострілу з вогнепальної зброї без натискання на спусковий гачок; комп'ютерне діагностування і прогнозування характеристик механізмів замикаючих пристроїв; комп'ютерне моделювання дорожньо-транспортної події з метою встановлення швидкості транспортних засобів в момент зіткнення та ін.

Список використаних джерел:

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. Грищенко О. В. Використання балістичного обліку експертної служби мвс україни в розслідуванні кримінальних правопорушень. Автореф. дис. … канд. юрид. наук. Київ, 2021. 23 с. URL: https://elar.naiau.kiev.ua/server/api/core/bitstreams/6ba4f07f-48fb-4bca-bbe5-d0960fb958e6/content

3. Кобець М. В. Апаратно-програмний комплекс «Cellebrite Ufed» як засіб отримання інформації з мобільних терміналів. *Актуальні питання та перспективи використання оперативно-розшукових засобів у розкритті злочинів в умовах воєнного стану* : матеріали міжвідом. наук.-практ. конф. (Київ, 30 берез. 2023 р.). Київ : Нац. акад. внутр. справ, 2023. С. 70–73.

4. Про державну реєстрацію геномної інформації людини : Закон України №2391-IX від 09.07.2022. URL: https://zakon.rada.gov.ua/laws/show/2391–20#Text

Наталія Алексик
студентка 4-го курсу
Навчально-наукового інституту права
Київського національного університету імені Тараса Шевченка,
м. Київ, Україна

ПРОБЛЕМНІ ПИТАННЯ ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС ДОСУДОВОГО РОЗСЛІДУВАННЯ

Враховуючи стрімкий розвиток штучного інтелекту у світі, неможливо оминути увагою актуальність його використання органами досудового розслідування, зокрема під час проведення ними окремих слідчих (розшукових) дій.

Це обумовлено як самою метою використання максимально ефективних методів та способів проведення розслідувань кримінальних правопорушень так і забезпечити швидке, повне та неупереджене розслідування, встановити особу, яка вчинила кримінальне правопорушення та притягти її до відповідальності.

Незважаючи на відносно недавнє «проникнення» штучного інтелекту у діяльність правоохоронних органів України, більшість міжнародних органів правопорядку вже активно використовують штучний інтелект у своїй діяльності.

Зокрема, можна виокремити розроблений вченими Мадридського університету імені Карла III та Кардіфського університету в Уельсі штучний інтелект «VeriPol», який здатен виявляти неправдиві повідомлення, направлені в поліцію, на основі аналізу їх змісту. Система була апробована ще у 2017 році поліцією Іспанії та високо оцінена правоохоронцями [1].

У свою чергу, дослідники зі Стенфордського університету розробили штучний інтелект, який здатен асистувати судді під час обрання стосовно підсудного запобіжного заходу у вигляді тримання під вартою або застави. Даний алгоритм був розроблений на основі 100 тисяч проаналізованих судових справ. Як було зазначено дослідниками, одні судді в 90% випадків дозволяють громадянам виходити під заставу, тоді як інші – тільки в 50%. Програма дає змогу справедливо оцінити ризики і обирати тримання під вартою значно меншій кількості осіб [2].

Зазначені кейси не є одиничними спробами дослідити впровадження штучного інтелекту у правоохоронну діяльність. Однак, слід зауважити, що розвиток та застосування штучного інтелекту випереджає його юридичне урегулювання.

Більшість країн світу розуміють необхідність у закріпленні відповідних норм, що стосуються використання штучного інтелекту у побуті та у правоохоронній діяльності.

Так, Сполучені Штати Америки, Велика Британія та ще 16 країн представили першу міжнародну угоду щодо захисту штучного інтелекту від шахраїв. В даній угоді зазначено, що підприємства, які займаються розробкою та використанням штучного інтелекту, повинні розробляти та впроваджувати його з метою захисту клієнтів та громадськості від можливих зловживань. Угода не має обов'язкової сили та містить загальні рекомендації, але є першою і, вочевидь, не останньою спробою врегулювати питання, які стосуються застосування штучного інтелекту [3].

У 2020 році Європейською Комісією було опубліковано Білу книгу зі штучного інтелекту, в якій були запропоновані варіанти ведення політки для майбутньої нормативної бази Європейського Союзу щодо штучного інтелекту. В основі документу покладена ідея людиноцентризму: в практичному застосуванні, штучний інтелект повинен бути прозорим та зрозумілим його користувачам, а також повністю підконтрольний людині. Окрім того, в даній Книзі зазначається, що остаточне рішення в будь-яких питаннях повинно належати саме людині, а не механізованим алгоритмам [4].

Попри наявні прогресивні приклади інших країн, питання застосування штучного інтелекту під час досудового розслідування повинно бути узгоджено з особливостями національного законодавства України.

Згідно Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні» від 2 грудня 2020 р. №1556-р, де визначені мета, принципи та завдання розвитку технологій штучного інтелекту в Україні як одного з пріоритетних напрямів у сфері науково-технологічних досліджень. Разом з тим, у даній Концепції не зауважується про впровадження штучного інтелекту під час проведення досудового розслідування [5].

Вважається, що необхідність дослідження та поступове впровадження технологій штучного інтелекту під час проведення окремих слідчих (розшукових) дій є особливо актуальним.

У світлі цього, на нашу думку, важливим є окреслити основні положення, що визначатимуть доцільність та правильність застосування штучного інтелекту в роботі органів досудового розслідування та прокурорів. Основна ідея закріплення вказаних положень полягає в тому, що з огляду на особливості кримінального провадження, не у всіх процесуальних діях може використовуватися штучний інтелект. Робота органів досудового розслідування, в переважній більшості, пов'язана з фізичною взаємодією зі сторонами кримінального провадження. Тому використовуючи штучний інтелект під час розслідування кримінальних правопорушень, важливим є дотримання наступних положень:

1. Автоматизоване застосування штучного інтелекту відбувається в операціях з обробки великих обсягів даних, розпізнаванні образів, аналізі текстів.

2. Застосування штучного інтелекту відбувається з обов'язковою повторною перевіркою людиною у складних або потенційно спірних ситуаціях.

3. Обмеження або повна заборона застосування штучного інтелекту відбувається у випадках, коли можлива загроза правам та законним інтересам чи безпеці осіб.

Законодавче закріплення вказаних положень в Кримінальному процесуальному кодексі України [6] має пряме практичне значення та повинно слугувати більш швидкому та ефективному проведенню окремих слідчих (розшукових) дій.

Разом з тим, необхідно зазначити, що застосування штучного інтелекту до або під час проведення допиту (стаття 224 КПК України), пред'явлення особи для впізнання (стаття 228 КПК України), обшуку (стаття 234 КПК України), слідчого експерименту (стаття 240 КПК України) повинно відбуватися виключно як допоміжний інструмент, а його використання чітко визначено в нормах Кримінального процесуального кодексу України.

Законодавча імплементація норм, що стосуються використання штучного інтелекту під час розслідування повинно відбуватися комплексно та планомірно. Доречно також здійснити розробку стандартів та протоколів щодо впровадження застосування штучного інтелекту під час проведення окремих слідчих (розшукових) дій, а також постійно підвищувати кваліфікацію суб'єктів розслідування щодо коректного його використання.

Тому пропонуємо, доповнити Кримінальний процесуальний кодекс України статтею 106–2. Використання штучного інтелекту під час досудового розслідування та викласти її у наступній редакції: «Використання штучного інтелекту під час досудового розслідування повинно відбуватися з обов'язковим дотримання наступних положень:

1. Автоматизоване застосування штучного інтелекту відбувається в операціях з обробки великих обсягів даних, розпізнаванні образів, аналізі текстів.

2. Застосування штучного інтелекту відбувається з обов'язковою повторною перевіркою людиною у складних або потенційно спірних ситуаціях.

3. Обмеження або повна заборона застосування штучного інтелекту відбувається у випадках, коли можлива загроза правам та законним інтересам чи безпеці осіб».

Як підсумок, зазначено, що використання штучного інтелекту під час проведення окремих слідчих (розшукових) дій є досить перспективним напрямком і вимагає більш детального дослідження з боку вітчизняних науковців та практиків. Важливим моментом є визначення основоположних положень застосування штучного інтелекту, з подальшим їх закріпленням в Кримінальному процесуальному кодексі України.

Список використаних джерел:

1. Шрамко С. С. Використання технологій штучного інтелекту у протидії злочинності. Матеріали науково-практичного онлайн-семінару / С. С. Шрамко, О. В. Гальцова. – Харків: \«Право\», 2020. – 112 с.

2. Ковальова О. В. Шляхи удосконалення інформаційного забезпечення досудового розслідування в сучасних реаліях [Електронний ресурс] / О. В. Ковальова. – 2022. – Режим доступу до ресурсу: http://apnl.dnu.in.ua/3_2022/17.pdf.

3. Raphael S. US, Britain, other countries ink agreement to make AI \'secure by design\' [Електронний ресурс] / S. Raphael, B. Diane // Reuters. – 2023. – Режим доступу до ресурсу: https://www.reuters.com/technology/us-britain-other-countries-ink-agreement-make-ai-secure-by-design-2023-11-27/.

4. European Commission. White Paper on Artificial Intelligence: a European approach to excellence and trust [Електронний ресурс] / European Commission. – 2020. – Режим доступу до ресурсу: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

5. Про схвалення Концепції розвитку штучного інтелекту в Україні : Розпорядження Кабінету Міністрів України; Концепція від 02.12.2020 № 1556-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/1556–2020-%D1%80

6. Кримінальний процесуальний кодекс України : Кодекс України; Закон, Кодекс від 13.04.2012 № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/go/4651–17

Василь Білоус
кандидат юридичних наук, доцент, доцент кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

ОСОБЛИВОСТІ ПРОВЕДЕННЯ ЕМПІРИЧНИХ ДОСЛІДЖЕНЬ ПРИ НАПИСАННІ ДИСЕРТАЦІЙ З КРИМІНАЛІСТИКИ В УМОВАХ ВОЄННОГО СТАНУ

Указом Президента України №64/2022 від 24.02.2022 р. «Про введення воєнного стану в Україні» у зв'язку з військовою агресією Російської Федерації проти України з 05 години 30 хвилин 24 лютого 2022 р. в Україні введено воєнний стан, який триває до тепер. Задовго до цього країна-агресор розпочала вчиняти проти України найтяжчі злочини в безпрецедентних для XXI ст. масштабах. Так, станом на 14 грудня 2023 р. лише від початку повномасштабного вторгнення загарбників в Україну Офісом генерального прокурора обліковується вже 116411 злочинів агресії та воєнних злочинів, 113085 з яких становлять порушення законів та звичаїв війни (ст. 438 Кримінального кодексу України), 88 – планування, підготовка або розв'язання та ведення агресивної війни (ст. 437 КК), 67 – пропаганда війни (ст. 436 КК) та 3171 інші; 15803 злочини проти національної безпеки, з яких 3876 – посягання на територіальну цілісність і недоторканість України (ст. 110 КК), 2858 – державна зрада (ст. 111 КК), 6785 – колабораційна діяльність (ст. 111–1 КК), 1011 – пособництво державі-агресору (ст. 111–2 КК), 81 – диверсія (ст. 113 КК) та 1192 інші злочини. Щоденно обсяг вчинених злочинів неухильно зростає.

Припинення цієї злочинної діяльності та унеможливлення її повторення у майбутньому можливе тільки у тому випадку, коли кожен злочинець, що уникнув справедливої відплати на полі бою, буде притягнутий до суворої кримінальної відповідальності. І в цьому сенсі перед силами безпеки України постало не менш відповідальне завдання, ніж перед силами оборони. Адже як жодна армія світу з часів завершення Другої світової війни не зазнавала ворожої навали таких масштабів, так само правоохоронна і судова система жодної сучасної країни не опинялася під тиском такої кількості кримінальних правопорушень.

Кримінальні провадження у цих справах і фіксування перебігу та результатів слідчих (розшукових) дій здійснюють органи досудового розслідування Національної поліції України, Служби безпеки України та Державного бюро розслідувань під процесуальним керівництвом органів прокуратури. Воєнні злочини рф розслідує також Спільна слідча група (JIT) з розслідування воєнних злочинів рф, яка була створена Україною, Литвою та Польщею і розширена до 7 країн за рахунок приєднання Естонії, Латвії, Словаччини та Румунії. Учасниками JIT є також Євроюст та вперше у своїй історії Офіс прокурора Міжнародного кримінального суду. Однак для повного та своєчасного розслідування і цього виявляється не достатньо. Тому питання мобілізації у широкому сенсі всіх можливих резервів є нагальним не тільки для сектору безпеки і оборони України, але й освітньої та наукової криміналістичної спільноти. Адже перемогти ворога, що значно переважає в живій силі та озброєнні, та забезпечити невідворотність покарання цілком реально не числом, а умінням, силою духу і глибиною знань.

Війна – це злочин. А криміналістика – наука, що в усі часи перебуває на передньому краї боротьби зі злочинністю. Відтак, криміналіст, за визначенням, є професійним борцем зі злочинністю. Чи є можливим поєднання воїна-захисника і вченого-криміналіста в одній особі? Досвід та результати добровільної участі всесвітньо відомого швейцарського криміналіста Рудольфа Арчибальда Рейсса у Першій світовій війні та багатьох українських криміналістів у війні сучасній засвідчують риторичність цього запитання. Водночас, чинне законодавство забезпечує широкій науково-педагогічній криміналістичній спільноті й можливість продовжувати виконання конституційного обов'язку із захисту Вітчизни, незалежності та територіальної цілісності України на цивільній науково-практичній ниві. При цьому для кожного вченого, який поринув у вирій науки не заради здобуття вченого ступеню чи наукового звання, справа особистої гідності – забезпечити відповідність результатів здійснюваного наукового дослідження жорстким критеріям актуальності, новизни, високої теоретичної цінності та практичної значущості. Адже для забезпечення торжества невідворотності покарання за вище згадану лавину злочинності потрібні міцні наукові підвалини та розроблені на їх основі криміналістичні рекомендації, ефективність яких не викликає жодних обґрунтованих сумнівів.

Чи створює правовий режим воєнного стану проблеми для емпіричних досліджень з криміналістики? Відповідь на це питання є теж очевидною. Адже, хто хоче зробити, той шукає і/або створює можливості, а хто не хоче, – шукає причини. Історія людства рясніє прикладами народження вагомих наукових здобутків у різних галузях науки і техніки не завдяки, а всупереч тяжким обставинам. І сучасний етап становлення нашої Держави не є тому виключенням. Війна зумовлює потребу в проривних технологіях і водночас створює унікальні можливості для їх відкриття, апробації та впровадження. У тому числі, в усіх без виключення розділах криміналістики (загальній теорії, криміналістичній техніці, тактиці й методиці). При цьому загальні закони розвитку науки – інтеграція і диференціація наукових знань очевидно пояснюють доцільні алгоритми індивідуальних і колективних дій.

Наприклад, з метою пошуку й упровадження в практику Сил безпеки і оборони дієвих засобів опору неспровокованій збройній агресії рф проти України на початку 2014 р. розпочав свою фактичну діяльність Центр криміналістичних інновацій «**i**ntelligen**Trident**». В рамках започаткування окремої теорії аерокосмічної криміналістики першочергово було розроблено методологічні засади й упроваджено в навчальний курс криміналістики та криміналістичну практику аерозйомку із застосуванням безпілотних літальних апаратів мультироторного типу при провадженні різних слідчих (розшукових) дій. Суто криміналістичні навички з пілотування БпЛА, пошуку, виявлення і фіксування криміналістично значущих об'єктів з повітря після початку повномасштабної агресії з урахуванням вимог фізичної та інформаційної безпеки конвертувалися у навички з пошуку, виявлення та фіксування відкритих і замаскованих об'єктів ворога. На вимогу часу вони були швидко розвинуті в напрямку аеророзвідки, цілевказання, коригування вогню артилерії, нанесення вогневого враження, ареромоніторингу поля бою, переміщення цільового спорядження тощо з використанням добре відомих з довоєнних часів технічних засобів. Ці ж самі техніко-криміналістичні засоби універсального призначення повернулися з лінії бойового зіткнення у криміналістичну практику в формі надання органам досудового розслідування технічної допомоги з аерозйомки й аеросканування в кримінальних провадженнях про воєнні злочини. Для масштабування позитивного досвіду невідкладно було засновано загін аерокриміналістів «Сокіл» (Air Criminalists Squad «Falcon») з числа осіб, готових виконувати завдання

в умовах, що потенційно або реально загрожують життю та здоров'ю. У криміналістичну практику та службову діяльність Сил безпеки і оборони України було впроваджено метод сферичного аеропанорамування місцевості. Інноваційні цифрові докази збройної агресії країни-агресора, виготовлені аерокриміналістами у процесуальному статусі спеціалістів (ст. 71 КПК України), візуалізували матеріали значного числа резонансних кримінальних проваджень.

У червні 2022 р. було організовано й успішно проведено на базі НЮУ ім. Я. Мудрого науково-практичну конференцію «Проблематика документального оформлення, визначення шкоди та відшкодування збитків, завданих Україні та її громадянам внаслідок збройної агресії Російської Федерації». На основі реальних даних і апробованих «у полях» рекомендацій підготовлено електронну та друковану версію пам'ятки щодо фото-відеофіксування шкоди, завданої внаслідок збройної агресії Російської Федерації; виготовлено навчально-методичний відеофільм «Фото-відеофікування шкоди, завданої внаслідок збройної агресії Російської Федерації»; розроблено навчальний онлайн-курс «Застосування аерозйомки під час огляду місця події при розслідуванні воєнних злочинів» для Державного бюро розслідувань. Регулярно організовуються вишколи з аерокримінслістики для представників Сил безпеки і оборони (органів досудового розслідування, цивільного захисту, військовослужбовців) та судових експертів, тісна взаємодія з якими збагачує унікальним професійним досвідом і останніми емпіричними даними та дидактичними засобами невпинну науково-дослідну та навчальну діяльність, слугує джерелом переосмислення, модернізації та доукомплектування мобільного комплексу техніко-криміналістичного забезпечення «**i**ntelligen**Trident**», створеного напередодні повномасштабної війни в рамках реалізації проєкту Еразмус+CRIMHUM «Модернізація магістерських програм для майбутніх суддів, прокурорів, слідчих з урахуванням європейських стандартів з прав людини».

Функціональні модулі цього комплексу (аерокриміналістики, індивідуального захисту, виявлення, освітлення, зв'язку, дослідження, вимірювання, фіксування, вилучення, консервування, зберігання, транспортування та презентації доказів) разом з комплектом криміналістичного приладдя «**i**ntelligen**Trident**» були неодноразово успішно апробовані на практиці, регулярно оновлюються і доукоплектовуються сучасним обладнанням. За відгуками обізнаних вчених і практиків, мобільний

комплекс техніко-криміналістичного забезпечення «**i**ntelligen**Trident**» є унікальним і прогресивним за змістом і способом його формування, не тільки в контексті вітчизняних закладів вищої освіти. Діяльність криміналістів Центру криміналістичних інновацій «**i**ntelligen**Trident**» з його застосування під час розслідування воєнних злочинів неодноразово ставала предметом уваги професійних кіл, вітчизняних і зарубіжних засобів масової інформації.

Україна на залишена на одинці зі своєю бідою, люди доброї волі у цілому світі, волонтери і країни-партнери докладають вагомих зусиль до оснащення вітчизняних органів досудового розслідування і експертних установ найсучаснішими техніко-криміналістичними засобами: мобільними ДНК-лабораторіями, лазерними сканерами, безпілотними літальними апаратами з різним корисним навантаженням, роботами-саперами тощо. То ж де, як не в процесі плідної взаємодії з безпосередніми експлуатантами останніх, здобувати та генерувати нові знання? А щоб інтерес до співпраці був обопільним, кожен, хто здійснює наукове дослідження за спеціальністю 12.00.09, має пам'ятати, що апріорі він є достатньо підготовленим для надання дієвої допомоги у кримінальних провадженнях в процесуальному статусі спеціаліста.

Справедливо відзначити, що для досліджень у царині судової балістики та криміналістичної вибухотехніки емпіричний матеріал знаходиться буквально під ногами. І не тільки на полі бою чи деокупованих територіях, але й далеко від лінії бойового зіткнення. Адже ворог щоденно завдає підступних ударів баражуючими боєприпасами, ракетами і авіабомбами по всій території України, артилерійськими снарядами, реактивними ракетами, мінами і FPV-дронами тощо по прикордонню. Крім того, внаслідок збройної агресії рф Україна набула статусу найбільш замінованої країни світу. Для вирішення певних проблемних питань у співпраці з колегами із Служби безпеки України підготовлено практичні порадники «Безпілотні повітряні засоби ураження сил вторгнення російської федерації» і «Застосування безпілотних літальних апаратів під час досудового розслідування».

Українське громадянське суспільство слугує взірцем самоорганізації і пасіонарності, прикладом налагодження ефективних горизонтальних, вертикальних і комбінованих зв'язків для досягнення суспільно корисних цілей. Криміналісти є однією з провідних професійних верств громадянського суспільства і можуть та повинні індивідуально та ко-

лективно створювати осереддя для консолідації конструктивних зусиль провідних представників різних галузей. То ж з метою поглиблення міжгалузевої співпраці з ініціативи Центру криміналістичних інновацій «**i**ntelligen**Trident**» Національним юридичним університетом імені Ярослава Мудрого укладено меморандуми про співпрацю з провідними закладами вищої освіти і судово-експертними установами, а саме з: Національним технічним університетом «Харківський політехнічний інститут» (19 серпня 2021 р.); Харківським науково-дослідним експертно-криміналістичним центром Міністерства внутрішніх справ України (24 травня 2022 р.) і Національним університетом цивільного захисту України (8 грудня 2023 р.). Започатковано здійснення низки науково-дослідних робіт міжгалузевими колективами. Відкритість усіх учасників до нових ідей і готовність до їх активного втілення у життя лежить в основі синергетичного ефекту конструктивної взаємодії.

То ж змарнувати чи сповна скористатися нагодою у скрутні для Батьківщини часи проявити найкращі особистісні якості та всебічно допомогти своєму Народу, розвиваючи криміналістику як науку, навчальну дисципліну і галузь правозастосовної практики, – справа сумління кожного, хто має сміливість іменувати себе криміналістом. Вже в недалекому майбутньому на унікальному практичному досвіді та наукових здобутках українських криміналістів буде навчатися весь цивілізований світ, зацікавлений у непоширенні жахіття, якого зазнала Україна.

Ольга Брендель
завідувач лабораторії Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м. Харків, Україна

СУЧАСНІ МОЖЛИВОСТІ ЗАСТОСУВАННЯ СУДОВОЇ ЕКСПЕРТИЗИ У ПРОТИДІЇ КІБЕРНЕТИЧНІЙ ЗЛОЧИННОСТІ

Використання інформаційних технологій у сучасному розвитку суспільства майже безмежне. Але досягнення науково-технічного прогресу, у тому числі й віртуального простору, використовуються і у нових формах злочинності, особливо у інформатизаційно-коммунікаційній галузі. Про це свідчить зростання кількості судових комп'ютерно-технічних та телекомунікаційних експертиз, що пов'язані із кіберзлочинами. Окрім комп'ютерно-технічних та експертиз електронних комунікацій, в аспекті розслідування кримінальних правопорушень, передбачених розділом XVI Кримінального кодексу України «*Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*» проводяться також експертизи об'єктів інтелектуальної власності та економічні експертизи.

Реалізація кібернетичних загроз пов'язана з використанням відповідних ресурсів інформаційно-телекомунікаційних систем. Щодня у людей та компаній крадуть персональні дані, кошти з рахунків, збирають безліч конфіденційної та комерційної інформації, блокують діяльність підприємств, державних органів, засобів зв'язку тощо. Уразливими для таких загроз є об'єкти, функціонування яких пов'язане з використанням комп'ютерних систем та ресурсів кіберпростору, а саме, банківські рахунки, паролі, інші персональні дані та особиста інформація фізичних осіб, бізнесу та державного сектору. З кожним роком зростає актуальність розслідування кіберзлочинів, оскільки безпосередньо зростає кількість кібератак, що можуть спричинити різні негативні наслідки від загрози національній безпеці, включаючи атаки на комп'ютерні системи державних установ та критичної інфраструктури, до втрати даних та порушення безпеки захисту конфіденційної інформації звичайного інтернет-ко-

ристувача. Наслідки кіберзлочинів також призводять до нанесення значних економічних збитків, які пов'язані із втратою фінансових активів, порушеннями виробничого процесу, розкриттям конфіденційної інформації та шкодою для репутації фізичних та юридичних осіб. Реалізація кібернетичних загроз може призвести до настання таких негативних наслідків як [1]: надзвичайна ситуація; блокування роботи або руйнування стратегічно важливих для економіки та безпеки держави підприємств, систем життєзабезпечення та об'єктів підвищеної небезпеки; блокування роботи державних органів; блокування діяльності органів військового управління, Збройних Сил України в цілому, або втручання в автоматизовані системи керування зброєю; порушення безпечного функціонування банківської або фінансової системи держави; розголошення державної таємниці тощо.

Після повномасштабного вторгнення російської федерації в Україну, в умовах запровадженого військового стану, збільшилась кількість правопорушень, які пов'язані із кібератаками і зламами. В наш час війна в інформаційному просторі може завдати не меншої шкоди, аніж війна на полі бою. Крім того, під час воєнного стану активізуються атаки не лише для завдання шкоди обороноздатності України з боку ворога, а й з боку банальних злочинців, які вирішили скористатися ситуацією перезавантаженості співробітників правоохоронних органів, та за допомогою шахрайських схем з використанням електронних засобів привласнити кошти інших громадян.

Розслідування кіберінцидентів вимагає постійного удосконалення та співпраці між правоохоронними органами та безпосередньо експертними установами. Судова експертиза у розслідуванні кіберінцидентів відіграє дуже важливу роль. Так, експерти в межах комп'ютерно-технічної експертизи та експертизи електронних комунікацій (телекомунікаційної експертизи) відповідно до п.п. 13.2, 14.3 розділу ІІ «Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» [3] вирішують основні питання що допомагають при розслідування кіберінцедентів:

– встановити інформацію, що міститься на певних засобах комп'ютерної техніки;

– виявити інформацію про певні дії користувача (суб'єкта кіберзлочину) на певній комп'ютерній техніці; інформацію про те, чи піддавався

досліджуваний накопичувач певним процедурам з метою знищення інформації;

– встановити факт про те, чи створювалась інформація на певній комп'ютерній техніці або вона була перенесена з іншого носія;

– встановити наявність/відсутність на досліджуваному накопичувачі певного (шкідливого) програмного забезпечення, яке використовувалось суб'єктами кіберзлочину;

– встановити можливість виконання певних дій за допомогою досліджуваного програмного забезпечення;

– встановити характеристики підключення телекомунікаційного засобу до мережі; визначити за допомогою яких програмних засобів здійснювалось підключення до телекомунікаційної мережі; встановити налаштування окремих пристроїв, що використовуються; виявити факт зміни налаштувань, в який час вони здійснені, які їх значення;

– встановити наявності/відсутності факту передачі (отримання) інформації в телекомунікаційній системі та способу здійснення такої передачі;

– встановити ознаки втручання в телекомунікаційну систему; встановити факт доступу до телекомунікаційної системи, використання ресурсів та інформації в телекомунікаційній системі та способу їх використання;

– визначити шляхи маршрутизації даних у телекомунікаційній системі та встановити можливості використання телекомунікаційного засобу (обладнання) для вказаних цілей.

Слід зазначити, що наведений перелік питань не є вичерпним. В свою чергу, експерти у галузях експертизи об'єктів інтелектуальної власності та судових економічних експертиз, відповідно до п. 2.1 розділу ІІІ, п.5.5 розділу V «Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень» [3], вирішують такі завдання: щодо підтвердження документальної обґрунтованості розрахунків економічного показника майнової шкоди (збитки, втрачена вигода), спричиненого суб'єктами кіберзлочинів; встановлення розміру матеріальної шкоди, завданої автору (правовласнику) об'єкта права інтелектуальної власності унаслідок дій суб'єкта кіберзлочину; встановлення ринкової вартості (або іншого виду вартості згідно із законодавством) майнових прав об'єкта права інтелектуальної власності станом на певну дату та багато інших.

Таким чином, висновки судових експертів можуть допомогти слідству встановити низку вагомих обставин щодо правопорушення, що розслідується та сприятимуть своєчасному виявленню, запобіганню і нейтралізації реальних і потенційних загроз важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Стабільна робота державних органів, що переходять на електронний документообіг, стабільна діяльність банківського сектору, залізниці й авіатранспорту, великих підприємств, безпосередньо залежить від стабільності кіберпростору, з яким вони працюють, та базується на комунікації за допомогою електронних засобів зв'язку.

Боротьба з кіберзлочинністю має носити системний характер, виходячи із сучасних ризиків та викликів у кіберпросторі, а інституційне середовище забезпечення кібербезпеки постійно вдосконалюватися. Повне, всебічне та об'єктивне встановлення обставин подій для з'ясування механізму злочину та винуватості учасників, при розслідуванні злочинів, окрім перелічених вище, може забезпечити саме судова експертиза, яка допоможе слідству встановити низку вагомих обставин щодо правопорушення, котре розслідується, наприклад:

– підтвердити факти наявності/відсутності певної інформації, що міститься/містилась на певних засобах комп'ютерної техніки;

– встановити наявності/відсутності факту передачі (отримання) інформації в телекомунікаційній системі та способу здійснення такої передачі та інші ознаки втручання в роботу такої системи;

– підтвердити ступінь причетності кожного із учасників до правопорушення; відношення потенційної жертви а також безпосередньо злочинців до певної події (кіберзлочину), що відбувається;

– встановити дані, за якими можна реконструювати поведінку учасників, ситуацію та умови, в яких відбувається подія;

– виявити інформацію про певні дії користувача (суб'єкта кіберзлочину) на певній комп'ютерній техніці; інформацію про те, чи піддавався досліджуваний накопичувач певним процедурам з метою знищення інформації тощо.

Отримана за допомогою судової комп'ютерно-технічної (або іншої) експертизи інформація створює максимальний потік доказів, які дозволять довести факт події, яка відбулась; викрити певну особу, причетну до скоєння кіберзлочину, або, навпаки, обґрунтувати алібі певній особі; може містити інформацію або відомості, що корисні для слідства про

осіб, які скоїли або причетні до скоєння кіберзлочину; про обставини скоєння такого злочину (або приховування слідів кіберзлочину) тощо.

Список використаних джерел:

1. Шеломенцев В. П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2012. Вип. 1. С. 312–320.

2. Закон України Про основні засади забезпечення кібербезпеки України від 05.10.2017 № 2163-VIII URL : https://kodeksy.com.ua/pro_osnovni_zasadi_zabezpechennya_kiberbezpeki_ukrayini.htm

3. Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень : затв. наказом Мін'юсту України від 08.10.1998 р. No 53/5 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/z0705-98#Text

Ольга Брендель
завідувач лабораторії Національного наукового центру «Інститут судових експертиз ім. Засл. проф. М. С. Бокаріуса» Міністерства юстиції України, м. Харків, Україна

ДОСЛІДЖЕННЯ АВТЕНТИЧНОСТІ ЦИФРОВИХ ВІДЕО- ТА ЗВУКОЗАПИСІВ

В матеріалах досудових та судових проваджень широко використовуються речові докази у вигляді цифрових відео- та звукозаписів. З огляду на відносну легкість створення, модифікування, розповсюдження цифрових записів, логічно що в слідства чи суду виникає питання їх достовірності (автентичності). Вирішення цієї проблеми вимагає постійного оновлення спеціальних експертних знань у галузі дослідження цифрових відео- та звукозаписів.

Найбільш складними та проблемними були і залишаються на теперішній час експертні завдання, пов'язані з технічним дослідженням цифрових відео- та звукозаписів. Визначені раніше тлумачення понять «оригіналу», «копії» у цифрових записах втрачають свою актуальність, оскільки особливість цифрових записів полягає в тому, що цифрова копія (дублікат) може зовсім не відрізнятись від оригіналу запису. Крім того, в експертній практиці все частіше отримати для дослідження первинний, тобто «оригінальний» цифровий запис майже неможливо. На сьогоднішній день в кращій іноземній практиці при дослідження цифрових записів поряд із поняттям «оригінальності» запису використовується поняття «автентифікація», яке в вітчизняній експертній практиці найчастіше використовується у правовому контексті.

Автентифікація – (з грец. αυθεντικός; реальний або істинний) – це процес обґрунтування істинності тверджень щодо походження даних SWGDE/SWGIT Digital & Multimedia Evidence Glossary [1].

Автентичність – (дав.-гр. αὐθεντικός – справжній) – доказ походження, вірогідність. Автентичний – цілком вірогідний, заснований на першоджерелах, такий, що відповідає оригіналу, дійсний, той, що ґрунтується на першоджерелі [2, с. 18]. Синоніми до слова «автентичний»: справжній, непідроблений, істинний, дійсний тощо [3, с. 668–669; 4, с. 2]. Як визначено в SWGDE Best Practices for Forensic Audio [5], експертиза автентич-

ності аудіозапису полягає в тому, щоб визначити, чи є запис відповідним способу, яким він, як стверджується, був записаний.

Термін «автентичний» щодо фонодокументів у сенсі «справжній», «достовірний» широко використовується в англомовному праві, спочатку прийнятий польськими криміналістами в теорії криміналістичного дослідження фонограм [6], використовується американськими експертами [7].

В SWGDE Best Practices for Forensic Audio [5] визначено що експертиза автентичності аудіозапису полягає в тому, щоб визначити, чи є запис відповідним способу, яким він, як стверджується, був записаний.

Якщо розглядати «широке загальне» тлумачення питання щодо встановлення автентичності відео- та звукозапису в цілому, то при відповіді на таке запитання експерт/експерти за допомогою своїх спеціальних знань має/мають вирішити цілий комплекс завдань:

– встановити, чи зафіксовано на записі мовлення зазначених осіб; чи ними вимовляються зазначені слова та фрази; або встановити, чи зафіксовано на записі зображення зазначених осіб в певних обставинах/ місцевості/ умовах тощо;

– чи є запис оригінальним (первинним) або копією;

– чи немає привнесених ознак зміни «достовірності» зафіксованої інформації (монтажу, стирання, дописок тощо);

– чи здійснювалася запис за зазначених умов і з допомогою зазначених відео- та звукозаписуючих пристроїв;

– чи не мають зафіксовані відео- та звукозаписи технічно та ситуаційно не виправданих перерв, випадань сигналу тощо;

– чи дотримано часову послідовність виникнення звукових сигналів на відео- та звукозаписі;

– чи записані сигнали відео- або звукової інформації безпосередньо від їх джерел; чи одночасно фіксувалися сигнали всіх джерел звуку, що відбувалися в момент запису; чи належать сигнали звукової інформації саме тим конкретним джерелам, які зумовлені обставинами запису.

Щодо відеофонограм часто висловлюються сумніви в тому, що запис звуку та зображення проводився одночасно: чи не міг запис звуку проводитися за якихось інших умов та обставин, ніж запис зображення, а згодом обидва сигнали були з'єднані в один файл.

На теперішній час складно створити конкретну методику автентифікації цифрового відео- та звукозапису. Це пов'язано з тим що, кожна експертиза є новим невідомим раніше матеріалом, найчастіше не описаним в літературі або на семінарах. У зв'язку з цим можна лише охарак-

теризувати напрямки виявлення певних ознак для відповідного аналізу та прийняття рішень. Експерт не повинен покладатися тільки на інструментальний аналіз, а повинен використовувати повний набір діагностичних та ідентифікаційних ознак, включаючи аудитивний і лінгвістичний аналіз. Експерт зобов'язаний повністю скласти схему всіх змін, що відбулися з первинним сигналом у вигляді звукової хвилі до отримання її відображення у вигляді аудіофайлу. Якщо навіть за знайденими ознаками, наявними на фонограмі, був сформований порядок всіх змін, для перевірки їх необхідно максимально це підтвердити, роблячи відповідні запити у відповідні органи, звідки надійшов матеріал на дослідження.

По-перше, експерту необхідно ознайомитись, на які конкретні питання намагається отримати відповідь заявник. Необхідно уникнути потенційно сумнівної інформації, яку може надати заявник. Фактори, що мають бути визначені експертом, можуть включати пояснення від замовника, чи є наданий запис оригінальним записом. Якщо ні, необхідно запросити оригінальний запис. В деяких обставинах оригінал, який визначено першим виявом записаного звуку, недоступний або більше не існує. У цих умовах для експертизи може бути використана веріфікована копія оригінального носія.

Перекодовані версії оригінального запису не є оригінальними записами. Декодована копія (у форматі PCM) кодованого оригіналу може містити інформацію корисну для аналізу автентичності, але аналіз формату файлу щодо оригінального формату стає неможливим.

Наступні фактори, які бажано визначити експерту до початку проведення досліджень:

– яка історія зберігання та передачі запису, який вважається оригінальним;

– які дата та час створення запису вважаються дійсними;

– чи є обладнання використане для запису, доступним для дослідження;

– яка система запису, пристрій та носій даних вважаються оригінальними. Необхідно запросити пристрій (певної моделі та серійного номеру), включаючи мікрофони, що використовувались, інші технічні деталі, які можуть бути корисними, наприклад, джерело живлення;

– яким було фізичне місце, де, як стверджується, здійснено запис, та акустичне середовище зазначеного місця;

– які специфічні чи спірні питання стосуються доказу автентичності записів;

– які формати кодування файлів та аудіо підтримуються передбачуваною оригінальною системою запису;

– які формати кодування звуку може використовувати пристрій;

– які формати файлів може створювати / експортувати пристрій;

– який знімний фізичний носій інформації можна використовувати в пристрої;

– які особи, як вважається, були присутніми, коли запис був, як це стверджується, зроблений;

– чи може пристрій передавати або отримувати інформацію електронним шляхом тощо.

Також експертові бажано з'ясувати, чи є у функціональних можливостях пристрою відео- та звукозапису вбудовані функції безпеки. Крім того, з'ясувати, чи потрібні додаткові предмети, щоб виконати повне дослідження, наприклад, обладнання для записування зразків та/або зразки даних чи записів. Можливо, також буде потрібним доступ до заявленого місця запису.

Виходячи з відповідей на вищезазначені питання, експерт визначає, чи доцільне дослідження на «автентифікацію» для того, щоб відповісти на запитання заявника. Якщо ні, експертові необхідно співпрацювати з заявником, щоб змінити запит у міру необхідності.

На підставі повідомлених тверджень, пов'язаних із доказами, може бути корисно перевірити ці твердження як гіпотези під час експертизи. Якщо потрібно протестувати пристрій доказу (наприклад, цифровий пристрій аудіозапису, що не має знімних носіїв, який, як стверджується, записав докази), отримайте дозвіл від необхідної сторони, щоб це зробити, і попередьте, що це тестування ризикує змінити стан цього пристрою.

Експертиза автентичності цифрового аудіо – це процес, який приводить до висновку, що базується на інтерпретації результатів дослідження, і повинен складатися з чітко визначеного набору аналізів. Як і будь-яка наукова експертиза, процес має бути систематичним, об'єктивним і повторюваним. Результати досліджень повинні бути відтворювані. Процес досліджень повинен бути розроблений таким чином, щоб приділяти пильну увагу когнітивній упередженості, її джерелам і впливу, і таким чином, щоб зменшити її наслідки.

Перш ніж дійти певного висновку, експертові необхідно перевірити результати проведених аналізів іншими результатами. Необхідно інтер-

претувати результати з наукової точки зору і надати технічне пояснення в неупередженому стилі.

Висновки щодо автентичності повинні інформативно викладати результати наукових досліджень, і повинні бути ретельно підтверджені проведеними аналізами. Висновки аналізу не повинні бути перебільшеними або применшеними. У висновку дослідження необхідно зазначати про всі факти, встановлені при проведенні аналізів. Жодне наукове дослідження, у тому числі криміналістичне, не забезпечує абсолютної впевненості. Тому висновки досліджень автентичності цифрових відео- та звукозаписів не повинні бути сформульовані в абсолютних термінах. Слід уникати висловів, що передбачають 100% впевненість, якщо мова не йде про відомі зміни або видалення [8]. Як і будь-яка наукова експертиза, процес має бути систематичним, об'єктивним і повторюваним. Результати досліджень повинні бути відтворювані. Процес досліджень повинен бути розроблений таким чином, щоб приділяти пильну увагу когнітивній упередженості, її джерелам і впливу, і таким чином, щоб зменшити її наслідки.

Список використаних джерел :

1. Scientific Working Group on Digital Evidence, «SWGDE Digital & Multimedia Evidence Glossary». URL : https://www.swgde.org/documents/Current%20Documents

2. Словник іншомовних слів : 23 000 слів та термінологічних словосполучень / уклад. Л. П. Пустовіт. Київ : Довіра, 2000. 1018 с.

3. Энциклопедический словарь 2009 URL : http://nnm-club.ru/forum/viewtopic.php?t=222875

4. Абрамов Н. Словарь русских синонимов и сходных по смыслу выражений / Н. Абрамов. Москва : Рус. словари, 1996. 500 с.

5. Scientific Working Group on Digital Evidence, «SWGDE Best Practices for Forensic Audio». URL : https://www.swgde.org/documents/Current%20Documents

6. Проблемы криминалистики. Варшава, 1971. №90. С. 159–183

7. Hollien H. The Acoustics of Crime: The New Science of Forensic Phonetics. Florida, 1994.

8. C. Grigoras, D. Rappaport, and J. Smith, Analytical Framework for Digital Audio Authentication, in AES 46th International Conference, Denver, CO, USA, 2012, 4 p.

Олеся Ващук
доктор юридичних наук, професор, професор кафедри криміналістики, детективної та оперативно-розшукової діяльності Національного університету «Одеська юридична академія», м. Одеса, Україна

ШТУЧНИЙ ІНТЕЛЕКТ ДЛЯ ШВИДКОСТІ ОБРОБКИ ДАНИХ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ

Використання штучного інтелекту (далі – ШІ) для підвищення швидкості обробки даних в контексті розслідування злочинів є однією з ключових переваг цієї технології. Ось як ШІ сприяє ефективності цього процесу:

- обсяги даних. Сучасні розслідування часто залежать від аналізу величезних обсягів даних, включаючи цифрові комунікації, фотографії, відеозаписи, дані з соціальних мереж, фінансові транзакції, та інші. Традиційно, обробка такої кількості інформації вручну є часозатратною та схильною до помилок.

– швидкість аналізу. ШІ може автоматично обробляти та аналізувати дані з неймовірною швидкістю, значно перевищуючи можливості людини. Це означає, що слідчі швидше отримають доступ до важливої інформації, що прискорить розслідування та допоможе оперативніше встановити обставини провадження.

– точність і виявлення закономірностей. Виявлення складних закономірностей та зв'язків в даних, які можуть бути неочевидними для людини, що включає виявлення схованих тенденцій, повторюваних дій, або взаємозв'язків між різними подіями або особами.

– автоматизація рутинних завдань. Багато аспектів обробки даних можуть бути автоматизовані за допомогою ШІ, включаючи сортування, категоризацію та попередній аналіз, що звільняє слідчих від рутинних завдань, дозволяючи їм зосередитись на більш складних аспектах розслідувань.

– обробка природної мови. Технології обробки природної мови (NLP), які є частиною ШІ, дозволяють аналізувати текстові дані, такі як електронні листи, соціальні мережі, звіти, та інші документи, на предмет ключових слів, фраз, або тем, що спрощує пошук релевантної інформації.

– відеоаналіз. ШІ аналізує відеоматеріали, автоматично ідентифікуючи важливі події, осіб, або навіть предмети, що можуть мати значення для розслідування та включає розпізнавання обличь, номерних знаків автомобілів, або навіть аналіз поведінки.

– зменшення часу реакції. Швидка обробка даних за допомогою ШІ значно зменшує час від моменту виявлення злочину до вжиття заходів правоохоронними органами, що може бути критично важливим для запобігання подальшим злочинам або виявлення злочинців.

Отже, використання ШІ при розслідуванні злочинів для підвищення швидкості обробки даних не тільки покращує ефективність і результативність розслідувань, але й дозволяє правоохоронним органам краще використовувати свої ресурси, пришвидшує аналіз даних, та сприяє оперативній ідентифікації та реагуванню на злочинну діяльність.

Використання ШІ для підвищення швидкості обробки даних при розслідуванні злочинів, хоча й пропонує численні переваги, також супроводжується рядом ризиків і потенційних недоліків, які необхідно враховувати:

1. Упередженість алгоритмів. ШІ може ненавмисно включати упередження, які присутні в навчальних даних. Якщо історичні дані, використані для тренування алгоритмів, містять дискримінаційні патерни або упередження, ШІ може відтворювати або навіть посилювати ці упередження, що може призвести до несправедливого ставлення до певних груп населення.

2. Приватність і захист даних. При використанні ШІ для аналізу великих обсягів даних існує ризик порушення приватності осіб, чиї дані обробляються. Це стосується зокрема персональних даних, таких як особисті повідомлення, фінансова інформація, або місцезнаходження.

3. Залежність від технології. Підвищена залежність від ШІ може призвести до зменшення навичок та інтуїції людських слідчих. Існує ризик, що важливі елементи розслідування можуть бути пропущені або неправильно інтерпретовані, якщо слідчі занадто покладаються на автоматизований аналіз.

4. Верифікація і точність даних. ШІ швидко обробляє величезні обсяги даних, але точність таких висновків залежить від якості та актуальності цих даних. Існує ризик, що алгоритми можуть зробити невірні висновки на основі неточних або застарілих даних.

5. Відповідальність за помилки. У випадку помилок або неправильних висновків, виникає питання про відповідальність. Визначення, хто несе відповідальність за помилки ШІ (розробники програмного забезпечення, користувачі, чи самі алгоритми), є складним.

6. Безпекові ризики. Системи, що використовують ШІ, є вразливими до кібератак або зловмисного програмного забезпечення, що може призвести до витоку або маніпуляції з даними та підірвати розслідування.

7. Етичні питання. Використання ШІ в розслідуваннях порушує етичні питання, зокрема щодо втручання в особисте життя, право на конфіденційність та можливість невинуватих осіб бути неправильно ідентифікованими або помилково звинуваченими.

Таким чином, хоча ШІ значно покращує швидкість і обсяг обробки даних у розслідуванні злочинів, важливо враховувати зазначені вище ризики. Впровадження стратегій з управління ризиками, забезпечення прозорості алгоритмів, постійний моніторинг та оцінка етичних аспектів, а також розробка правових рамок значно допоможуть мінімізувати потенційні негативні наслідки використання ШІ. Тому, для мінімізації ризиків і потенційних недоліків, пов'язаних з використанням ШІ для підвищення швидкості обробки даних при розслідуванні злочинів, можна застосувати наступні стратегії:

1. Розробка та впровадження етичних принципів. Створення етичних кодексів для розробки та використання ШІ, які враховують приватність, справедливість, прозорість та відповідальність. Включення етичних перевірок в процес розробки та впровадження ШІ-систем.

2. Забезпечення прозорості та розуміння. Документування та пояснення алгоритмів ШІ, щоб слідчі та інші користувачі могли зрозуміти, як приймаються рішення. Проведення аудитів алгоритмів на предмет упередженості та точності, залучення незалежних експертів.

3. Мінімізація упередженості. Використання різноманітних наборів даних для тренування ШІ, щоб зменшити ризик впровадження упереджень. Постійне оновлення та перевірка моделей ШІ на предмет упередженості та точності.

4. Захист приватності та даних. Застосування методів анонімізації та псевдонімізації даних перед їх обробкою ШІ. Використання технологій захисту даних, таких як шифрування, для забезпечення безпеки інформації.

5. Відповідальність та контроль. Розробка механізмів відповідальності для визначення, хто несе відповідальність за рішення, прийняті за допомогою ШІ. Забезпечення можливості втручання людини, щоб слідчі могли втручатися або переглядати рішення ШІ, коли це необхідно.

6. Освіта та підвищення кваліфікації. Навчання слідчих основам роботи з ШІ, щоб вони могли ефективно використовувати технологію та розуміли її обмеження. Підвищення обізнаності серед правоохоронців щодо потенційних ризиків використання ШІ.

7. Правове регулювання. Розробка законодавчих та інших нормативних актів, які регулюють використання ШІ в правоохоронній діяльності, з особливим акцентом на захист прав людини та приватності.

Отже, застосування цих стратегій може допомогти мінімізувати ризики і забезпечити, що використання ШІ в розслідуванні злочинів відбувається етично, відповідально та законно, при цьому захищаючи права та приватність осіб.

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

РИЗИКИ ПЕРЕВЕДЕННЯ ДОКУМЕНТООБІГУ В ЦАРИНІ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ В ЕЛЕКТРОННУ ФОРМУ: ІДЕНТИФІКАЦІЯ ТА КЕРУВАННЯ

При переведення документообігу в царині кримінального провадження в електронну форму основними видами можливих негативних ефектів є блоки ризиків, пов'язані із: порушення інформаційної безпеки електронного кримінального провадження (витік, втрата, пошкодження інформації, порушення її конфіденційності); створенням перешкод для ефективної реалізації прав учасників процесу (через недостатню цифрову компетентність та цифрову нерівність учасників процесу, приналежність учасників провадження до інклюзивної групи тощо); зайвим дублюванням процесуальних документів через гібридний варіант документообігу, а тож додаткового навантаження на органи кримінальної юстиції, додаткові процесуальні витрати часового ресурсу ; втратою доказової сили документів, виготовлених в електронному вигляді через невизначеність закону щодо оригінальності документу та ін.

Ризик порушення інформаційної безпеки електронного кримінального провадження потребує окремого розгляду. З приводу створенням перешкод для ефективної реалізації прав учасників процесу (через недостатню цифрову компетентність та цифрову нерівність учасників процесу, приналежність учасників провадження до інклюзивної групи тощо),як ми вже зазначали у попередніх публікаціях «пріоритетність цифрового формату має балансувати із гнучкістю щодо конкретного випадку, коли у конкретній правовій ситуації найбільш приємним та доцільним з урахуванням основного вектору цифровізації – прав та свобод учасників процесу буде обрання саме паперового формату документу-

вання. Адже, усі гарантії справедливого судового розгляду поширюються на цифрове судове провадження. Зміни до регламенту у зв'язку з цифровізацією судочинства, у тому числі актів і документів, мають бути внесені з дотриманням права на справедливий суд. Доступ до ефективних засобів судового захисту має надаватись у випадку негативного впливу або шкоди основним правам будь-якого користувача через використання технології»[1].

Оскільки на перехідному гібридному етапі документообігу неминучою є процедура переведення письмових матеріалів кримінального провадження в електронний формат (оцифрування матеріалів провадження)[1] слід окремо брати до уваги можливі негативні правові наслідки, зокрема у вигляді втрати юридичної сили оцифрованих документів, порушення права на захист через об'єктивні складності передання всіх суттєвих рис матеріальних об'єктів –речових доказів та ін. Такі ризики виникають як через технічні причини (недостатня якість, відсутність необхідних пристроїв), так і недостатню правову визначеність, зокрема у частині оригінальності цифрових копій, об'єктивних складнощів оцифрування матеріальних об'єктів.

У контексті зайвого дублювання електронних документів паперовими нагальною є, по-перше, визначеність в законі питань конвертації

[1] На даний час з огляду на неможливість повноцінно використовувати в усіх органах досудового розслідування інформаційну-телекомунікаційну систему «іКейс», а також з огляду на обмеження щодо обсягу процесуальних документів, які можуть бути виготовлені в електронній формі з використанням кваліфікованого електронного підпису, оцифрування є одним з доступних засобів виконання органом досудового розслідування обов'язку збереження в електронній формі копії матеріалів кримінальних проваджень, досудове розслідування в яких здійснюється в умовах воєнного стану (ч. 14 ст. 615 КПК у редакції зі змінами, внесеними згідно із Законом № 2137-IX від 15 березня 2022 р. та Законом № 2201-IX від 14 квітня 2022 р).[2, с. 43–44]. Оцифрування матеріалів кримінального провадження на практиці здійснюється шляхом сканування або фотографування матеріалів кримінального провадження з наступною їх обробкою та збереженням результатів на електронному носії (жорсткі диски, флеш-пам'ять, CD, DVD, хмарні сховища тощо). Дізнавач, слідчий чи прокурор повинен забезпечити збереження також тих матеріалів досудового розслідування, що існують в електронному вигляді, зокрема матеріалів фотозйомки, звукозапису, відеозапису тощо, які містяться на електронних носіях інформації. Збереженню також підлягає інформація про речові докази. Процесуальні документи щодо проведення негласних слідчих (розшукових) дій можуть бути оцифровані лише після їх розсекречування в порядку, визначеному законодавством. Оцифровані матеріали кримінального провадження **повинні відповідати оригіналу та мати достатню якість для подальшої роботи з ними.**

процесуальних документів з однієї форми в іншу (зокрема, у законі мають бути прямо передбачені випадки, коли електронний процесуальний документ повинен бути роздрукований і приєднаний до паперового кримінального провадження тощо), що попереджуватиме невиправдене дублювання електронних процесуальних документів на паперових носіях. По-друге, на стратегічному рівні має бути переглянуто доцільність дублювання фіксації певних процесуальних дій у паперовому протоколі[1].

Питання спрощення процесуальної форми закономірно постало під час воєнного стану та об'єктивувалось у низці законодавчих рішень, пов'язаних, зокрема із спрощенням фіксуванням провадження. Так, відповідно до п. 1 ч. 1 ст. 615 КПК України, в умовах воєнного стану процесуальні дії під час кримінального провадження фіксуються у відповідних документах, а також за допомогою технічних засобів фіксування кримінального провадження, крім випадків, якщо фіксування за допомогою технічних засобів неможливе з технічних причин. За відсутності можливості складання процесуальних документів про хід і результати проведення процесуальних дій фіксація здійснюється доступними технічними засобами з подальшим складанням відповідного протоколу не пізніше сімдесяти двох годин з моменту завершення процесуальних дій . Отже при здійсненні процесуальних дій в умовах воєнного стану за відсутності можливості скласти паперовий протокол вчасно, фіксацію такої дії можна здійснити доступними технічними засобами. Однак в такому разі, все одно складання протоколу поспіль є обов'язковим.

В цьому сенсі підтримуємо позицію Т. О. Лоскутова в тому, що « норми КПК України повинні містити положення щодо спрощеної, альтернативної фіксації особливого порядку кримінального провадження, обумовленого правовим режимом воєнного стану. Спрощення та варіативність фіксування кримінального провадження в умовах воєнного

[1] Зайве дублювання процесуальних документів кримінального провадження спотворює економічну ефективність електронного кримінального провадження. Розумними в цьому сенсі є питання, що ставляться в публікаціях практикуючими правниками: чи виправдані будуть витрати на впровадження ІТСДР в роботу органів досудового розслідування і суду, якщо по суті доведеться дублювати паперові матеріали в електронному вигляді? До прикладу, ст. 224 КПК України передбачає право допитуваної особи викладати власноручно свої покази. З метою забезпечення вказаного права особи, необхідно буде надалі оцифровувати письмовий протокол, що призведе до дублювання матеріалів кримінального провадження та зайвого навантаження на орган досудового розслідування [3]

стану має визначатися балансом між паперовою та технічною формами фіксації. Якщо застосовується фіксація за допомогою технічних засобів, то немає необхідності використовувати паперову форму фіксації у повному обсязі шляхом оформлення складних протоколів [4, с.343]. Дійсно ЦКП вимагає більш рішучих законодавчих рішень, в тому числі щодо визнання «повноцінності» електронного документу (як процесуального рішення чи у певних випадках засобу фіксації процесуальної дії) та навіть стосовно ординарної кримінальної процедури.

На сьогодні, в правовій літературі у контексті фіксації процесуальних дій лунають пропозиції щодо надання цифровим документам самостійного правового значення. Так, наприклад М. Потоцький вважає, що оптимальним підходом щодо використання цифрової інформації під час здійснення затримання в умовах воєнного стану є надання самостійності таким «цифровим доказам» в незалежності від фіксування процесуальної дії у відповідному протоколі. Адже, як зазначає автор – електронна форма фіксування затримання особи за підозрою у вчиненні кримінального правопорушення (в більшості мова йде про відеофіксацію) може сприйматись як універсальний засіб фіксації будь-якого виду затримання. Відеофіксація, яка застосовується в момент затримання є «неупередженим очевидцем» цих подій. В умовах воєнного стану, якщо основні етапи затримання особи фіксують за допомогою технічних засобів (відеофіксації), вбачається, що складання протоколу при такому затриманні виглядає додатковою обтяжуючою роботою. Застосування сучасних інструментів фіксації кримінального процесуального затримання дозволить гарантувати належне забезпечення прав і свобод затримуваних осіб. Однак, в цьому разі, така цифрова інформація повинна мати самостійне доказове значення без додаткового закріплення результатів процесуальної дії у відповідному документі [5, с.182].

В цілому підтримуючи автора, зазначимо, що певному перегляду у контексті ЦКП підлягає й ординарна процедура фіксації процесуальних дій, знаходження балансу між фіксацією «наживо» та додатковим протоколюванням, так щоб уникнути зайвих часових витрат та в той же час не спотворити загрози для прав людини у цьому зрізі спрощення процесуальної форми (презюмування достовірності цифрової фіксації в цьому сенсі має супроводжуватися прозорістю такої фіксації та наявністю нормативних компенсаторних механізмів, що надавали б зокрема можливість оскарження її правдивості для того, щоб особа вважалась

такою, яка « .. не залишається при цьому без засобів захисту, бо може висувати доводи (Falk v Netherlands , 66273/01, 19 жовтня 2004 року)).

В цьому ракурсі виникає й питання щодо доцільності збереження інституту понятих в кримінальному провадженні, котре здебільшого отримує негативну відповідь на сторінках сучасних правових публікацій з огляду на, з одного боку, високу інформативність відеозапису, який надає можливість подальшого відтворення як картини всієї слідчої дії (за умови безперервності ведення запису), з іншого – формальний характер участі понятих у проведенні слідчих дій, що на практиці нерідко зводиться лише до їх присутності та підпису на протоколі, який вони засвідчують [1].

Не намагаючись на цих сторінках надати відповіді з позначених та інших актуальних питань фіксації провадження, лише вкажімо на те, що в межах даного вектору ЦКП очікуваним та потрібними є системні законодавчі рішення (створення правової підстави для переходу в кримінальному провадженні на електронний документообіг), котрі мають бути спрямовані на розумне спрощення кримінальної процесуальної форми з урахуванням позначених правових ризиків.

Список використаних джерел:

1. Глинська Н. В. Правовий аспект запровадження режиму paperless в кримінальному провадженні України. *Питання боротьби зі злочинністю*

[1] Безперечною перевагою відеозапису перед іншими засобами фіксації ходу слідчих (розшукових) дій є можливість одночасної фіксації як візуальної, так і аудіо інформації, що дозволяє відобразити хід слідчої дії у всій повноті, для подальшого аналізу як в цілому, так і окремих, найбільш важливих моментів – законність здійснення процесуальних дій, поведінку учасників процесуальної дії тощо. З іншого боку практиці залучення понятих відомі непоодинокі випадки, коли поняті не були присутніми під час здійснення процесуальних дій, а лише ставили розпис; коли поняті не пересувалися за слідчим під час проведення обшуку у будинку, а лише очікували на одному місці; коли поняті були зацікавленими особами і підтверджували своїми підписами дані, які насправді не відбувалися тощо. Наведена негативна практика знижує ефективність залучення понятих до участі у процесуальних діях та ставить питання щодо вилучення понятих із переліку учасників кримінального провадження. Такі приклади свідчать, що в окремих випадках участь понятих може порушувати права та законні інтереси інших учасників – підозрюваного, потенційного підозрюваного, потерпілого. [6]. Спроба ої відмови від інституту понятих на законодавчому рівні вже мала місце у законопроекті № 6454 «Про внесення змін до Кримінального процесуального кодексу України (щодо дотримання розумних строків кримінального провадження)»

/ редкол.: В. С. Батиргареєва (голов. ред.) та ін. Вип. 45. Харків: Право, 2023. С. 86–96. URL: https://ivpz. kh. ua/wp-content/uploads/2023/10/%D0%97%D0%B1_%D0%9F%D0%B8%D1%82%D0%B0%D0%BD%D0%BD%D1%8F-%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B8_%E2%84%9645_2023_%D0%9F%D0%923. pdf.

2. Гловюк І., Дроздов О., Тетерятник Г., Фоміна Т., Рогальська В., Завтур В. Особливий режим досудового розслідування, судового розгляду в умовах воєнного стану: науково-практичний коментар Розділу IX-1 Кримінального процесуального кодексу України. Видання 2. Електронне видання (Дніпро-Львів-Одеса-Харків, 2022) .

3. Е-кримінальне провадження: бути чи ні?//URL: https://loyer.com.ua/uk/e-kryminalne-provadzhennya-buty-chy-ni/

4. Лоскутов Т. О. Правове регулювання фіксування кримінального провадження в умовах воєнного стану. Електронне наукове видання «Аналітично-порівняльне правознавство». № 1. 2022. с. 343. URL : http://nbuv.gov.ua/UJRN/anpopr_2022_1_64

5. Потоцький М. М. Затримання особи за підозрою у вчиненні кримінального правопорушення. Дисертація на здобуття ступеня вищої освіти доктора філософії за спеціальністю 081 – Право. – Донецький державний університет внутрішніх справ Міністерства внутрішніх справ України, Кропивницький. – 2022.

6. Кисленко, Д. (2021). Захист прав особи в аспекті діджиталізації кримінального провадження. Scientific Notes of Lviv University of Business and Law, 29, 114–119. Retrieved from https://nzlubp.org.ua/index.php/journal/article/view/426.

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

ВИКОРИСТАННЯ ПЕРЕДОВИХ ТЕХНОЛОГІЙ У РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ[1]

Широке використання технологій у нашому повсякденному житті, зростаючий обсяг цифрових даних призвів до розробки нових методів та інструментів для збору, аналізу та збереження цифрових доказів. Серед численних викликів, з якими стикаються це: швидкий розвиток технологій, питання, пов'язані з конфіденційністю та захистом даних, а також складна правова база для збору та аналізу цифрових доказів. Незважаючи на ці виклики, цифрові докази стали важливим інструментом для правоохоронних органів та правової системи, надаючи вирішальні докази у кримінальних справах. Серед основного завдання використання технологій – розслідування кіберзлочину. Дві загальні категорії кіберрозслідувань – це цифрова криміналістика та розвідка з відкритим кодом. Щоб спротити процес прийняття рішень під час судового розгляду шляхом аналізу відповідних доказів і представлення відповідних висновків доцільно використовувати автоматизовану ідентифікацію цифрових доказів і аналіз змішаних даних. Використання технологій у сучасному суспільстві має велике значення при розслідуванні кіберзлочинів. Глобалізація та цифровізація світу породжує нові виклики, нові види кіберзлочинності, вимагає запровадження нових передових технологій. Деякі країни вважають, що штучний інтелект становить потенційно катастрофічну небезпеку для людства, уклавши першу міжнародну декларацію, присвячену цій швидкозростаючій технології [1].

Ще однією важливою тенденцією є конвергенція ШІ з іншими передовими технологіями, такими як Інтернет речей і блокчейн. Сучасні комп'ютерні пристрої створюють великі обсяги інформації та відповіда-

[1] Підготовлено на виконання фундаментальної теми «Теоретико-правові проблеми цифровізації кримінального провадження в Україні», що досліджується в НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України (№ державної реєстрації в УкрІНТЕІ 0121U114401).

ють за пошук, зберігання та обробку інформації протягом нашого повсякденного життя. Нові технології, які швидко розвиваються, можуть ускладнити розслідування, оскільки вони охоплюють застосування в різних галузях, починаючи від сільського господарства, авіації, розваг, електроніки, інформаційних технологій тощо [2].

Використання нових передових технологій, таких як машинне навчання в поєднанні з автоматизацією, ефективно забезпечує суттєву додаткову підтримку в запобіганні кібератакам, швидкому відновленні даних і зменшенні людських помилок [3].

Як зазначає Лаура Нейва, інформаційні технології і великі дані все більше використовуються в правоохоронних підрозділах та мають певні переваги і недоліки у кримінальних розслідуваннях. Переваги пов'язані з можливостями допомагати у протидії організованій і транснаціональній злочинності, просувати кримінальні розслідування та розширювати доступність наборів інформації. Недоліки застосування таких систем обумовлюються відсутністю нормативно-правового регулювання, загрозами правам людини та ймовірності отримання помилкових висновків [4].

Для досягнення очікуваних результатів у розслідуванні кіберзлочинів, потрібно посилити оперативну спроможність правоохоронних та/або судових органів для розслідування кібератак і кіберзлочинів тощо. До них відносяться цифрова криміналістика (наприклад, криміналістика мобільних пристроїв, комп'ютерів, мереж, Інтернету речей і транспортних засобів); візуальний аналіз даних; аналіз шкідливих програм і можливості зворотного проектування; аналіз і арешт криптовалют; ефективне зберігання; обробка; аналіз і передача великих даних; розуміння та використання «розвідки про загрози» та метаданих; і моніторинг Dark Web [5].

Розслідування кіберзлочинів є складною сферою, яка постійно розвивається, оскільки з'являються нові загрози та технології. Як наслідок, слідчі повинні бути в курсі найновіших методів та інструментів, щоб ефективно розслідувати кіберзлочини та пом'якшувати їх. Розслідування кіберзлочинів вимагає використання спеціалізованих інструментів і програмного забезпечення для збору, збереження та аналізу цифрових доказів. Ці інструменти можна використовувати для ідентифікації підозрюваних, відстеження їх діяльності та збору доказів для побудови проти них справ. Програмне забезпечення використовується для відновлення видалених файлів, аналізу метаданих і перевірки журналів мережевого трафіку (EnCase, FTK і Autopsy). Інструменти аналізу мережі використовуються для моніторингу мережевого трафіку, виявлення під-

озрілої активності та відстеження потоку даних (Wireshark, tcpdump і Netscout). Інструменти аналізу шкідливих програм використовуються для аналізу та зворотного проектування зловмисного програмного забезпечення, щоб зрозуміти його поведінку та визначити джерело (IDA Pro, OllyDbg і Binary Ninja). Інструменти відновлення пароля використовуються для відновлення паролів із зашифрованих файлів, баз даних або інших джерел цифрових доказів (Каїн і Авель, Джон Різник і Hashcat). Інструменти аналізу соціальних мереж використовуються для відстеження діяльності підозрюваних і збору доказів із платформ соціальних мереж (Hootsuite, Followerwonk і Mention) [6].

Як зазначається, автоматизація розслідувань на основі машинного навчання може підвищити загальну ефективність процесів розслідування та полегшити забезпечення цілісності інформації під час аналізу справ. Інтернет речей змінив спосіб роботи мобільного зв'язку та систем і забезпечив взаємозв'язок між фізичною та цифровою інфраструктурами. Користувачі обмінюються своїми даними між кількома платформами, і, незважаючи на низку переваг використання додатків IoT, середовища завантажені різними кіберзагрозами, такими як руйнування мереж IoT, DoS-атаки, програми-вимагачі та масовий моніторинг. Збереження та вилучення важливих доказів незалежно від технологічних обмежень і реагування на вимоги розслідування без втручання користувача. Відстеження активності USB-підключення в мережах здійснюється для допомоги в розслідуванні. Криміналістика соціальних медіа набула значного поширення з появою технологій Web 2.0 та Industry 4.0. Різні соціальні медіа-платформи (Instagram, LinkedIn, Facebook і Twitter) піддаються хакерам, а їхні бази даних найбільш вразливі до атак зловмисного програмного забезпечення. Цифрові артефакти можна витягти з часових позначок, URL-адрес, паролів, зображень та інших мобільних програм соціальних мереж для аналізу. Програми Reviver і Mismo використовуються для виявлення подібності міжплатформного двійкового коду та аналізу для виявлення вразливостей у смартфонах і пристроях. Автоматизована ідентифікація цифрових доказів і розширений аналіз змішаних даних використовуються для спрощення процесу прийняття рішень під час судового розгляду шляхом аналізу відповідних доказів і представлення відповідних висновків. Технологія штучного інтелекту використовується для розпізнавання шаблонів у кластерах, а дерева рішень використовуються в поєднанні з нейронними мережами, щоб допомогти з ідентифікацією початкових шаблонів, що є критично важливим для кримінальних

розслідувань. Технології штучного інтелекту використовуються для вивчення образів віртуальних дисків і можуть автоматизувати процеси, провести аналіз для закриття справ у рекордно короткі терміни [7].

Важливість розслідування кіберзлочинів важко переоцінити, оскільки кіберзлочинність продовжує розвиватися та становить значні ризики для підприємств, урядів та окремих осіб у всьому світі, особливо під час повномасштабного вторгнення рф в Україну . Разом з тим, все більше платформ використовують хмарні обчислення, штучний інтелект для аналізу даних та доказів. Водночас доступне розміщення інформації, спрощена та безпечна обробка, зберігання та збереження інформації, а також нові технології і вдосконалення, які допомагають у процесі розслідування кіберзлочинів. Повнота даних і збереження конфіденційності даних повинні бути сумісні і для цього використовуюють нові технології. Поєднання машинного навчання та автоматизації для отримання доказів вищого рівня та безпечного протоколювання кроків розслідування. На сьогодні, застосування таких технологій повинно здійснюватися з дотриманням прав людини, захисту персональної інформації тощо.

Список використаних джерел :

1. Дунаєва Т. Є. Окремі аспекти використання цифрових технологій при розслідування кіберзлочинів. *Актуальні питання у сучасній науці. Серія «Право».* Київ, 2023. №12 (18). С. 502–512.
2. Barracuda Network. URL: https://www.barracuda.com/.
3. Advancements in Cybercrime Investigation and Digital Forensics. Ed. by A. Harisha, Amarnath Mishra, Chandra Singh. Routledge, 2024. URL: https://www.routledge.com/Advancements-in-Cybercrime-Investigation-and-Digital-Forensics/Harisha-Mishra-Singh/p/book/9781774913031#
4. Neiva, L. (2023). Big Data technologies in criminal investigations: The frames of the members of Judiciary Police in Portugal. Criminology & Criminal Justice, Vol. 0(0). URL: https://doi.org/10.1177/17488958231192767.
5. Staniforth, A. Cybercrime innovation: Transforming digital investigation tools, techniques, and technologies. *Policing Insight.* 13th August 2022. Retrieved from: https://policinginsight.com/feature/analysis/cybercrime-innovation-transforming-digital-investigation-tools-techniques-and-technologies/.
6. Cybercrime Investigation Tools and Techniques You Must Know! URL: https://cybertalents.com/blog/cyber-crime-investigation.
7. Overill, R. (2012, January). Digital quantum forensics: Future challenges and prospects. Retrieved from ResearchGate: http://dx.doi.org/10.1504/IJITCC.2012.050410.

Володимир Журавель
доктор юридичних наук, професор, академік НАПрН України,
президент Національної академії правових наук України,
м. Харків, Україна

ПРОГРАМУВАННЯ ЯК ЗАСІБ ПІДВИЩЕННЯ ЯКОСТІ РОЗСЛІДУВАННЯ

Намагання науковців надати практиці передові рекомендації щодо підвищення якості слідчої діяльності, і такого її аспекту як планування, закономірно привернули їх увагу до розроблення і запровадження програм розслідування. При цьому гносеологічним підґрунтям для реалізації ідеї програмування процесу розслідування слід вважати наявність багатоваріантного підходу до розв'язання пізнавальних та управлінських завдань. Відомо, що завдання, в тому числі й в сфері кримінального судочинства, можуть вирішуватись евристичним (творчим) і алгоритмічним шляхами. Перші завдання за своєю природою і змістом є більш ускладненими, другі — простішими і в їх розв'язанні простежується елемент повторюваності. У зв'язку з цим вагомого значення набуває виділення в науці криміналістиці таких категорій як типова слідча ситуація, типова версія, типове тактичне завдання і рішення. Функціональною основою можливості програмування розслідування є запровадження в криміналістичну науку кібернетичних підходів, зокрема щодо розроблення схем типових рішень і типізованих дій слідчого в деяких типових слідчих ситуацій з використанням персональної комп'ютерної техніки.

Програмування слід розглядати як теоретико-прикладну діяльність учених-криміналістів спрямовану на створення відповідних програм розслідування злочинів як певної сукупності приписів, тобто жорстко детермінованих систем дій, а також правил рекомендаційного характеру, призначених для ефективного управління слідчою ситуацією під час розслідування злочинів окремих груп, видів і підвидів. Програми як правило надаються у відповідному схематичному вигляді, вони мають більш узагальнену структуру в порівнянні з алгоритмами і за своїм змістом менш формалізовані, а ніж останні. Водночас, зведення програмування розслідування до суто організаційно-управлінських заходів є помилковим і неадекватним тій ідеї, яку визначально проголошено. Як видається, більш продуктивною є позиція за якою, програму слід розглядати як са-

мостійний елемент структури окремої криміналістичної методики, котрий знаходиться у взаємодії з іншими структурними елементами, зокрема з типовими слідчими ситуаціями та типовими версіями, які, в свою чергу, виступають підґрунтям для формування програм розслідування. На нашу думку, і описову і алгоритмічну форми викладення методичних криміналістичних порад потрібно розглядати як необхідні наукові засоби криміналістики, що функціонують паралельно. Ці форми не тільки не суперечать, а навпаки доповнюють одна одну, забезпечуючи викладення методичних порад стосовно оптимального, найбільш ефективного підходу до організації розкриття та розслідування певних злочинних проявів.

Більше того, форма викладення необхідних методичних рекомендацій свідчить про ступінь сформованості самих окремих криміналістичних методик, рівень їх практичної реалізації. На сьогодні криміналістичні методики мають головним чином описовий вигляд. Ця форма знаходить своє відображення головним чином у підручниках з криміналістики і розрахована на студентську аудиторію, а саме на осіб які тільки розпочинають формування уявлень щодо даної галузі знань. Ось чому в такого роду методиках поряд з суто практичними рекомендаціями можна зустріти і деякі пояснення тих чи інших теоретичних концепцій, які дійсно збільшують обсяг викладеного матеріалу. Але в даному разі вони є виправданими і мають своє гносеологічне навантаження. Інша річ, коли йдеться про рекомендації для слідчих, дізнавачів, які повинні бути більш лаконічними і доступними для сприйняття і застосування, а тому подані у вигляді певних програм розслідування в типових ситуаціях. Результати побудови програм розслідування доцільно відображати в науково-практичних виданнях для слідчих, дізнавачів, оскільки саме вони є головними споживачами такого роду наукового продукту. При цьому, самі програми до певної міри базуються на інформації, яку викладено в описовій криміналістичній методиці, а саму «книжкову» методику можна вважати першим і необхідним кроком щодо їх формування.

Разом із тим, треба пам’ятати і враховувати, що криміналістична методика в будь-якій формі її викладення завжди буде зберігати певний рівень абстракції, оскільки не можливо «без залишку» типізувати всі ймовірні версії та слідчі ситуації і до них запропонувати відповідні програми розслідування. Саме в силу відповідного рівня абстракції криміналістична методика не може претендувати на повну «технологічність»,

тобто стовідсотково формалізувати розв'язання завдань розслідування, а тому обов'язково вагомим залишається творчий (евристичний) підхід.

Виходячи з того, що розслідування це завжди складний пізнавальний процес, реалізація якого здійснюється головним чином евристичним (творчим) шляхом, де алгоритмічний виконує лише допоміжну роль, то й програмування є складовою частиною, підґрунтям планування. Слідчий, спираючись на розроблені в науці програми дій, у відповідності до ситуації, що виникла, і враховуючи реальні можливості, обирає оптимальний шлях здійснення процесу доказування. За таких обставин значення програмування, як засобу доведення методичних рекомендацій до слідчого, полягає в тому, що воно надає йому можливості в тих випадках, коли є готові оптимальні рішення не займатися їх винаходом, а брати і використовувати вже готові. При цьому обов'язково треба враховувати, що методичні приписи, котрі містяться в програмі це лише передумови до діяльності, в той же час успіх розслідування досягається не стільки ступенем їх опанування, скільки професійним використанням в умовах конкретної ситуації. А раз так, то застосування програм розслідування вимагають від слідчого значних інтелектуальних зусиль. Програмування розслідування не повинно позбавляти слідчого можливості пошуку евристичних рішень, навпаки програма повинна стимулювати його ініціативу щодо відшукання нового оригінального рішення навіть й такого, яке не передбачено її розробниками.

Отже, програми розслідування ні в якому разі не призначені для того щоб заміняти індивідуальність, професіоналізм, стиль мислення слідчого, тим більше, що при всьому бажанні нестандартне рішення в розслідуванні злочинів запрограмувати не можливо. Їх метою є стимулювання ділової активності слідчого. Саме вони в різноманітних типових слідчих ситуаціях здатні забезпечити швидкість прийняття рішення з урахуванням усіх без виключення рекомендацій криміналістики і вимог чинного законодавства. За їх допомогою розумова діяльність слідчого істотно полегшується, не втрачаючи при цьому своїх творчих засад. При цьому самі програми виступають своєрідним способом концентрації криміналістичних знань, акумулятором узагальненого досвіду слідчої діяльності, підвищують її ефективність, перетворюючи на програмнокеровану та більш контрольовану при розв'язанні однотипних завдань розслідування, створюючи відповідні умови до економії інтелектуального труда слідчого, його автоматизації там, де це можливо і необхідно.

Крім того, принципи та ідеї програмування набувають особливого значення ще й тому, що виникає об'єктивна можливість їх реалізації засобами комп'ютерної техніки, оскільки на сьогодні кожний слідчий має в користуванні персональний комп'ютер. Зазначене зумовлює ще один напрямок спільних досліджень криміналістів і математиків-програмістів стосовно формалізації існуючих і створення нових програм розслідування, які б мали вигляд довідково-консультаційного посібника для слідчих. Звернення до цих джерел й могло б стати тим необхідним засобом оперативного одержання управляючої інформації, який реально сприятиме підвищенню рівня ефективності пізнавальної та організаційної діяльності слідчого.

Маріетта Капустіна
кандидатка юридичних наук, доцентка,
доцентка кафедри криміналістики Національного юридичного
університету імені Ярослава Мудрого, м. Харків, Україна

МОЖЛИВОСТІ СУЧАСНИХ ІНФОРМАЦІЙНИХ СИСТЕМ У СУДОВОМУ ПРОВАДЖЕННІ

Серед криміналістичних засобів інформаційного забезпечення найпоширенішими є інформаційні системи під якими прийнято розуміти організаційно впорядковану сукупність масивів інформації про певні об'єкти та інформаційні технології, у тому числі засоби сучасної комп'ютерної техніки, програмного забезпечення та мереж зв'язку, що забезпечують процеси введення, опрацювання та видачі інформації користувачеві [1, с. 59].

Наряду з інформаційними системами, які використовуються на стадії досудового розслідування, окреме місце посідають та менш важливого значення набувають системи, що використовуються у судовому провадженні.

Сучасними інформаційними системами, що використовуються на сьогодні в судовому провадженні є:

1) єдина судова інформаційно-телекомунікаційна система, яка являє собою сукупність інформаційних та телекомунікаційних підсистем (модулів), які забезпечують автоматизацію визначених законодавством процесів діяльності судів, органів та установ в системі правосуддя, включаючи документообіг, автоматизований розподіл справ, обмін документами між судом та учасниками судового процесу, фіксування судового процесу та участь учасників судового процесу у судовому засіданні в режимі відеоконференції, складання оперативної та аналітичної звітності, надання інформаційної допомоги суддям, а також автоматизацію процесів, які забезпечують фінансові, майнові, організаційні, кадрові, інформаційно-телекомунікаційні та інші потреби користувачів цієї системи. В цю систему входять наступні підсистеми (модулі): «Електронний кабінет», «Електронний суд» та підсистеми відеоконференцзв'язку. До основних можливостей Єдиної судової інформаційно-телекомунікаційної системи відносять: ведення електронного діловодства в межах та між відповідними органами та установами, що здійснюють реєстрацію надісланих й отриманих електронних документів та етапів їх руху; централізоване

надійне зберігання в єдиній базі судових документів та інформації; безпечне зберігання, автоматичний аналіз і статистична обробка інформації; зберігання судових та інших документів в електронних архівах; здійснення обміну документами та інформацією в електронній формі між судами, іншими установами, учасниками судового процесу; здійснення відеоконференцзв'язку між учасниками судового процесу у режимі реального часу; здійснення автоматизації основних аналітичних показників діяльності суду в режимі реального часу; здійснення віддаленого доступу користувачам системи до всієї інформації, що зберігається в електронній формі, з урахуванням диференційованих прав доступу; визначення суддів (доповідачів) для розгляду окремих справ у порядку, встановленому процесуальним законом; визначення присяжних для судового розгляду з числа зазначених у списку присяжних; здійснення розподілу справ у Вищій раді юстиції, Вищій кваліфікаційній комісії суддів України та її установах; здійснення відео- та аудіофіксації судових засідань, засідань Вищої кваліфікаційної комісії суддів України, Вищої ради правосуддя; ведення Єдиного державного реєстру судових рішень; ведення Єдиного державного реєстру виконавчих документів тощо [2].

2) автоматизована система документообігу суду, яка являє собою сукупність комп'ютерних програм і відповідних програмно-апаратних комплексів судів та Державної судової адміністрації України, що забезпечує функціонування документообігу суду, обіг інформації між судами різних інстанцій та спеціалізацій, передачу інформації до центральних баз даних залежно від спеціалізації судів, захист від несанкціонованого доступу тощо. До основних можливостей автоматизованої системи документообігу суду відносять: реєстрація та розсилка вхідних повідомлень, реєстрація вихідних повідомлень та внутрішніх судових документів; здійснення розподілу судових справ між суддями; здійснення фіксації етапів проходження документів до їх передачі в електронний архів та передачі судових справ з однієї судової інстанції до іншої; реєстрація процесуальних дій і документів у судовому провадженні; здійснення контролю за дотриманням процесуальних строків розгляду судової справи; використання ЕЦП для підписання оригіналу електронного документа суду; здійснення оперативного пошуку судових справ та документів за їх реквізитами; здійснення індексації документів; виготовлення копій судових рішень та виконавчих документів на основі даних, що містяться в автоматизованій системі, у тому числі передача оригіналів електронних судових рішень засобами електронного зв'язку; зберігання текстів судо-

вих рішень та інших документів, сформованих автоматизованою системою; відправлення оригіналів електронного судового рішення до Єдиного державного реєстру судових рішень; надання інформації про стан судового провадження в установленому законодавством порядку; створення та автоматичне формування статистичних даних, зведень та аналітичних показників,отриманих на підставі внесеної до автоматизованої системи інформації; здійснення підготовки судових звітів про стан судового розгляду; здійснення передачі судових справ в електронний архів; надсилання оригіналів електронних документів суду до державних реєстрів та інформаційних систем інших державних органів і установ [3].

Перевагами зазначених інформаційних систем є: підвищення ефективності обміну інформацією між користувачами та учасниками судового провадження; суттєве зменшення затрат часу та ресурсів у судовому провадженні; ефективна координація учасників кримінального процесу; наявність в реальному часі актуальної та об'єктивної інформації про стан судового провадження; усунення можливостей фальсифікації матеріалів та зменшення корупційних ризиків.

Отже, запровадження та функціонування інформаційних систем у судовому провадженні сприяє автоматизації роботи судів, органів й установ в системі правосуддя та правопорядку. Оскільки, автоматизація як процес загального якісного поліпшення технології обробки інформації істотно підвищує оперативність і ефективність інформаційних систем. Крім того, важливого значення набуває процес автоматизованої взаємодії цих систем з іншими автоматизованими, інформаційними, інформаційно-телекомунікаційними системами органів та установ у системі правосуддя та органів кримінальної юстиції.

Список використаних джерел :

1. Бірюков В. В. Теоретичні основи інформаційно-довідкового забезпечення розслідування злочинів: монографія. Луганськ: РВВ ЛДУВС, 2009. 664 с.

2. Положення про порядок функціонування окремих підсистем (модулів) Єдиної судової інформаційно-телекомунікаційної системи затв. Рішенням Вищої ради правосуддя 17 серпня 2021 року №1845/0/15-21URL: https://zakon.rada.gov.ua/rada/show/v1845910-21#Text

3. Положення про автоматизовану систему документообігу суду затв. Рішенням Ради суддів України 02.04.2015 №25 URL: https://zakon.rada.gov.ua/rada/show/v0025414-15#Text

Артем Коваленко
кандидат юридичних наук, доцент,
старший науковий співробітник науково-дослідної лабораторії
публічної безпеки громад факультету № 2 Донецького державного
університету внутрішніх справ, м. Кропивницький, Україна

МЕТАДАНІ ЯК ДЖЕРЕЛО КРИМІНАЛІСТИЧНО ЗНАЧУЩОЇ ІНФОРМАЦІЇ

Унаслідок суцільної комп'ютеризації сучасного життя, практично будь-яка діяльність людини знаходить своє відображення у так званому «цифровому світі» – в дописах у соціальних мережах, повідомленнях у месенджерах, цифрових фото-, аудіо- та відеофайлах, системних даних у пам'яті смартфона, розумного холодильника або wifi-роутера, на сервері провайдера інтернет послуг тощо. Утворені таким чином комп'ютерні дані можуть, зокрема, містити відомості про обставини вчинених кримінальних правопорушень, і через це ставати предметом інтересу правоохоронців. Водночас варто зазначити що, комп'ютерні технології розвиваються та видозмінюються із кожним днем, а тому практики постійно потребують актуальних та своєчасних рекомендацій щодо застосування кримінальних процесуальних та криміналістичних засобів опрацювання комп'ютерних даних.

Основним процесуальним засобом збирання й дослідження подібної інформації є передбачений ч. 1, 2 ст. 237 КПК України огляд комп'ютерних даних. У межах проведення згаданої слідчої (розшукової) дії, об'єктом дослідження виступають комп'ютерні дані, котрі можна визначити як інформацію, що міститься в запам'ятовуючому пристрої електронно-обчислювального приладу у форматі, придатному для обробки, пересилання й інтерпретування обчислювальними пристроями комп'ютерної техніки. У разі, якщо такі дані були створені або змінені правопорушником чи іншими особами у зв'язку з учиненням кримінального правопорушення, їх варто вважати електронними (цифровими) слідами кримінального правопорушення [1, с. 114]. При цьому, у результаті проведення даної С(Р)Д, у її протоколі має бути зафіксовано зміст оглянутих даних (або за формулюванням абз. 2 ч. 2 ст. 237 КПК України, інформацію, яку вони містять) у формі, придатній для сприйняття людиною.

Як правило, комп'ютерні дані запаковані у контейнери (файли), що містять у зашифрованому вигляді структуровану відповідно до вимог певного формату інформацію щодо роботи електронно-обчислювального приладу та операцій користувачів з таким приладом. Згадані дані можна назвати основними, і вони підлягають першочерговому дослідженню та фіксуванню під час проведення огляду комп'ютерних даних.

Водночас комп'ютерні системи створюють та зберігають також і додаткову інформацію, що характеризує основні дані (файл «контейнер» даних або каталог «папку» індексації даних). Таку інформацію прийнято називати метаданими (від давньогрецького μετά – після, за межами та англійського data – дані). Подібні дані також здатні нести криміналістично значущі відомості, а відтак мають виявлятися та досліджуватися уповноваженими особами під час проведення огляду комп'ютерних даних.

Перелік та зміст метаданих залежить від формату основних даних, операційної системи, типу файлу та програмного забезпечення, з яким даний файл асоційовано тощо. В операційних системах Microsoft Windows метадані файлу можна відобразити на екрані за кліком по ньому правою кнопкою миші та вибором опції «Властивості». Базовими метаданими є розмір файлу (міра кількості даних, вихідною одиницею є байт), назва, розширення назви (наприклад *.doc, *.exe), назва асоційованого програмного забезпечення за замовченням, каталог розташування, час створення, час останнього редагування, час останнього відкриття, кількість редакцій, найменування користувача, який створив чи останнім редагував файл тощо.

Базові метадані притаманні більшості форматів файлів та підлягають обов'язковому дослідженню й фіксуванню під час проведення огляду комп'ютерних даних. Зокрема зазначення у протоколі назви, розміру та каталогу розміщення кожного файлу дозволяють їх належними чином ідентифікувати та індивідуально позначити. Відомості про час створення й редагування певного файлу та найменування користувача, котрий його створив чи редагував, є основою для висунення версій щодо хронології та обставин утворення основних комп'ютерних даних. Крім того, велике значення має розширення назви і відповідний формат кожного дослідженого файлу, адже така інформація дозволяє підібрати відповідне асоційоване програмне забезпечення, що дозволить вивчити основний вміст таких даних.

В окремих випадках дослідженню й фіксуванню також підлягають специфічні метадані, що притаманні певним різновидам комп'ютерних файлів. Так, доказове значення можуть мати метадані характерні для текстових файлів, зображень, аудіо- та відеофайлів, виконуваних файлів тощо.

Зокрема, для текстових документів у метаданих, як правило, додатково зберігаються відомості про кількість сторінок, слів, знаків, строк, абзаців, відповідність шаблону, наявність посилань, мову документа, час останнього друку тощо.

Для зображень притаманні такі специфічні метадані як роздільна здатність, глибина кольору, кольоровий простір (наприклад RGB, sRGB, DCI-P3 та ін.), ступінь стиснення тощо. Крім того, для графічних файлів певних форматів (зокрема фотознімків) розроблено спеціальний стандарт опису додаткової інформації Exif (Exchangeable image file format). Метадані, створені відповідно до згаданого стандарту, можуть містити відомості про модель та виготовлювача камери, значення діафрагми, витримки, швидкості ISO, експокорекції, фокусної відстані та про геолокацію місця виконання знімку (за умови що відповідна камера обладнана системами геопозиціювання, наприклад GPS) тощо. Перелічені exif-дані можуть бути досліджені як з використанням засобів стандартної програми-провідника операційної системи, так за допомогою специфічного програмного забезпечення (ExifTool, Exif Viever та ін).

Під час дослідження цифрових фотознімків рекомендується в обов'язковому порядку перевіряти наявність exif-даних та фіксувати у протоколі основні відомості, що вони несуть. Особливо цінною у даному контексті є інформація про місце (gps-координати) та час зйомки, а також камеру (або інший пристрій), за допомогою якого було виконано фотознімок. Згадані дані можуть дозволити прив'язати основний вміст файлу-зображення до конкретної місцевості, часових меж та осіб, що могли виконати знімок. Вміст exif-даних також є одним із об'єктів дослідження під час проведення судових фототехнічних експертиз.

Для мультимедійних аудіо-, відеофайлів притаманні такі специфічні метадані як довжина, роздільна здатність, швидкість передачі даних, частота кадрів, бітова частота передачі, кількість каналів, частота дискретизації звуку та інше. В окремих випадках згадані метадані також можуть нести цінну для органів досудового розслідування та суду інформацію.

Таким чином, у результаті експлуатації комп'ютерної техніки утворюються комп'ютерні дані, котрі, зокрема, можуть нести відомості про обставини кримінальних правопорушень. За загальним правилом подібні дані містять зашифровану та структуровану відповідно до вимог певного формату інформацію про роботу електронно-обчислювального приладу та операції користувачів з таким приладом. Згадана інформація є основними даними, або основним вмістом комп'ютерних даних, і підлягає обов'язковому фіксуванню під час їх дослідження. Водночас комп'ютерні системи також створюють і зберігають так звані метадані – додаткову інформацію, що характеризує основні дані. Перелік та зміст метаданих залежить від формату основних даних, операційної системи, типу файлу тощо. Базовими для більшості форматів файлів є відомості про розмір файлу, назву, розширення назви, асоційоване програмне забезпечення, каталог розташування, час створення, останнього редагування та відкриття, найменування користувача, який створив чи останнім редагував файл тощо. Указана інформація дозволяє ідентифікувати та індивідуально позначити у протоколі кожен досліджений файл, а також висунути версії щодо хронології та обставин створення досліджених комп'ютерних даних. Крім того, існують специфічні метадані, притаманні певним різновидам комп'ютерних файлів. У певних випадках криміналістичне значення можуть мати метадані характерні для текстових файлів, зображень, аудіо- та відеофайлів, виконуваних файлів тощо.

Список використаних джерел :

1. Криміналістика: криміналістична техніка : навч. посіб. / Р. Л. Степанюк, В. О. Гусєва, В. В. Кікінчук та ін. ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2023. 388 с.

Олексій Кожевніков
завідувач відділу досліджень
у сфері інформаційних технологій
Харківського науково-дослідного експертно –
криміналістичного центру МВС України, м. Харків, Україна

ПИТАННЯ СУТНОСТІ ТА ФОРМ ВИКОРИСТАННЯ СПЕЦІАЛЬНХ ЗНАНЬ НА ОКРЕМИХ ЕТАПАХ OSINT РОЗСЛІДУВАНЬ

Суттєвим чинником, що впливає на ефективне розслідування кримінальних правопорушень в умовах воєнного стану, є своєчасне та якісне інформаційно-аналітичне забезпечення діяльності суб'єктів розслідування. Одним з перспективних джерел для отримання корисної та значущої (для кримінального провадження) інформації можна розглядати технологію отримання даних під назвою Open source intelligence (OSINT) – розвідка на основі аналізу відкритих джерел інформації. Базова ідея OSINT – цілеспрямований збір інформації щодо об'єкта зацікавленості з метою подальшої обробки та різновекторного контент-аналізу отриманих даних (створення «портрету» особи, виявлення неочевидних фактів чи зв'язків, прогноз її поведінки тощо) [1].

Процес пошуку та добування даних з використанням наведеної технології не є шаблонним, проте в ньому можна виділити окремі умовні етапи: підготовчі дії, збирання даних, порівняння даних, оцінка та обробка, аналіз, підготовка висновків.

Збирання інформації з відкритих джерел розпочинається з вивчення вхідних даних, або визначення ідентифікаторів, що окреслюють об'єкт пошуку. На цьому етапі аналізуються можливі напрямки пошуку та логічні зв'язки між вхідними даними, які здатні підвищити ефективність застосовуваних рішень. Зображення зовнішнього вигляду людини є достатньо поширеним ідентифікатором OSINT розслідувань [2, 3, 4].

В процесі OSINT пошуку на етапах підготовчих дій, а також порівняння даних, критично важливим є використанні спеціальних знань для повного, всебічного та науково-обґрунтованого вивчення відображень зовнішності людини. Специфікою даного виду розслідувань є потреба у якісному та водночас оперативному опрацюванні значної кількості зображень зовнішності з метою розмежування «схожих» та «тотожних»

осіб [5, с. 23–24]. Наслідком попереднього хибного висновку, щодо тотожності/відмінності зображень осіб, яке ґрунтується на підставі суб'єктивного сприйняття ознак зовнішності, може бути некоректний кінцевий результат розслідування [6].

Структура зовнішнього вигляду людини складна й містить систему елементів – частин, деталей зовнішнього вигляду, які можуть бути цілком виразно виділені при візуальному вивченні. Криміналістично значущими елементами є помітні деталі зовнішньої будови органів і ділянок голови, обличчя, тіла, кінцівок людини, предметів одягу й носильних речей, наочні функціональні прояви людини, загальнофізичні дані (стать, вік та ін.).

З точки зору криміналістики зовнішній вигляд людини є предметом вивчення криміналістичної габітоскопії, що досліджує закономірності відображення ознак зовнішності людини на різних носіях інформації, розробляє рекомендації щодо застосування техніко-криміналістичних засобів та методів збирання, дослідження та використання даних про зовнішність з метою встановлення істини у кримінальному провадженні [7]. Найбільш суттєва роль в ідентифікації особи належить криміналістичній портретній експертизі, за результатами проведення якої встановлюється факт тотожності. Уповноваженими на проведення даного виду досліджень є спеціалісти, що мають кваліфікацію за експертною спеціальністю 6.2 «Ідентифікація особи за ознаками зовнішності за матеріальними зображеннями» [8].

Під час проведення ідентифікації особи за ознаками зовнішності за матеріальними зображеннями вирішується дві основні групи завдань – ідентифікаційні та діагностичні:

– ідентифікаційні завдання – встановлення тотожності або відмінності осіб, зображених на фото/відеозаписах або інших об'єктивних відображеннях зовнішнього вигляду людини.

– діагностичні завдання – встановлення факту придатності/непридатності для ідентифікації за ознаками зовнішності, визначення расово-етнічної, статевої, вікової належності людини.

В науковій літературі спеціальні знання визначаються як результат оволодіння певним рівнем знань і навичок діяльності в конкретній професії та спеціальності. Загальновизнаними є дві процесуальні форми використання спеціальних знань у кримінальному провадженні – судова експертиза та участь спеціаліста під час проведення процесуальних дій [9, с. 278–286]. З огляду на специфіку проведення OSINT розслідувань

найбільш оптимальною формою використання спеціальних знань у галузі габітоскопії є консультація спеціаліста під час проведення слідчої дії.

Проведений аналіз на підставі викладених фактів дає підстави для висновку про те, що розвідувальна діяльність із використанням відкритих джерел збільшує можливості спеціальних служб, але в її роботі є критичні компоненти, на які необхідно звернути увагу. Найбільш вагомим є об'єктивна потреба в кваліфікованому експертному вивчені зовнішності осіб на окремих етапах OSINT розслідувань, що підвищує ефективність та результативність процесу прийняття кінцевих рішень.

Список використаних джерел :

1. Буслов П. В., Зоренко Д. С., Рябуха Ю. М. Використання технологій OSINT для отримання пошукової інформації : практичний порадник. Х.: ІПЮК для СБУ України, 2021. 28 с.
2. Шепітько В. Ю., Білоус В. В. Роль сучасних інформаційних технологій у встановленні особи злочинця. *Теорія та практика судової експертизи і криміналістики* : зб. наук. пр. Харків, 2014. Вип. 14. С. 5–11.
3. Ідентифікація російського військового-мародера з Polaroid та виправлення помилки Мінцифри. URL https://informnapalm.org/ua/identyfikatsiia-rosiiskoho-viiskovo/
4. Мародерство в Бучі: встановлені особи 10 військових рф.URL https://www.slovoidilo.ua/2022/06/02/novyna/suspilstvo/maroderstvo-buchi-vstanovleni-osoby-10-vijskovyx-rf
5. Шевцов С. О., Кожевніков О. А.. Консультації спеціаліста на стадії досудового розслідування : практ. посібник / М-во внутр. справ України; Експертна служба; Харківський наук.-дослід. експерт.-криміналіст. центр./. Харків, 2020. 43 с.
6. Катування та вбивство українського полоненого: Molfar ідентифікує військових злочинців. URL: https://www.molfar.global/blog/terrorist
7. Криміналістика : підручник / [В. В. Пясковський, Ю. М. Чорноус, А. В. та ін.] ; за заг. ред. В. В. Пясковського. – 2-ге вид., перероб. і допов. Київ : Філія вид-ва «Право», 2020. 752 с.
8. Методика ідентифікації особи за ознаками зовнішності за матеріальними зображеннями / уклад. Ковальов К. М., Коструб А. М., Павленко О. С., Чашницька Т. Г. Вид. 2-ге, перероб. і допов. Київ: ДНДЕКЦ МВС України, 2021. 48 с.
9. Мединська Л. В. Використання спеціальних знань у кримінальному провадженні України. Прикарпатський юридичний вісник. 2014. Вип. 2 (5). С. 278–286.

Анна Колодіна
кандидатка юридичних наук, доцентка, доцентка кафедри криміналістики, детективної та оперативно-розшукової діяльності Національного університету «Одеська юридична академія», м. Одеса, Україна

ІННОВАЦІЙНІ ТЕХНІКО-КРИМІНАЛІСТИЧНІ ТЕХНОЛОГІЇ У ПРАКТИЦІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ

У сучасних умовах розслідування злочинів постають виклики щодо криміналістичної техніки, що потребують з'ясування та дослідження. Так, використання штучного інтелекту у боротьбі зі злочинністю останніми роками стає все більш актуальним. Широке обговорення відповідної діяльності з використанням інноваційних технологій дасть можливість підвищити обізнаність громадськості щодо перспектив та реальних можливостей останнього у протидії злочинності. На теперішній час правоохоронні органи деяких країн використовують технології штучного інтелекту під час виконання покладених на них завдань, тому дискусії з приводу підготовлених наукових праць, зокрема, вивчення міжнародного досвіду використання алгоритмів штучного інтелекту в кримінальному провадженні та їх обговорення допоможуть дослідникам у подальших наукових розвідках.

Дослідження викликів щодо криміналістичної техніки розслідування злочинів проводилися такими науковцями, як: Блізнюк В., Гаркуша А. О., Гаркуша Є. О., Деревягін О. О., Дунаєва Т. Є, Матуєлене С., Шевчук В. М., Шепітько В. Ю., Цехан Д. М., Топчій В. В., Філіпенко Н. Є., Лукашевич С. Ю. та ін.

Сучасний контекст кримінальної діяльності визначає необхідність надзвичайно ефективних та інноваційних методів розслідування злочинів. Однією з ключових складових, що значно вдосконалює процес розкриття та припинення правопорушень, є застосування криміналістичної техніки. Завдяки стрімкому розвитку технологій та постійному зростанню складності злочинів, використання новітніх та передових засобів стає невіддільною частиною професійної практики слідчих та експертів.

Деякі з основних викликів цієї галузі включають:

1) Швидкі зміни в технологіях, що потребують постійного оновлення та адаптації криміналістичних методів та інструментів для ефективного розслідування.

2) Різноманітність даних та збільшення даних з соціальних мереж вимагає розроблення нових методів їх обробки та аналізу.

3) Зростання обсягів кіберзлочинів вимагає спеціальних методів та інструментів для виявлення та розслідування цих видів правопорушень.

4) Проблеми конфіденційності та приватності: використання криміналістичної техніки може породжувати етичні питання стосовно збереження конфіденційності та приватності осіб.

5) Забезпечення високого рівня підготовки та навичок експертів-криміналістів, які володіють сучасними технічними знаннями, є важливим завданням.

Вирішення цих викликів вимагатиме поєднання технічних інновацій, правового регулювання та сталих практичних підходів для забезпечення ефективного та етичного використання криміналістичної техніки у розслідуванні злочинів [1, С. 490].

Розглянемо виклики щодо криміналістичної техніки розслідування злочинів в контексті використання технологій штучного інтелекту (далі – ШІ). Криміналістичне дослідження сучасної злочинності показало, що комп'ютерна криміналістика стає все більш важливим інструментом у боротьбі зі злочинністю, а її інноваційні технології все більше застосовуються у практиці розслідування, зокрема: криміналістичній техніці, тактиці і методиці розслідування окремих видів злочинів. Ера штучного інтелекту вже настала і це ставить нові виклики та завдання перед наукою зокрема.

Міністерство цифрової трансформації України навіть розробило Концепцію розвитку сфери штучного інтелекту (СШІ) в Україні та планує розробити Етичний Кодекс використання СШІ з урахуванням європейського досвіду [2].

Штучний інтелект може допомогти поліпшити ефективність розслідувань, знизити кількість помилок та зайвих витрат часу і зусиль, а також допомогти аналізувати великі обсяги інформації і виявляти можливі зв'язки між різними фактами, що можуть мати ключове значення для розслідування злочинів розвідки, протидії кіберзагрозам

у сфері оборони, а також аналізу можливостей військових підрозділів [2].

Можливості використання штучного інтелекту у кримінальному провадженні в Україні досліджено у роботі В. Блізнюк [3]. Автор розглядає доцільність використання штучного інтелекту в кримінальному провадженні, оцінює вплив використання цієї технології та описує можливі проблеми, які можуть виникнути при такому застосуванні, та пропонує шляхи їх вирішення.

Зокрема, погоджуємося із позицією автора щодо можливості застосування штучного інтелекту для автоматизації деяких етапів кримінального розслідування.

Тож, використання криміналістичної техніки у розслідуванні злочинів несе за собою ряд викликів, які вимагають уваги та системного підходу для забезпечення ефективності та законності. Сучасні технології та швидкий розвиток криміналістики ставлять перед фахівцями завдання постійного оновлення та адаптації до нових реалій. Вирішення цих викликів вимагатиме поєднання технічних інновацій, правового регулювання та постійного вдосконалення практичних навичок, щоб забезпечити сучасний та ефективний підхід до розслідування злочинів в умовах такого, що швидко змінюється технологічного та кримінального середовища.

У результаті дослідження нових викликів криміналістичної техніки розслідування злочинів можна зробити висновок, що наявна потреба в оновленні криміналістичних методів і інструментів, та створенні адаптивних стратегій для швидкого реагування на технічні зміни та вдосконалення розслідувань. Такі виклики, як значна кількість даних, необхідність забезпечення безпеки даних та розслідування кіберзлочинів, приватність та конфіденційність, можуть бути вирішені шляхом використання ШІ.

Список використаних джерел:

1. Філіпенко Н. Є., Лукашевич С. Ю. Діяльність судово-експертних установ щодо запобігання злочинності з використанням прогресивних інформаційних методик та технологій. Журнал наукові інновації та передові технології. 2023. Вип. 14 (28). С. 487–495. http://perspectives.pp.ua/index.php/nauka/article/download/7907/7951/7950

2. Повідомлення про проведення публічного громадського обговорення проєкту розпорядження Кабінету Міністрів України «Про схвалення

Концепції розвитку штучного інтелекту в Україні». Міністерство та комітет цифрової трансформації України : веб-сайт. https:// thedigital.gov.ua/regulations/povidomlennya-pro-provedennya publichnogo- gromadskogo-obgovorennya-proyektu-rozporyadzhennya-kabinetu-ministriv- ukrayini-pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini

3. Блізнюк В. Можливості використання штучного інтелекту у кримінальному провадженні в Україні. Вісник Харківського національного університету імені В. Н. Каразіна. 2023. Вип. https://periodicals.karazin.ua/law/article/view/22344

Людмила Ляшевська,
кандидатка юридичних наук, .
Національний юридичний університет імені Ярослава Мудрого,
м. Харків, Україна

СУТНІСТЬ ЦИФРОВИХ ДОКАЗІВ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

Рівень злочинності, пов'язаної із застосуванням інформаційних технологій, постійно зростає, тому у кримінальній процесуальній науці тема цифрових доказів є актуальною.

Дослідженню цифрових (електронних) доказів в кримінальному провадженні присвячені праці таких вчених та науковців: Н. М. Ахтирської, В. В. Білоуса, К. Л. Брановицького, В. Г. Гагловського, Ю. Ю. Орлова, О. В. Сіренка, В. І. Решетняка, М. Г. Щербаковського та ін.

Неодноразово вченими наголошувалась необхідність закріплення поняття цифрових доказів або електронних (комп'ютерних) в КПК. В результаті був поданий проект Закону №4004 від 01.09.2020 р. про внесення змін до Кримінального процесуального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю та використання електронних доказів, який розглядався Верховною Радою України 05.09.2023 р.

У чинному КПК (ст. 237) йдеться про огляд комп'ютерних даних, який проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації за допомогою електронних засобів, фотозйомки, відеозапису, зйомки та/або відеозапису екрана тощо або у паперовій формі [1].

Згідно п. 1 ч. 2 ст. 99 КПК до документів, які можуть бути використані як докази, належать матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (у тому числі електронні) [1]. Отже, докази визначаються в КПК як відомості в цифровому вигляді.

Учені дають різні поняття електронних доказів. Н. М. Ахтирська вважає, що «електронні докази» – це дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем. Джерелами таких електронних доказів є електронні пристрої: комп'ютери, периферійні пристрої, комп'ютерні мережі, мо-

більні телефони, цифрові камери та інші портативні пристрої, мережі Інтернет [3].

В. В. Мурадов, О. І. Котляревський, Д. М. Киценко під електронними доказами визнають сукупність інформації, яка зберігається в електронному вигляді на будь-яких типах електронних носіїв та в електронних засобах [10; 8].

При дослідженні сутності цифрових (електронних) доказів слід звернути увагу на сукупність їх ознак. Серед загальних ознак цифрових (електронних) доказів фахівці вказують на такі:

– існують у нематеріальному вигляді;

– можуть бути створенні як людиною, так і бути результатом функціонування інформаційної системи;

– вони не в змозі існувати без носія інформації – вільно переміщуються в електронній мережі без технічного носія;

– їх не можна безпосередньо сприймати та досліджувати, тільки за допомогою технічних засобів і програмного забезпечення;

1. потребують специфічного порядку збирання, перевірки й оцінки;

– мають здатність до копіювання або переміщення на інший носій без втрати своїх характеристик;

2. докази не складно знищити або піддати певним змінам;

3. мають особливий статус оригіналу і можуть існувати в такому ж статусі в декількох місцях [2, с. 252; 9].

У вітчизняній практиці, як правило, поняття «цифрові» та «електронні докази» ототожнюють. Однак деякі автори вважають, що поняття «електронний» та «цифровий» доказ не тотожні. І посилаються на закордонну юридичну практику. Так, цифровий доказ «digital evidence» належить до доказування, а термін «електронний» застосовується до приладів, які використовують для роботи електрони «electronic device» [9].

Ще однією проблемою цифрових доказів виступає відсутність чіткого правового регулювання відносно процесуальної процедури вилучення, оцінки та дослідження електронних доказів на законодавчому рівні.

Серед проблем, пов'язаних із застосуванням цифрових доказів, спеціалісти також вказують на необхідність підвищення рівня обізнаності в сфері ІТ технологій усіх осіб, які мають відношення до пошуку, фіксації та дослідження доказів у судовому засіданні [9].

Проблемою дослідження електронних носіїв інформації в кримінальному судочинстві є також необмежені можливості сторони обвинувачен-

ня доступу до приватної інформації, що може призводити до порушень прав у сфері таємниці особистого життя, тому на законодавчому рівні треба закріпити механізм та випадки визнання їх недопустимими у кримінальному провадженні.

Слід також зазначити, що електронна (цифрова) інформація, що містить відомості про вчинення кримінального порушення – це не лише електронні документи, фото-, відео- та звукозапис, а й електронна інформація телекомунікаційних, мережевих та супутникових систем пристроїв штучного інтелекту, охоронні та пропускні системи, платіжні термінали, навігаційні системи, інформаційні ресурси у вигляді певних реєстрів тощо.

Таким чином, інститут цифрових (електронних) доказів потребує вдосконалення як на законодавчому рівні (закріплення поняття, процедури вилучення, оцінки та дослідження електронних доказів), так і в практичному застосуванні.

Список використаних джерел :

1. Кримінальний процесуальний кодекс України від 13.04.2012 р. №4651-VI. URL : https://zakon.rada.gov.ua/laws/show/4651–17#Text

2. Алєксєєва-Процюк Д. О., Брисковська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування // Науковий вісник публічного та приватного права. 2018. Вип. 2. С. 247–253.

3. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження [Електронний ресурс] / Н. М. Ахтирська // Науковий вісник Ужгородського національного університету. 2016. Вип. 36(2). С. 123–125.

4. Білоус В. В. Цифрова фотовідеографія : інноваційна форма фіксування та презентації юридично значущої інформації. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці*: матеріали міжнар. «кругл. столу» (Харків, 12 груд. 2019 р.) / Нац. акад. прав. наук України, НДІ вивч. проблем злочинності ім. акад. В. В. Сташиса. Харків : Право, 2019. С. 26–29.

5. Гарасимів О. І., Марко С. І., Ряшко О. В. Цифрові докази: деякі проблемні питання щодо їх поняття та використання у кримінальному судочинстві // Науковий вісник Ужгородського національного університету. Серія: Право. Т. 2. 2023. №75. С. 158–162.

6. Гуцалюк М. В., Антонюк П. Є. Процесуальна спроможність використання електронної (цифрової) інформації як доказу в кримінальному провадженні. *Інформація і право*. 2022. №2(41). С. 116–122.

7. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні // Юридичний науковий електронний журнал. 2020. №8. С. 418–421.

8. Котляревський О. І. Комп'ютерна інформації як речовий доказ у кримінальній справі / О. І. Котляревський, Д. М. Киценко // Інформаційні технології та захист інформації: збірник наукових праць. 1998. №2. С. 70–79.

9. Метелев О. П. Цифрові докази у кримінальному процесі: поняття, критерії та проблеми правозастосування. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення* : матеріали пост. діючого наук.-практ. семінару (м. Харків, 20 жовт. 2017 р.) / СБУ, Нац. юрид. ун-т ім. Ярослава Мудрого, Ін-т підготовки юрид. кадрів для СБУ. Харків: Право, 2017. Вип. 9. С. 87–91.

10. Мурадов В. В. Електронні докази: криміналістичний аспект використання. Порівняльне правознавство. 2013. №3–2. С. 313–315.

11. Сіренко О. В. Електронні докази у кримінальному провадженні. Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика). 2019. Вип. 14. С. 208–214. URL: http://nbuv.gov.ua/UJRN/muvnudp_2019_14_24

12. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету*. 2013. №5. С. 256–259.

13. Горбан Н. В., Тарасенко Д. І. Щодо електронного документа і цифрового доказу у новому кримінальному процесі. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення*: Матеріали постійно діючого наук.-практ. семінару, 19 жовт. 2012 р. / СБУ, Ін-т підгот. юрид. кадрів для СБУ Нац. ун-ту «Юрид. акад. України ім. Ярослава Мудрого». Харків : ТОВ «Оберіг», 2012. Вип. 4. С. 280–282

Юрій Мороз
завідувач сектору дактилоскопічних досліджень відділу криміналістичних видів досліджень Луганського науково-дослідного експертно-криміналістичного центру МВС України
м. Дніпро, Україна

Альона Ясенок
старша судова експертка сектору дактилоскопічних досліджень відділу криміналістичних видів досліджень Луганського науково-дослідного
експертно-криміналістичного центру МВС України
м. Дніпро, Україна

ПРОБЛЕМИ ФОРМУВАННЯ І РОЗВИТКУ ЦИФРОВОЇ КРИМІНАЛІСТИКИ

З кожним роком інноваційні технології все більше впроваджуються в різні сфери суспільного життя. Не винятком є і криміналістична експертиза, яку сучасні інформаційні технології вивели на новий етап розвитку. Зокрема, завдяки новітнім технологіям з'явилася нова галузь криміналістики – цифрова криміналістика.

Цифрова криміналістика – прикладна наука про розкриття злочинів, пов'язаних з комп'ютерною інформацією, про дослідження цифрових доказів, методи пошуку, отримання і закріплення таких доказів.

Цифрова криміналістика є «однією з галузей криміналістики, яка зосереджена на кримінально-процесуальному праві і доказах стосовно комп'ютерів і пов'язаних з ними пристроїв», такими, як мобільні пристрої (телефони, смартфони тощо), ігрові приставки та інші пристрої, що функціонують через Інтернет (пристрої для здоров'я та фітнесу та медичні прилади тощо). Цифрова криміналістика, зокрема, має відношення до процесу збору, отримання, збереження, аналізу та подання електронних доказів (також відомих як цифрові докази) з метою отримання оперативно-розшукових відомостей і здійснення розслідування та кримінального переслідування по відношенню до різних видів злочинів, включаючи кіберзлочини. Цифрова криміналістика виникла орієнтовно у 80-ті роки XX століття. Перший етап розвитку цифрової криміналістики охоплює 1985–1995 роки. Цей етап включав використан-

ня програмних кодів для перегляду даних у внутрішніх операційних системах та апаратних засобах комп'ютерів. Другий етап розвитку цифрової криміналістики припадає на 1995–2005 роки. Він ознаменувався появою кіберзлочинності і необхідністю боротьби з нею. Третій етап розвитку цифрової криміналістики відбувся у 2005–2010 років. У цей період виникають складні цифрові моделі розслідування злочинів. Однією з таких моделей, яка широко використовується у світі, стала «загальна модель комп'ютерних криміналістичних розслідувань» (Generic Computer Forensic Investigation Model – GCFIM). Сучасний етап розвитку цифрової криміналістики починається приблизно в 2010 році та продовжується по цей час [1, с. 176–180].

У судових науках сформовано окрему галузь – цифрову криміналістику, яка являє собою систему наукових методів дослідження цифрових доказів з метою сприяння виявленню та розслідуванню кримінальних правопорушень. Водночас у вітчизняній системі криміналістики відповідні засоби та методи належного місця досі не знайшли. Тому в Україні існує нагальна потреба у становленні окремого розділу криміналістичної техніки, присвяченого криміналістичному дослідженню цифрових доказів, зміст якого включатиме наукові положення цифрової криміналістики як галузі судових наук, адаптованих до реалій вітчизняної правоохоронної практики та криміналістичної теорії.

Цифрова криміналістика ґрунтується на загальних принципах криміналістики. Зокрема, одним із головних з них є принцип обміну Едмона Локара: коли об'єкти і поверхні вступають в контакт один з одним, відбувається перехресне перенесення матеріалів. У контексті цифрової криміналістики люди, після використання інформаціоно-комунікаційних тех-нологій (ІКТ), залишають цифрові сліди. Зокрема, особа, яка використовує ІКТ, може залишити «цифрові відбитки». Дані, залишені користувачами ІКТ, можуть розкрити відомості про них, включаючи інформацію про вік, стать, расову та етнічну приналежність, громадянство, сексуальну орієнтацію, думки, уподобання, звички, хобі, історію хвороби і проблеми зі здоров'ям, психологічні розлади, статус, зайнятість, приналежність до будь-якої спільноти, особисті відносини, геолокацію, розпорядок дня та інші активності. Такі дані можуть використовуватися для доведення або спростування твердження про факт; підтвердження або спростування показань потерпілого, свідка і підозрюваного; визначення причетності або непричетності підозрюваного

до скоєння злочину. Дані зберігаються в цифрових пристроях (наприклад, комп'ютерах, смартфонах, планшетах, телефонах, принтерах, «розумних» телевізорах (Smart TV) і будь-яких інших пристроях, які мають цифрову пам'ять), зовнішніх запам'ятовуючих пристроях (наприклад, зовнішніх жорстких дисках і USB-флеш накопичувачах), мережевих компонентах і пристроях (наприклад, маршрутизаторах), серверах і хмарному сховищі (де дані зберігаються «в кількох центрах даних в різних географічних точках).

Перш ніж цифрові докази можуть бути представлені в суді в якості прямих або непрямих доказів, їх треба розпізнати (тобто необхідно показати, що докази відповідають передбачуваній меті) [2, с. 275–279].

У порівнянні з традиційними доказами (наприклад, паперовими документами, зброєю, контрольованими речовинами та ін.), цифрові докази створюють унікальні складності при аутентифікації через обсяг доступних даних, їх швидкості (тобто швидкості, з якою вони створюються і передаються), нестійкості (тобто вони можуть швидко зникнути при перезапису або видаленні) і уразливості (тобто їх легко можна обробити, змінити або пошкодити). У той час як одні країни впровадили норми доказового права, що включають в себе вимоги щодо аутентифікації, які конкретно відносяться до цифрових доказів, інші країни для аутентифікації традиційних доказів і цифрових доказів використовують схожі вимоги. У Франції, наприклад, як паперові, так і електронні документи повинні аутентифікуватися шляхом перевірки особистості творця документів і цілісності документів.

Перевірка цілісності документів означає не тільки перевірку їх точності, а й здатності зберігати точність (тобто несуперечливість) з плином часу. Більш того, для того щоб уніфікувати режими поводження з нецифровими і цифровими доказами Сінгапур вніс поправки в норми процесуального права, прийнявши Закон про докази 2012 року, щоб забезпечити однакову практику аутентифікації для нецифрових і цифрових доказів. У 2012 році Міжнародна організація зі стандартизації (ISO) і Міжнародна електротехнічна комісія (МЕК) опублікували міжнародні стандарти, що стосуються поводження з цифровими доказами (ISO / IEC 27037 Керівництво по ідентифікації, збирання, одержання і збереження свідчень, представлених в цифровій формі). Пропонуються наступні чотири етапи поводження з цифровими доказами: Ідентифікація. Цей етап включає в себе пошук і розпізнавання відповідних доказів,

а також їх документування. На цьому етапі пріоритетні завдання збору доказів визначаються на основі цінності і мінливості доказів.

Збір. Цей етап передбачає збір всіх цифрових пристроїв, які можуть містити дані, що мають доказову цінність. Ці пристрої потім транспортуються в лабораторію судової експертизи або іншу установу для збору і аналізу цифрових доказів. Цей процес називається збором даних в статичному режимі. Однак бувають випадки, коли збір даних в статичному режимі є практично нездійсненним. У таких ситуаціях здійснюється збір даних в реальному часі.

Отримання. Цифрові докази необхідно отримувати без шкоди для цілісності даних. Таке отримання даних без їх зміни здійснюється шляхом створення копії вмісту цифрового пристрою (процес, відомий як створення неспотвореного образу) з використанням пристрою (блокувальника запису), який призначений для запобігання зміни даних в процесі копіювання. Для того щоб визначити, чи є дублікат точною копією оригіналу, значення хешфункції розраховується з використанням математичних обчислень; тут для отримання значення хешфункції використовується криптографічна хешфункція. Якщо значення хешфункції для оригіналу та копії збігаються, то вміст копії є точно таким же, що і в оригіналі.

Збереження. Цілісність цифрових пристроїв і цифрових доказів – «процес, за допомогою якого слідчі забезпечують охорону місця злочину (або події) і збереження доказів протягом всього періоду провадження у справі.

У журнал реєстрації записують інформацію про те, хто здійснював збір доказів, де і яким чином вони були зібрані, які особи отримали ці докази, і коли вони їх отримали. Ретельне документування процесу цифрової судової експертизи на кожному етапі має важливе значення для забезпечення допустимості доказів у суді. [3, с. 79–84].

Список використаних джерел :

1. Колодіна А. С., Федорова Т. С. Цифрова криміналістика: проблеми теорії і практики. Київський часопис права. 2022. Вип. 1. С. 176–180.

2. Самодін А. В. Сучасне розуміння феномену «цифрова криміналістика». Інновації в криміналістиці та судовій експертизі : матеріали міжвідом. наук.-практ. конф. (Київ, 25 листоп. 2021 р.) / [редкол.: В. В. Чернєй, С. С. Чернявський, А. А. Саковський та ін.]. Київ : Нац. акад. внутр. справ, 2021. С. 275–279.

3. Когутич І. І. Застосування цифрових технологій –новий напрям криміналістики. Наукові читання пам'яті Ганса Гросса: збірник тез міжнародної науково-практичної конференції (м. Чернівці, 09 грудня 2021 р.). Чернівецький національний університет імені Юрія Федьковича. Чернівці : Технодрук, 2021. С. 79–84

Владислав Негребецький
кандидат юридичних наук, доцент,
науковий співробітник НДІ вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України,
доцент кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого, м. Харків, Україна

МОЖЛИВОСТІ ЦИФРОВИХ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ В ПРАВООХОРОННІЙ ДІЯЛЬНОСТІ: ДОСВІД ВЕЛИКОБРІТАНІЇ

У зв'язку війною на Україні особлива роль відводиться роботі правоохоронних органів щодо підтримання суспільного порядку, подолання та документування наслідків, порушень норм та звичаїв війни, норм міжнародного права. У зв'язку з цими трагічними подіями вельми актуальним стало питання забезпечення безпеки через застосування інноваційних автоматизованих систем перевірки осіб за допомогою біометричних технологій.

Ідея перевірки й підтвердження особи людини при перетинанні державного кордону, контрольно-пропускного пункту, 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. *В умовах воєнного стану впровадження таких документів набуло особливої актуальності*.

Біометричні паспорти набувають все більшого поширення у світі [1]. 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 [2]. В 2017 році Уряд України затвердив Положення про національну систе-

му біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства [3]. 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.

Державна прикордонна служба у грудні 2017 р. презентувала систему фіксації біометричних даних іноземців та осіб без громадянства [4]. Демонстрація роботи системи відбулася в столичному аеропорту «Київ». Ця система фіксації біометричних даних іноземців та осіб без громадянства було розгорнуто на виконання Указу Президента України від 30 серпня 2017 р. №256 «Про рішення Ради національної безпеки та оборони України від 10 липня 2017 р. «Про посилення контролю за в'їздом в Україну, виїздом з України іноземців та осіб без громадянства, додержання ними правил перебування на території України» [5]. 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. З діючих пунктів пропуску 157 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. Під час паспортного контролю інспектори Держприкордонслужби здійснюють перевірку паспортних документів іноземців, в тому числі за базами Інтерполу. Також відбуватиметься зчитування інформації (відбитки пальців) за допомогою рідерів, яка надходитиме 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 спів-

падіння даних особу буде направлено на додатковий контроль для з'ясування обставин.

Національний банк розробив мобільний додаток UAPassportReader для зчитування інформації з біометричних документів (2020) [6].

Позитивним є досвід поліції провідної країни – Великобританії в галузі використання біометричних технологій. Поліція Великобританії у лютому 2018 р. розпочала використовувати мобільну систему відбитків пальців, яка дозволяє перевірити особу невідомої людини менш ніж за хвилину. Відбитки пальців, зібрані на вулиці, будуть порівнюватися з 12 мільйонами записів, що містяться в національних базах даних про відбитки пальців злочинців та імміграції, і, якщо буде знайдено збіг, повернуть ім'я особи, дату народження та іншу ідентифікаційну інформацію. Офіцери вдаватимуться до сканування відбитків пальців лише в тому випадку, якщо вони не можуть ідентифікувати особу іншими способами. Пристрої Strategic Mobile являють собою невеликі електронні сканери, які фіксуються на смартфони і дозволяють поліцейським фіксувати відбитки пальців людини з більшою роздільною здатністю, ніж датчики, вбудовані в телефони. Вони були введені, щоб допомогти офіцерам перевірити особу невідомої людини і можуть отримати результати менш ніж за 60 секунд. Після сканування відбитків пальців людини він перевіряється з двома урядовими базами даних: IDENT1, яка містить відбитки пальців тих, кого в минулому взяла під варту поліція; та IABS, яка зберігає відбитки пальців громадян, які не є громадянами Великобританії, які в'їхали в країну. Станом на липень 2020 року поліцейські виконали щонайменше 100 сканувань на 100 000 людей, які проживають у відповідних районах [7].

З метою розшуку підозрюваних осіб поліцейськими використовуються й інші біометричні системи. Так, у 2018 р. співробітники поліції в Чжэнчжоу, Китай одержали для роботи незвичайні сонцезахисні окуляри, оснащені програмним забезпеченням для розпізнавання осіб [8]. Ці устрої поліція Китаю досить успішно застосовує для піймання розшукуваних злочинців.

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 використовували системи BAT

(Biometrics Automated Toolset) або HIIDE (Handheld Interagency Identity Detection Equipment) [9].

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 [9]. 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.

В судово-експертній діяльності існує перспектива розширення використання біометричних технологій з метою ідентифікації особи. Так, матеріали відеозапису, де зафіксовані ознаки ходи особи, можуть потрапляти до сфери кримінального провадження із численних камер спостереження, відеореєстраторів, камери мобільних телефонів. Ходу визначають через ознаки (темп ходи, особливості, положення рук і тулуба під час ходьби). При цьому зважають на її швидкість, визначають довжину та ширину кроку, положення та ступінь підіймання стоп. Хода у кожній особи – унікальна. Вивчення ходи разом з іншими ознаками дає змогу ідентифікувати особу за матеріалами відеозапису з високим ступенем імовірності.

Криміналістичний аналіз ходи людини з використанням біометричних технологій використовувався як доказ у кримінальних провадженнях, приміром, у Великій Британії (Birch, Gwinnett, & Walker, 2016; Nirenberg, Vernon, & Birch, 2018), Данії (Larsen, Simonsen, & Lynnerup, 2008), Нідерландах. Розробки в цій сфері здійснюють у США та Японії [10].

Список використаних джерел :

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. 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

3. 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

4. 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/

5. Про рішення Ради національної безпеки та оборони України від 10 липня 2017 р. «Про посилення контролю за в'їздом в Україну, виїздом з України іноземців та осіб без громадянства, додержання ними правил перебування на території України»: Указ Президента України від 30 серпня 2017 р. № 256. URL: https://www.president.gov.ua/documents/2562017–22506

6. Національний банк розробив мобільний додаток UAPassportReader для зчитування інформації з біометричних документів (14.05.2020). URL: https://www.facebook.com/NationalBankOfUkraine/photos/a.150551338299616 2/2572459809634842/?type=3&theater

7. Police use of fingerprint scanners disproportionately targets Black Britons (03.11.2020). URL: https://www.wired.co.uk/article/police-fingerprint-scan-uk

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

9. 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

10. Хахановський В. Г. Ідентифікація особи за ходою, зафіксованою в матеріалах відеозапису. *Криміналістичний вісник* Вип. 1 (33), 2020. С.72–80. URL: https://visnyk.dndekc.mvs.gov.ua/index.php/visnuk/article/view/103/69

Ярослав Неділько
доктор філософії у галузі права (PhD), асистент кафедри кримінального процесу та криміналістики Навчально-наукового інституту права Київського національного університету імені Тараса Шевченка, м. Київ, Україна

ОСОБЛИВОСТІ ВИКОРИСТАННЯ МОЖЛИВОСТЕЙ ШТУЧНОГО ІНТЕЛЕКТУ ПІД ЧАС РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ КІБЕРПРАВОПОРУШЕНЬ

Штучний інтелект стрімко проникає у всі сфери життєдіяльності людини. Інтернет, медицина, безпека, освіта, культура вже масово використовують сучасні можливості штучного інтелекту. З одного боку, наприклад, це сприяє швидкому пошуку необхідної інформації, встановленню вірного діагнозу та призначення ефективного лікування у медицині, мінімізації людських ресурсів у інших галузях тощо. З іншого, виникають нові криміногенні виклики, спричинені розвитком штучного інтелекту.

Так, можна виокремити випадки, коли штучний інтелект використовується як засіб вчинення кримінального правопорушення або є «суб'єктом» вчинення протиправного діяння.

У США люди похилого віку дедалі частіше стають жертвами телефонних шахраїв. Використовуючи штучний інтелект, що допомагає відтворити голос, інтонацію і тембр близьких родичів пенсіонерів, злочинці виманювали у них кошти [1].

У іншому випадку, злочинці завдяки використанню штучного інтелекту підробили голос директора компанії та зуміли незаконно заволодіти 35-ма мільйонами доларів [2].

З інтенсивним розвитком штучного інтелекту почали фіксуватися випадки, коли штучний інтелект вчиняв кримінальні правопорушення.

Після тривалих розмов з чат-ботом на основі штучного інтелекту особа вчинила самогубство. 30-літній чоловік думав про самогубство як єдиний вихід із ситуації, а чат-бот спонукав його до таких дій, пишучи повідомлення наступного змісту: «Якщо ти хотів померти, чому ти не зробив це раніше?» [3].

І хоча використання штучного інтелекту у злочинних цілях набуває поширеного розвитку, у той же час правоохоронні органи також використовують його можливості для розслідування та розкриття кримінальних правопорушень.

Наприклад, поліція США використовує систему «Clearview», що дозволяє завантажувати фотографії облич підозрюваних та знаходити збіги в базі даних із мільярдів зібраних зображень з мережі Інтернет. Дана система вважається однією з найточніших у розпізнаванні облич [4].

У іншій ситуації, поліція Нью-Йорку використала штучний інтелект під назвою «Rekor», що допоміг встановити торговця наркотиками. Аналізуючи маршрут злочинця, дана система встановила, що він здійснював поїздки у місця, які використовувалися злочинцями для збуту наркотичних засобів [5].

Враховуючи міжнародний досвід та наукові дослідження щодо використання можливостей штучного інтелекту під час розслідування кримінальних правопорушень, можна запропонувати шляхи його впровадження в процес розслідування кримінальних кіберправопорушень.

1. Використання штучного інтелекту під час планування розслідування зазначених протиправних діянь. Беручи за основу успішно розслідуванні кримінальні кіберправопорушення, штучний інтелект може складати ефективний план їх розслідування. Однак, варто зауважити, що план складений штучним інтелектом повинен мати рекомендаційний характер, а остаточне рішення про проведення тих чи інших процесуальний дій повинно належати суб'єкту розслідування.

2. Використання штучного інтелекту до або під час проведення допиту свідка, потерпілого чи підозрюваного під час розслідування даних протиправних діянь. Штучний інтелект може рекомендувати питання, які необхідно ставити залежно від виду та специфіки розслідування кримінальних кіберправопорушень, що допоможе спрямовувати перебіг допиту в ефективне русло.

3. Використання штучного інтелекту до або під час проведення огляду веб-сайту під час розслідування кримінальних кіберправопорушень. Штучний інтелект може самостійно аналізувати відповідну інформацію, що міститься на сайті, після чого скласти відповідний протокол огляду.

4. Використання штучного інтелекту спеціалістом при складанні висновків у зазначених протиправних діяннях. Під час розсліду-

вання кримінальних кіберправопорушень може виникнути необхідність у отриманні доказів. З цього приводу, можна залучати спеціаліста, який володіючи спеціальними знаннями та навичками може надавати висновки, що можуть визнаватися доказом у кримінальному провадженні (стаття 298–1 КПК України). Під час формування даного висновку спеціаліст може користуватися можливостями штучного інтелекту в залежності від конкретної ситуації. Наприклад, при дослідженні шкідливого програмного забезпечення, збирання даних з відкритих джерел тощо.

Незважаючи на позитивні моменти впровадження штучного інтелекту в криміналістичну діяльність, зокрема використання його можливостей під час розслідування кримінальних кіберправопорушень, світове співтовариство з обачністю ставиться до його впровадження у всі сфери людської життєдіяльності.

Отже, пропонуємо наступний алгоритм дій, що стосуються впровадженню використання можливостей штучного інтелекту під час досудового розслідування кримінальних кіберправопорушень:

1) чітка законодавча регламентація використання можливостей штучного інтелекту під час досудового розслідування кримінальних кіберправопорушень у Кримінальному процесуальному кодексі України;

2) створення окремого технічного підрозділу у складі Національної поліції України, який буде здійснювати постійний моніторинг та вдосконалення можливостей штучного інтелекту, що використовують суб'єкти розслідування;

3) підвищення практичного рівня користування штучним інтелектом слідчими, дізнавачами, прокурорами шляхом проведення відповідних тренінгів;

4) створення окремих структурних підрозділів у складі Національної поліції України, які будуть проводити розслідування кримінальних кіберправопорушень, вчинених з використанням штучного інтелекту.

Список використаних джерел :

1. ШІ допомагає всім, навіть шахраям. Як штучний інтелект став новою зброєю кіберзлочинців та стимулював фери на 8 млрд. https://forbes.ua/innovations/shi-dopomagae-vsimi-navit-shakhrayam-yak-shtuchniy-intelekt-stimulyuvav-aferi-na-8-mlrd-19092023–16102

2. Банк в ОАЕ пограбували на $35 мільйонів завдяки штучному інтелекту. URL:https://www.ukrinform.ua/rubric-technology/3333688-bank-v-oae-pograbuvali-na-35-miljoniv-zavdaki-stucnomu-intelektu.html

3. Зафіксована перша смерть людини від штучного інтелекту. URL: https://it.comments.ua/ua/news/technology/zafiksovana-persha-smert-lyudini-vid-shtuchnogo-intelektu-711670.html

4. Clearview AI used nearly 1 m times by US police, it tells the BBC.

5. URL: https://www.bbc.com/news/technology-65057011 AI System Helped Cops Identify a Drug Trafficker Just by Analyzing His Driving Patterns. URL: https://gizmodo.com/rekor-ai-system-analyzes-driving-patterns-criminals-1850647270

Юлія Рєпіна
кандидат економічних наук, доцент, науковий співробітник відділу дослідження проблем кримінального процесу та судоустрою, Науково-дослідний інститут вивчення проблем злочинності ім. акад. В. В. Сташиса НАПрН України, м. Харків, Україна

РИЗИКИ ВИКОРИСТАННЯ ТЕХНОЛОГІЙ ШТУЧНОГО ІНТЕЛЕКТУ В КРИМІНАЛЬНІЙ ЮСТИЦІЇ В УКРАЇНІ

Використання технологій штучного інтелекту (далі – ШІ) стрімко поширюється на всі сфери життя. Зараз вже важко згадати, коли діалог із Siri – хмарним персональним помічником перестав дивувати, а використання чат-боту для онлайн-спілкування із організаціями та установами, в тому числі і державними, стало звичною справою в Україні. Втім «допомога» чат-боту наразі досить часто викликає одночасно зауваження та роздратування (в першу чергу, це стосується веб-сайтів/сторінок у соціальних мережах (месенджерах) надавачів державних послуг). Ще приклади – нав'язлива і нативна реклама товарів та послуг, яка з'являється, зокрема, при користуванні новинними ресурсами. На побутовому рівні часто у людей з'являється роздратування від зайвої та непотрібної/не корисної інформації. З'являється відчуття, що електронний гаджет про власника та його вподобання знає все. Втім, навряд чи це так. Достатньо подивитись якусь комерційну об'яву в Інтернеті, і гаджет самостійно пропонуватиме схожі об'яви своєму власникові ще протягом певного часу. Це і є проявом «машинного навчання», яке вбудовано в сучасні електронні пристрої. Очевидно, що проблема зайвих, непотрібних застосунків відома більшості сучасних людей. На жаль, в Україні під «діджиталізацією» (якщо подивитися державні програми, то можна прочитати в одному реченні через кому як напрями державної політики в якійсь сфері/галузі/царині діджитилізація та цифровізація чогось) розуміють «фасадні» нікому не потрібні, безглузді псевдо реформи. Чудовий приклад, який є одним із найдратівливіших для тих, хто змушений користуватися державними послугами – повсюдні та безальтернативні «електронні черги» від районної поліклініки до міграційної служби, у які дуже важко «попасти», переважно з технічних причин – недоліки у роботі веб-сайтів державних (комунальних) установ. Невдалих прикладів вимушеного користування інноваційними технологіями (інформаційни-

ми/інформаційно-(теле)комунікаційними, цифровими) насправді багато. Але необхідно усвідомлювати, що проблема полягає не в «поганих/шкідливих технологіях», а в винахідниках/розробниках/замовниках та їх некомпетентності і нехтуванні дотриманням етичних принципів, норм і правил при запровадженні та використанні таких. І якщо знання, навички, досвід – це справа часу, то етичні приписи – обов'язок держави. Саме держава встановлює правила шляхом правового регулювання суспільних відносин.

У той же час переваги, які надають технології ШІ людству, є надто суттєвими, щоб ними не скористатися. Але важливим є розуміння, що побутове користування «ШІ» для розваги та використання технологій ШІ для вирішення завдань кримінального провадження відповідно до статті 2 Кримінального процесуального кодексу України, хоч і «різні справи», але потребують однаково зваженої та продуманої державної політики у сфері цифрових інновацій .

Отже, технології ШІ пропонують великі можливості у правоохоронній сфері та кримінальному судочинстві, зокрема, у вдосконаленні методів роботи правоохоронних та судових органів, а також у підвищенні ефективності боротьби зі злочинами, особливо у фінансовій сфері, що пов'язані із відмиванням коштів і фінансуванням тероризму, та, так званими, кіберзлочинами (про що досить активно вже кілька років відзначається на дискусійних майданчиках різного рівня від студентських аудиторій до міжнародних регіональних та глобальних інституцій, зокрема Ради Європи та ЄС). Зазначимо, що наразі в світі технології ШІ вже використовуються в кримінальній юстиції, зокрема для: розпізнавання обличчя; автоматизованого розпізнавання номерних знаків транспортних засобів; ідентифікації мовця; ідентифікації мовлення; звукового спостереження (алгоритми виявлення пострілів); автономного дослідження і аналізу ідентифікованих баз даних; прогнозування (прогностична поліція та аналітика гарячих точок злочинності); детектору поведінки; автономної ідентифікації випадків фінансового шахрайства та фінансування тероризму; моніторингу соціальних медіа (збір даних та інтелектуальний аналіз для виявлення закономірностей); IMSI-кетчера (IMSI-перехоплювача) та автоматизованих систем виявлення, розпізнавання та спостереження об'єктів за різними можливостями виявлення (наприклад, виявлення серцебиття та розподіл температури) [1]. Що стосується застосування інструментів ШІ у судовій системі, то, знову ж таки

світовий досвід свідчить, що це можливо, зокрема, для (1) розрахунку ймовірності вчинення повторного правопорушення та (2) для вирішення завдань пробації або (3) при прийнятті рішення щодо покарання (принаймні такі напрямки використання технологій ШІ широко обговорюються як експертами, так і громадськістю у всьому світу).

Водночас застосування сучасних цифрових технологій потребує обережного впровадження у свою діяльність технологій ШІ органами кримінальної юстиції, які мають справу із обмеженнями прав і свобод людини. Адже, незважаючи на вигоди, які надає використання ШІ кримінальній юстиції, експертами в галузі прав людини виявлені потенційні ризики: (1) непрозорість прийняття рішень, (2) різні типи дискримінації, (3) втручання в приватне життя, (4) виклики для захисту (а) персональних даних, (б) людської гідності та (в) свободи слова та інформації (перелік не є вичерпним), які посилюються в секторі правоохоронних органів і кримінального судочинства, оскільки здатні вплинути на презумпцію невинуватості, основні права на свободу особи та особисту недоторканність, а також на ефективний засіб правового захисту та справедливий суд (та інші права і свободи, гарантовані як міжнародними конвенціями, так і внутрішнім законодавством більшості держав).

Національна кримінальна юстиція наразі має готуватися серед іншого до запровадження у свою діяльність технологій ШІ. Очевидно, що технологічний прогрес не зупиниться. Способом недопущення негативних наслідків використанням ШІ в кримінальному процесі України має всі підстави стати ризик орієнтований підхід – процес прийняття та виконання управлінських рішень, спрямованих на зменшення впливу негативних наслідків реалізації ризиків на кримінальне провадження, який передбачає (1) ідентифікацію, (2) аналізування, (3) оцінювання, (4) обробляння ризику та (5) моніторинг прийнятого рішення. В залежності від розрахованого/встановленого рівня ризику (від високого (не допустимого) до мінімального (допустимого)) для держави, суспільства і громадян, їх прав та інтересів (за якісними та кількісними показниками рівня ризику) і мають у подальшому прийматися рішення державною владою про впровадження або не впровадження/обмежене впровадження технологій ШІ в діяльність правоохоронних та судових органів України. Робота за цим напрямом в нашій країні тільки розпочинається.

Список використаних джерел :

1. European Parliament (2021). Artificial Intelligence in Criminal Law and its Use by the Police and Judicial Authorities in Criminal Matters : Resolution of 6 October 2021 (2020/2016(INI)). URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX%3A52021IP0405 (дата звернення: 29.12.2023)

Роман Сушко
завідувач відділу судової експертизи,
Дніпропетровський науково-дослідний експертно-криміналістичний
центр МВС України, м. Дніпро, Україна

ПРОБЛЕМИ ВПРОВАДЖЕННЯ СИСТЕМ АВТОМАТИЧНОГО РОЗПІЗНАВАННЯ ОБЛИЧ В УКРАЇНІ

Автоматичне розпізнавання обличчя – це метод ідентифікації або перевірки особистості людини за допомогою унікальних характеристик її обличчя. Ця технологія фіксує, аналізує та порівнює моделі з деталей обличчя кількох людей. Його можна використовувати для перевірки особи на зображеннях, відео або в режимі реального часу [1]. У криміналістиці в нашій державі, на жаль, система автоматичного розпізнавання облич майже не використовується. Відеокамери з системою автоматичного розпізнавання облич встановлено в деяких великих містах, але вони функціонують під патронатом органів місцевого самоврядування і на законодавчому рівні їх використання не врегульовано. Однак в найближчому майбутньому зазначена система має багато перспектив. Як приклад можна відзначити Китай, який є справжнім флагманом у світі по впровадженню систем автоматичного розпізнавання облич. На теперішній час в Китаї крім розшуку злочинців та зниклих осіб вона використовується для посадки в поїзд, оплати покупок, доступу до відеоігор з обмеженням по віку, зняття готівки в банкоматі, ідентифікації громадян, які вчинили дрібні правопорушення та у багатьох інших випадках.

Однак в контексті криміналістики ми розглянемо розпізнавання обличчя що використовується правоохоронними органами для пошуку підозрюваних і зниклих безвісти людей. Це може допомогти знайти людей, які вчинили злочини, і допомогти їх негайно затримати, що в свою чергу допоможе набагато збільшити безпеку у суспільстві, оскільки рецидивна злочинність в нашій державі на даний момент складає близько 30% [2], і це тільки за офіційною статистикою, не враховуючі латентні злочини. Також наявність таких систем дозволила б оперативно відслідковувати пересування як злочинців так і безвісно зниклих осіб, оперативно реагувати та планувати дії з їх розшуку. Однак, на жаль, в нашій державі використання таких систем законодавчо не врегульова-

но, тому ні самих систем, ні способів наповнення їх інформацією та матеріалами для ідентифікації, ні підстав для використання у підрозділах органів внутрішніх справ поки немає.

При впровадженні в практичну діяльність Автоматичних систем ідентифікації облич потрібно звертати увагу на наступні аспекти:

1. Точність. Одне з найбільших занепокоєнь щодо технології розпізнавання облич – чи вона точна. Якщо це не так, для особи можуть настати несприятливі наслідки. Наприклад, особу можуть помилково ідентифікувати як підозрюваного у злочині та заарештувати. Людину можуть помилково ідентифікувати під час посадки на рейс і затримати охорону аеропорту. Досвід показує, що недопрацьоване програмне забезпечення має труднощі з розпізнаванням певних людей, зокрема афроамериканців, представників етнічних меншин, жінок та молодих людей. Щоб уникнути звинувачень у расовому профілюванні чи інших підступних цілях, важливі високі оцінки точності. Так в ст. 22 Загального регламенту про захист даних [3] забороняється автоматизоване прийняття рішень, тобто будь-яке «рішення, засноване виключно на автоматизованій обробці, включаючи профілювання, яке спричиняє щодо нього юридичні наслідки або подібним чином істотно впливає на нього». Виняток до цієї заборони, якщо це дозволено законодавством Союзу або держави-члена, яке передбачає відповідні гарантії прав і свобод суб'єкта даних, принаймні право на втручання людини з боку контролера. Це означає, що збіги, засновані на технологіях розпізнавання облич мають бути підтверджені людьми (наприклад, експертами), які оцінять всі наявні ознаки та ситуацію, і на основі цієї оцінки вживають заходів. Багато помилкових спрацьовувань на цьому етапі вже виключено.

2. Прозорість. Системи розпізнавання обличчя часто працюють, завантажуючи базу даних біометричних даних, зображень або відео в комп'ютер і дозволяючи штучному інтелектові встановлювати збіги. Цей процес зазвичай вимагає величезної кількості даних. Загальний регламент про захист даних (GDPR) вимагає, щоб під час збирання та використання публічної інформації їм надавалося пояснення того, як збираються та використовуються їхні дані. Навіть у країнах, які не підпадають під GDPR, усім сторонам, які беруть участь у цій технології, важливо розуміти, кому належать дані, які збираються, і як вони будуть використовуватися.

3. Приватність та етичність. Використання таких технологій може порушувати приватність осіб, які не хочуть бути розпізнаними та випадки використання технології без згоди осіб.

Безпека. Оскільки програми розпізнавання обличчя можуть зберігати великі обсяги даних, важливо, щоб ці програми мали найвищий доступний рівень безпеки. Також важливо, щоб постачальники, які співпрацюють з замовниками послуг адміністрування систем, мали відповідні заходи безпеки, щоб уникнути будь-яких загроз кібербезпеки. Однак на даний час українське законодавство прямо не відносить зображення обличчя до персональних даних, які є захищеними на законодавчому рівні. Тому, на відміну від адміністрування паспортних даних, адміністратори систем відеоспостереження не мають значного інтересу у захисті такої інформації. Зазначена ситуація підлягає корегуванню як на законодавчому рівні, так і на рівні розробників систем.

Нейтральність та біас. Алгоритми розпізнавання обличь можуть бути піддатливими до біасів через неправильне навчання, недостатність різноманітності та репризентативності даних, неправильне навчання моделей, тощо.

Регулювання та законодавство. Дуже важливий аспект, який має бути ретельно розглянутим та опрацьованим. Наявність чіткого законодавства та ругулювання для використання цих технологій дуже важлива для їх впровадження в життя, продуктивності та запобігання можливих щловживань.

Проте, крім основних зазначених аспектів, слід звернути увагу і на численні інші проблеми, які виникають внаслідок застосування відеокамер з функцією розпізнавання обличчя. Ключовими серед них є:

можливість незаконного комерційного використання даних (як-от, рекламний таргетинг, зокрема, і політичний);

ризики дискримінації осіб через позитивні/негативні хиби системи, наявність інституційної дискримінації в суспільстві та подальшу її конвертацію в алгоритми системи;

ризики неправомірного притягнення осіб до відповідальності, коли система неправильно співвідносить людину з зображенням (що вже трапилося у практиці Сполучених Штатів [4]);

проблема статусу такої інформації як доказу у суді (зокрема, через відсутність правового регулювання);

ймовірність порушення права на свободу вираження поглядів у частині захисту журналістських та адвокатських джерел;

загрози для належної реалізації права на мирні зібрання (в тому числі створення «охолоджуючого ефекту» для активістів через страх

притягнення до відповідальності внаслідок участі у мітингах, демонстраціях, протестах);

можливість зловживань і використання систем для політичних переслідувань з боку держави, утисків вразливих та маргіналізованих груп тощо [5].

Найближчі 15–20 років наша держава може повністю перейти на біометричні паспорта та використання біометричних даних для ідентифікації особи. Звичайно під швидкий розвиток технологій потрібно буде розроблювати законодавчу та нормативно-правову базу для їх застосування, дотримання прав і безпеки громадян. Якраз більшість побоювань що до використання систем автоматичної ідентифікації облич пов'язано лише з відсутністю належного регулюючого законодавства та якісного підходу до роботи з такими технологіями. Закони про захист персональних даних прийняті вже в більшості країн Європи та дозволяють вже частково вирішувати дану проблему. Нашій країні ніщо не заважає застосовувати їх позитивний досвід у себе. Ще одним з факторів забезпечення безпеки запровадження таких систем є грамотний підхід до їх розгортання з використанням технологій шифрування протягом усього процесу, а персональні дані мають бути знеособлені.

Використання передового досвіду технологічно розвинених країн у розвитку систем автоматичного розпізнавання облич з пристосуванням його до реалій нашої держави, могло б значною мірою сприяти покращенню профілактики, розслідування та розкриття злочинів в нашій країні.

Список використаних джерел:

1. Hartwig B. The Benefits and Drawbacks of Automated Facial Recognition in Forensic Science [Електронний ресурс] / Ben Hartwig. URL: https://bit.ly/3NVKD8w

2. Статистичні данні Генеральної прокуратури України [Електронний ресурс]. URL: https://bit.ly/3aT6fDS

3. Загальний регламент про захист даних (GPDR). Офіційний переклад українською мовою [Електронний ресурс] URL: https://gdpr-text.com/uk/

4. Kashmir Hill. Wrongfully Accused by an Algorithm. *The New York Times*. June 24, 2020 P. A1.

5. Центр демократії та верховенства права: Чи легально встановлювати на міських вулицях камери із системою розпізнавання облич? URL: https://bit.ly/3xVfE6X

Лариса Тарнавська
аспірантка, молодший науковий співробітник Відділу дослідження проблем кримінального процесу та судоустрою Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

НАУКОВО-ТЕХНІЧНІ ЗАСОБИ КРИМІНАЛІСТИКИ: СУТНІСТЬ ТА ЗМІСТ

Криміналістика – інноваційна наука, яка використовує досягнення науки і техніки у протидії злочинності. З самого початку формування криміналістики її рекомендації стосувалися лише «поліцейської техніки». 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.

На сьогодні в криміналістиці використовуються різні поняття: «науково-технічні засоби», «техніко-криміналістичні засоби», «технічні засоби», «техніко-криміналістичні прийоми», «науково-дослідна техніка» та ін. Не зважаючи на схожість застосованої термінології, ці поняття певним чином відрізняються за своїм змістом. На нашу думку, більш широкою є категорія «науково-технічні засоби».

Традиційно в криміналістиці «науково-технічні засоби» визначаються як прилади, пристосування та матеріали, які використовуються для збирання, дослідження та використання доказів або створення умов, що ускладнюють вчинення злочинів (кримінальних правопорушень) [1, с. 47]. У цьому сенсі всі науково-технічні засоби поділялися на ті, що отримані без змін із різних природничо-технічних наук; ті, що спеціально прилаштовані для цілей криміналістики; ті, що спеціально розроблені для криміналістичних чи експертних цілей.

Досить важливим має бути й те, що розроблювані й пропоновані науково-технічні засоби мають використовуватися в діяльності різних суб'єктів – оперативних співробітників, слідчих, дізнавачів, детективів, прокурорів, суддів, адвокатів. Тобто, не лише в слідчій діяльності та розшуковій діяльності, а й у діяльності суду (сторони обвинувачення та сторони захисту).

Вивчення літературних джерел та практики правозастосування свідчить про те, що до науково-технічних засобів мають бути віднесені інноваційні (інформаційні) технології. Мова йде про використання у криміналістичних цілях різного роду баз знань, баз даних, криміналістичних обліків, комп'ютерних програм, інформаційних, інформаційно-аналітичних, інформаційно пошукових систем тощо. Останнім часом для практичних співробітників органів правопорядку та суду пропонуються Автоматизовані робочі місця (АРМ) (наприклад, АРМ слідчого, АРМ детектива, АРМ дізнавача, АРМ прокурора, АРМ судді, АРМ судового експерта та ін.). Окрім того, важливого значення набувають бази даних «Практика слідчого» (Свідоцтво №49389 про реєстрацію авторського права на твір від 30 травня 2013), «Слідчий прецедент» (Свідоцтво №60084 про реєстрацію авторського права на твір від 9 червня 2015) та ін. [2, с. 11–26].

Деякі науковці справедливо вказують, що до технічних (або науково-технічних) засобів, що застосовуються у кримінальному провадженні відносяться «технічні, програмно-технічні та програмні засоби, спеціальні пристрої, автоматизовані системи, речовини та обґрунтовані способи та прийоми їх використання…» [3, с. 133–135].

Важливою ознакою використання науково-технічних засобів в криміналістиці постає її мета. Тому, на наше переконання, слід виходити з того, що такі науково-технічні засоби можуть використовуватися не лише під час збирання, дослідження, та використання доказів, а й під час їх оцінки. Зрозумілий акцент того, що науково-технічні засоби можуть використовуватися під час збирання, дослідження та використання доказової інформації, а також «для створення умов, що утрудняють учинення злочинів» (В. Ю. Шепітько, В. В. Пясковський та ін.). Однак, на нашу думку, перспективним постає їх використання й під час оцінки доказів, що особливо виявляється в перспективах застосування штучного інтелекту (ШІ) [4, 5, 6], коли прийняття оцінка доказів та прийняття рішення буде здійснюватися з елементами ШІ, відповідної програми та науково-технічного засобу. На сьогодні використанню ШІ у протидії злочинності приділялася окрема увага і відбувалося обговорення актуальних проблем його впровадження [7].

У учасних умовах в криміналістиці та судовій експертизі значна увага приділяється інноваційним підходам, інноваціям та інноваційним продуктам. У літературних джерелах було аргументовано, що зміст тер-

міна «інновації в криміналістиці дещо відрізняється від сутності поняття «науково-технічні засоби в криміналістиці» та є значно ширшим. Інноваціями в криміналістиці є «розроблені та впроваджені в практику нові сучасні методи, прийоми, технології, технічні засоби, прилади, апаратура, інструменти, метою яких є оптимізація розслідування злочинів (судового розгляду), підвищення якості та ефективності правозастосовної діяльності і зменшення помилок» [8, с. 337, 338; 2, с. 11–26].

Список використаних джерел :

1. Шепітько В. Ю. Криміналістика: підручник. Київ: Ін Юре, 2010. 496 с.
2. Шепітько В. Ю., Авдєєва Г. К. Проблеми застосування науково-технічних засобів та інноваційних продуктів у діяльність органів правопорядку. *Теорія та практика судової експертизи і криміналістики.* 2019. № 20. С. 11–26.
3. Рогатинська Н. З. Використання та фіксування науково-технічних засобів у розшуковій діяльності слідчого. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право».* 2017. Вип. 24. С. 133–135.
4. 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;
5. 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$;
6. 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
7. Використання технологій штучного інтелекту у протидії злочинності: матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків: Право, 2020. 112 с. URL: https://ivpz.kh.ua/wp-content/uploads/2020/12/Матеріали-семінару_Використання-техн-штучного-інтел_5.11.2020.pdf
8. Шепітько В. Ю. Авдєєва Г. К. Інновації в криміналістиці. *Велика українська юридична енциклопедія: у 20 т. Т. 20: Криміналістика, судова експертиза, юридична психологія /* редкол.: В. Ю. Шепітько (голова) та ін. Харків: Право, 2018. 952 с.

Валерій Тіщенко
доктор юридичних наук, професор, професор кафедри криміналістики, детективної і оперативно-розшукової діяльності Національного університету «Одеська юридична академія», м. Одеса, Україна

ТЕХНОЛОГІЧНІ ТА ЕВРИСТИЧНІ АСПЕКТИ У РОЗСЛІДУВАННІ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

В історії криміналістики спостерігались різні підходи до характеристики діяльності з розкриття і розслідування злочинів. До 19-го століття злочин розглядався як таємниця, осягнути яку можливо лише завдяки особливим здібностям, надприродної обдарованості, інтуїції слідчого, а розкриття злочину уявлялось як особливе мистецтво встановлення істини і викриття зловмисника. Але вже в другій половині 19-го – на початку 20-го сторіччя на основі науково-технічного прогресу того часу з'являються праці, в яких здійснюються спроби наукового підходу до аналізу слідчої діяльності, хоча в їх назвах використовуються ще терміни «мистецтво розкриття злочинів» (Е. Анушат), «Таємниця злочинця» (Г. Шнейкерт). Ганс Грос підкреслює, що праця слідчого не є мистецтво, а є мистецькою, майстерною діяльністю [1, с. 13], яка повинна базуватися на сучасних наукових знаннях. І дійсно, криміналістика стала в обґрунтуванні своїх техніко-криміналістичних, тактичних і методичних рекомендацій використовувати наукові положення багатьох природничих, суспільних і технічних наук, що сприяло підвищенню ефективності розслідування.

Раціоналізація і наукова організація праці на виробничих підприємствах призвели до ідеї використання технічних правил, організаційних процедур у кримінальному провадженні, говорити про «техніку розслідування» (В. У. Громов, І. М. Якимов). Фактично в їх працях можна побачити зачатки тих підходів до характеристики розслідування, який значно пізніше став визначатися як технологічний підхід.

Розвиток і досягнення кібернетики в 70–80 роки минулого століття дозволили створювати криміналістичні програми і алгоритми розслідування різних видів (підвидів) злочинів. Дійсно, типізація слідчих ситуа-

ції, як на початковому, так і подальшому етапах розслідування відкривало можливості для чіткої постановки тактичних завдань і алгоритмів їх вирішення. Таким чином утворювалась конкретна програма розслідування, що сприяла оптимальній організації розкриття злочину у кримінальному провадженні. Всі ці наукові пошуки призвели до появи і розвитку *технологічного підходу* у криміналістиці, а також слідчих і експертних технологій у практиці розслідування злочинів [2, с.3–7; 3, с.22–23, 4, с.22, та ін.]. З практичної точки зору криміналістичні технології утворюють систему дій та процедур, що виконуються у певній послідовності для вирішення тих чи інших завдань розслідування [5, с.39]. Було запропоновано розмежовувати тактичні та технологічні аспекти розслідування, оскільки низка положень к проведенні слідчих дій включає в більшому чи в меншому співвідношенні не тільки тактичні *рекомендації*, але й *правила* технологічного характеру.

В. А. Журавель говорить про те, що у побудові криміналістичних методик розслідування повинні використовуватися технологічні підходи та й сама методика розслідування є «розумовий образ сукупності методів процесу (технології) розкриття і розслідування злочинів…» [6, с.98].

Всі названі зауваження щодо сутності і значення криміналістичних технологій як у формуванні і викладанні окремих розділів криміналістики, так і у розгляді слідчої діяльності безумовно резонні і заслуговують подальшої теоретичної розробки.

Втім не можна забувати про іншу сторону діяльності з розкриття і розслідування злочинів. Кожен злочин – це подія унікальна, яка виражає індивідуальні якості особи або комплекс таких якостей в організованій групі осіб. Це знаходить своєрідне відображення обставин злочину, особливих ознак його організатора і виконавців в обстановці і способах злочинного діяння, в характері зв'язку між всіма елементами його механізму та проявляється у наслідках такого діяння.

Розслідування ж являє собою процес специфічного пізнання сутності і обставин кримінально релевантної події, яке відзначається з одного боку суворою регламентацією процесуальних форм і засобів, а з іншою – пошуковим, творчим, індивідуальним підходом, що зумовлюється саме неповторністю кожної події злочину і тих психологічних характеристик, які уособлює його виконавець. Це означає, що не може бути якоїсь загальної та універсальної схеми, програми дій, які можна було б результативно застосовувати щодо всіх випадків, навіть типових, схожих,

слідчих і кримінальних ситуацій. Більше того, схожість ситуацій, обставин злочину, що розслідується, не повинна наводити слідчого на помилкову думку про безперечну аналогію минулої успішної діяльності. Уявна простота ситуації, що видається слідчому в такому випадку вводить його в оману і призводить до шаблонних дій і, нерідко, до глухої ситуації, коли він не може відгадати таємницю злочину і знайти методи його розкриття. Тому слідчому необхідно відшукати ту непримітну, приховану особливість, яка відрізняє конкретний випадок обставин злочинної події від попереднього і такого, здавалося б схожого. Визначення цієї особливості може підказати нові версії, вказати на зв'язки, які не були ним раніше виявлені, а між тим відіграють суттєву роль у справжніх обставинах події, вказують на причетних до злочину осіб, тобто веде до розкриття злочину.

Викладені зауваження можна віднести й до тактики і методики розслідування. Тактика слідчої дії характеризується не тільки її певними етапами і тактичними завданнями, алгоритмом дій, але й відшуканням і вибором таких тактичних прийомів, які б дозволили встановити психологічний контакт з кожним її учасником, зумовили його співпрацю зі слідчим, сприяли отриманню показань, в яких розкриваються справжні мотиви, наміри, цілі злочинця. Напружений і глибокий аналіз обставин події, поведінки підозрюваної особи, її зв'язків з іншими учасниками і причетними особами ведуть до пошуку нової або додаткової інформації, розробки нових версій та їх перевірки. У методиці розслідування велике значення має вибір напряму розслідування, пошукових дій, послідовності вирішення поставлених завдань, систематизація і оцінка доказів

Все це показує і визначає процес пізнання у розслідуванні злочинів як *евристичну*, *творчу* діяльність, що опирається на широкі наукові знання слідчого, його ерудицію, життєвий досвід, вміння вирішувати нестандартні завдання, знаходити і приймати правильні рішення в проблемних ситуаціях.

Сказане може викликати питання: що у розслідуванні більш важливе – знання і володіння технологією слідчої діяльності чи евристичний підхід до вирішення завдань розслідування? Можна прийти до висновку, що ці два аспекти у пізнавальній діяльності слідчого однаково значимі і потребують їх постійного поєднання, виваженого балансу у їх застосуванні при розв'язанні як тактичних, так і стратегічних задач розслідування.

Список використаних джерел :

1. Ганс Гросс. Руководство для судебных следователей как система криминалистики. Перепеч. с изд. 1906 г. М.: ЛексЭст, 2002. 1088 с.

2. Сегай М. Я., Стринжа В. К. Актуальні проблеми експертної технології в умова НТР. Криміналістика і судова експертиза. Київ, 1984.-Вип.29.

3. Тіщенко В. В. Криміналістичні технології в теорії і практиці розслідування. Актуальні проблеми держави і права, Вип.44. Одеса: Юрид. літ., 2008, с. 18–24.

4. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик: автореф. Дис…. д-ра юрид. наук: 12.00.09. Харків, 2011.

5. Тіщенко В. В., Барцицька А. А. Теоретичні засади і формування технологічного підходу в криміналістиці: монографія. Одеса: Фенікс, 2012.–198 с.

6. Журавель В. А. Криміналістичні методики: сучасні наукові концепції: монографія. Харків: Апостіль, 2012. 304 с.

,

Ярослав Фурман
кандидат юридичних наук, старший науковий співробітник, старший науковий співробітник науково-дослідної лабораторії з проблем криміналістичного забезпечення та судової експертології, навчально-наукового інституту № 2 Національної академії внутрішніх справ, м. Київ, Україна

ОСОБЛИВОСТІ ВИКОРИСТАННЯ БЕЗПІЛОТНИХ ЛІТАЛЬНИХ АПАРАТІВ ПІД ЧАС ОГЛЯДУ МІСЦЯ ПОДІЇ

Перед слідчим постає проблема використання своїх законних повноважень за обставин, що відрізняються від звичайної обстановки у його житті, а тому надання рекомендацій щодо застосування сучасних криміналістичних методів є актуальним і значущим в умовах триваючого сплеску злочинної діяльності. Крім того, для проведення негайного огляду місця події слідчий повинен застосувати низку сучасних технологій, у тому числі використання безпілотних літальних апаратів (БПЛА).

Огляд місця події – є найбільш складною, важливою і невідкладною слідчою дією, метою якої є виявлення слідів події злочину, обставин його вчинення та встановлення особи злочинця. Невідкладність огляду місця події пояснюється необхідністю своєчасно і швидко отримати інформацію про обставини події з метою організації розшуку злочинця, розкриття та розслідування злочину, ефективність огляду значною мірою залежить від додержання слідчим, прокурором спеціальних тактичних правил його проведення, використання необхідних сучасних науково – технічних засобів, належного процесуального оформлення як ходу огляду, так і отриманих результатів [1, с. 7].

Останнім часом великого поширення набули безпілотні літальні апарати (БПЛА). Здійснюючи політ заданого маршруту в автоматичному або в напівавтоматичному режимі, отримують точні та достовірні матеріали про особливості рельєфу місцевості, на якій будуть проводитися будівельні роботи, здійснюватиметься наземне лазерне сканування, відбуватиметься моніторинг стану автомобільних та залізничних доріг, аеропортів. Отримані матеріали цифрового аерофотознімання є основою для створення цифрових та електронних карт, складання топографічних

планів місцевості й можуть стати основою при складанні схем місця події. [2, с. 31].

В науці і техніці сформувалися і активно застосовуються деякі дефініції, які безпосередньо охоплюють досліджувану нами сукупність, серед яких слід виділити:

а) дрон (англ. drone – трутень) «безпілотний дистанційно-керований літальний апарат, оснащений відеозаписуючим пристроєм»;

б) квадрокоптер (іт. quattro – чотири + copter – літаючий) безпілотний дистанційно-керований літальний апарат, оснащений відеозаписуючим пристроєм, що має чотири мотори і чотири гвинтові механізму;

в) мультикоптер (англ. multi – багато + copter – літаючий) безпілотний дистанційно-керований літальний апарат, оснащений відеозаписуючим пристроєм, який має п'ять і більше моторів і відповідну кількість гвинтових механізмів [3, с. 37].

Цифрове аерознімання та вимірювання місцевості безпілотними апаратами на сьогоднішній день є актуальним та оптимальним розв'язанням більшості питань в галузі геодезії, картографії та маркшейдерії, тому виникла ідея щодо можливості застосування БПЛА у реєстрації та картографуванні місця події [2, с. 31].

Так, при проведенні огляду місця події на великій території, коли потрібно відтворити єдину картину, доцільно використовувати сучасні можливості застосування аеровідеозапису за допомогою використання в цих цілях БПЛА. Такий формат огляду дає можливість: отримати інформацію в короткі терміни, знаходитись стаціонарно, не застосовувати велику кількість людей до огляду прилеглої території, встановити точні координати місцевості, дозволить зробити аерофотознімок, на якому можна позначити, наприклад, місце виявлення трупа, а також інші позначення і долучити їх до матеріалів кримінального провадження. З розвитком БПЛА і програмного забезпечення до них, можливо «зависання» БПЛА на певній висоті, що невід'ємно дає значний плюс у використанні при огляді місця події, так слідчий може встановити БПЛА в «зависання» в підходяще, на його думку, місце для кращої фіксації і після вільно працювати з судмедекспертом, не відволікаючись на фото і відео фіксацію що відбувається при ОМП і при цьому отримати в кінці ОМП фото і відео фіксацію слідчої дії в високій якості. Можливо і пересування БПЛА в автоматичному режимі за об'єктом.

Завдання БПЛА не обмежуються тільки фото і відео фіксацією. Так, за допомогою методу аерозйомки можна побудувати 3D модель поверхні і відтворити 3D реконструкцію на основі відеопослідовності [4]. Такий підхід до реконструкції поверхні не вимагає додаткових витрат на спеціалізоване обладнання, так як БПЛА обладнані камерами високої якості зображення, системою глобального позиціонування (GPS, GNSS або Galileo) [5], а також системою автоматичного управління і контролю висоти. Всі ці компоненти є базовою комплектацією більшості БПЛА.

Підсумовуючи викладене, зазначимо, що успішне проведення огляду місця події є базисом для об'єктивного розслідування злочинів, а тому використання новітніх технічних засобів є необхідним для повного фіксування всіх обставин події.

Список використаних джерел :

1. Огляд місця події: процесуальні особливості, криміналістичні рекомендації. Науко-практичний посібник для слідчих, прокурорів, поліцейських патрульної та кримінальної поліції. – Харків: 2018. – С. – 7.

2. Атаманенко Ю. Ю. Геоінформаційна технологія реєстрації та картографування дорожньо-транспортних пригод із використанням безпілотних літальних апаратів: моногр.; ДЮІ МВС України. Кривий Ріг, 2019. 132 с.

3. Бегалиев Е. Н. Современный толковый словарь криминалиста. Астана: Лантар-трейд, 2019. 240 с.

4. Bing Han, Christopher Paulson, Dapeng Wu. 3D Dense Reconstruction from 2D Video Sequence via 3D Geometric Segmentation. Journal of VisualCommunication and Image Representation. July 2011. Vol. 22, Issue 5, pp 421–431.

5. Galileo begins serving the globe. The European Space Agency. URL: http://www.esa.int/Applications/Navigation/Galileo_begins_serving_the_globe.

Одарка Чабанюк
кандидатка економічних наук, судовий експерт
лабораторії товарознавчих та економічних досліджень
Львівського науково-дослідного інституту судових експертиз
Міністерства юстиції України,
доцент кафедри обліку, контролю, аналізу та оподаткування
Львівського торговельно-економічного університету,
м. Львів, Україна

НАПРЯМИ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В СУДОВІЙ ЕКОНОМІЧНІЙ ЕКСПЕРТИЗІ

Для забезпечення повноти проведення експертного дослідження та точного визначення необхідного обсягу даних експерт-економіст повинен аналізувати не лише всі документи, що містять вихідну інформацію про об'єкти дослідження та процеси, а й розглядати численні взаємозв'язки між обліковими даними. З урахуванням великого обсягу досліджуваної та супутньої інформації важливим є використання сучасних комп'ютерів у експертному дослідженні, що дає можливість групувати початкові дані та аналізувати облікову інформацію на будь-якому рівні деталізації, враховуючи всі багаточисельні характеристики та зв'язки між досліджуваними документами. Щодо комп'ютеризації процесу економічних експертиз, наразі актуальність набувають завдання створення не експертних систем, що повністю заміщують роль людини, але інтерактивних систем гібридного інтелекту, що охоплюють комп'ютеризоване робоче місце експерта.

На певний період часу автоматизовані кількісні методики втратили свою популярність, і це обумовлено етапом комп'ютеризації, де визнається лідируюче положення експерта та надається пріоритет його спеціальним знанням. Комп'ютеризація процесу економічної експертизи означає часткову заміну роботи експерта-економіста інтерактивними системами. Створення таких інтерактивних систем, де методика формалізується, призводить до спроб кількісної оцінки значущості різних ознак. Однак цей підхід виявляє безліч недоліків та різних тлумачень, оскільки експерти, а часто й розробники методик, не завжди детально розглядали або узгоджували їхні особливості.

Поєднання праці експерта і комп'ютера можна розглядати як експертну систему, яка здатна виконувати різноманітні експертні завдання із більшою швидкістю, ніж це міг би робити тільки експерт. У такій системі кожна її складова може контролювати іншу. Комп'ютеризація економічної експертизи дозволяє звільнити експерта від типових помилок і швидко виконувати рутинну роботу, тоді як експерт відповідає за контроль над аспектами, які комп'ютер не здатний виконати. Впровадження комп'ютеризованих систем у експертну діяльність надає можливість усунути більшість типових помилок, що можуть виникати при проведенні економічної експертизи традиційним способом. Комп'ютеризація процесу економічної експертизи розвивається в кількох ключових напрямках:

1. Розробка експертних систем:

– створення програм, які можуть моделювати та реалістично відтворювати експертні рішення;

– розробка інтелектуальних алгоритмів для аналізу економічних даних та надання рекомендацій.

2. Використання автоматизації:

– застосування алгоритмів машинного навчання для автоматизації процесів виявлення та аналізу економічних ситуацій;

– розробка систем, які можуть вчитися на основі нових даних та адаптуватися до змін в економічному середовищі.

3. Інтеграція баз даних:

– об'єднання різних джерел економічної інформації для забезпечення повноти та точності даних для аналізу;

– розробка систем, які можуть автоматично оновлювати і підтримувати бази даних.

4. Візуалізація даних:

– створення інтерактивних інтерфейсів та візуалізацій для зручного представлення складних економічних даних;

– використання графіків та діаграм для легкого сприйняття та аналізу результатів.

5. Захист інформації:

– впровадження технологій кібербезпеки для забезпечення конфіденційності та цілісності економічних даних;

– розробка систем контролю доступу до важливої інформації та захист від несанкціонованого доступу.

Ці напрямки сприяють автоматизації та вдосконаленню економічної експертизи за допомогою сучасних технологій.

Використання універсальних апаратних засобів та загальнопризначеного програмного забезпечення, насамперед, орієнтованих на операційну систему Windows та стандартного програмного забезпечення для неї. Це включає в себе:

1. Операційна система Windows:

– використання універсальних апаратних ресурсів, оптимізованих під Windows, для забезпечення стабільної та ефективної роботи системи.

2. Стандартне програмне забезпечення для Windows:

– застосування програм, які є стандартними для операційної системи Windows, з метою забезпечення сумісності та ефективного використання функціоналу;

– використання універсальних інструментів, таких як Microsoft Office, для організації робочих процесів та обміну даними.

Це підходить для забезпечення стандартизації та ефективності в робочих процесах, спрощуючи інтеграцію та управління програмним та апаратним забезпеченням.

Системи підготовки текстів призначені для створення та редагування документів. Розповсюдженням користуються різні версії текстового процесора Microsoft Word. Використання комп'ютера для підготовки текстових матеріалів дозволяє виконувати низку функцій, таких як редагування готового тексту, монтаж нового документа із наявних фрагментів, швидке знаходження необхідних розділів, коригування орфографії, введення графічної інформації та інші операції.

Різні варіанти електронних таблиць Microsoft Excel представляють собою електронні аркуші, де можна вводити текстові символи та математичні формули, а розрахунки проводяться автоматично. Це особливо зручно при розслідуванні та перевірці точності заповнення фінансових документів. Також можна задавати взаємозалежність між різними значеннями; при зміні значень у одній клітинці автоматично відбувається їх заміна в інших, що з ними пов'язані. Створена електронна таблиця відразу стає документом, який легко використовувати, модифікувати та роздрукувати в необхідній кількості примірників.

Отже, використання універсальних та багатофункціональних програмних комплексів, які можуть вирішувати різноманітні типові екс-

пертні завдання, дозволяє підняти рівень ефективності економічної експертизи на якісно новий рівень.

Перелік використаних джерел :

1. Воронко Р. М., Чабанюк О. М. Особливості судово-бухгалтерської експертизи та окремі питання її нормативно-правового регулювання / Р. М. Воронко, О. М. Чабанюк, М. Ю. Чік, Воронко О. С. *Вісник Львівського торговельно-економічного університету*. Львів : Вид-во Львівського торговельно-економічного університету, 2022. Вип. 67. С. 13–20. DOI: ttps://doi.org/10.36477/2522-1205-2022-67-02. URL : http://journals-lute.lviv.ua/index.php/visnyk-econom/article/view/1142/1077

2. Інструкція про призначення та проведення судових експертиз та експертних досліджень: затверджена наказом Міністерства юстиції України від 08.10.1998 р. №53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705–98

Віктор Шевчук
доктор юридичних наук, професор,
провідний науковий співробітник НДІ вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України,
м. Харків, Україна

ЦИФРОВІ ТЕХНОЛОГІЇ ТА ЄВРОПЕЙСЬКИЙ ВЕКТОР РОЗВИТКУ КРИМІНАЛІСТИКИ ПІД ЧАС ВІЙНИ

Сучасний стан злочинності в Україні та її динаміка під час війни значно вплинули на зміну пріоритетів завдань криміналістики та особливості формування й застосування криміналістичних знань. Така ситуація створює додаткове навантаженням на судові і правоохоронні органи, які у посиленому режимі забезпечують охорону громадського порядку, слідчих, детективів і прокурорів, на яких покладається виявлення та документування фактів воєнних злочинів та їх наслідків, а також суддів, які у цих складних і небезпечних умовах забезпечують здійснення судового контролю за кримінальним провадженням і правосуддя [3, с. 73–77].

Одним із головних завдань України в реаліях сьогодення є відсіч збройної агресії РФ та поновлення порушених прав і свобод українських громадян, а також забезпечення принципу невідворотності відповідальності винних осіб у вчинені злочинів, пов'язаних із вторгненням російських загарбників на терени нашої країни. Докази та доказування – основа будь-якого процесу, і від того, наскільки якісно та повно під час досудового розслідування буде зібрана доказова база, залежить ефективність розгляду кримінального провадження в суді і швидкість досягнення мети правосуддя [2, с. 634]. За таких обставин необхідно враховувати, що для судового розгляду таких воєнних злочинів, зокрема, як для судів України, так і будь-якого міжнародного суду основоположним буде не тільки виявлення, збирання та документування доказів воєнних злочинів, але й встановлення причинно-наслідкового зв'язку між винними діями країни-агресора та наслідками, що настали, тобто заподіяною шкодою.

Головним завданням криміналістики в такій ситуації є розроблення та застосування засобів, прийомів та методів, що дозволяють збирати, досліджувати, використовувати доказову інформацію в умовах війни. У зв'язку із цим, гостро постало питання щодо створення та запрова-

дження ефективного захисту відносин, що забезпечують умови охорони основ національної безпеки України, як кримінально-правовими, кримінально-процесуальними, так і криміналістичного засобами [5, с. 12–27].

Криміналістика, інтегруючи сучасні досягнення науки і техніки, сьогодні спрямовує свій науковий потенціал на створення ефективної системи криміналістичних засобів, прийомів та технологій, застосування яких направлено на вирішення практичних завдань, серед яких особливу значимість набувають можливості застосування криміналістичних знань в умовах війни. Тому перед криміналістикою постають завдання, які пов'язані із забезпеченням діяльності органів правопорядку та інших спеціальних суб'єктів такої протидії ефективними криміналістичними рекомендаціями у виявленні та розслідуванні злочинів, пов'язаних з військовою агресією РФ проти України [4, с.14]. Вбачається, що в сучасних реаліях практика застосування криміналістичних знань та цифрових технологій для збирання доказів під час війни є досить актуальною.

В сучасних умовах особливого значення набувають можливості застосування криміналістичних знань, цифрової інформації у протидії злочинності в реаліях війни та наближення до єдиного криміналістичного європейського простору [1, с. 638]. Інтеграція України у світову та європейську спільноту вимагає адаптувати національне законодавство до міжнародних стандартів і зобов'язань. Особливо це стосується криміналістики та кримінального процесу як у сфері протидії злочинності, так і у сфері охорони важливих конституційних прав, свобод та інтересів громадян з урахуванням реалій розвитку українського суспільства.

Сьогодні в Україні також простежується зміна вектора криміналістичних та кримінально-процесуальних досліджень [4; 5], наближення його до єдиного європейського простору. Тому перед Україною, яка визначила курс вступу до ЄС одним із пріоритетних напрямів діяльності, постає завдання привести національне законодавство у відповідність до європейських стандартів (зокрема, у сфері протидії злочинності, здійснення судочинства, формування системи органів військової юстиції) [1, с. 19–26]. Розв'язання цього питання потребує відповідного законодавчого врегулювання й розроблення концепції криміналістичного забезпечення діяльності органів військової юстиції. Відтак, актуальним є формування та розвиток європейської криміналістики й інтеграції криміналістичних знань до єдиного європейського криміналістичного простору.

В умовах війни та сучасних євроінтеграційних процесів відбувається перезавантаження криміналістики, пов'язане передусім із появою нових викликів до системи кримінальної юстиції й потребою розв'язувати першорядні завдання під час активних бойових дій на території України. У таких умовах криміналістика покликана розробити новітні засоби, прийоми й методи, спрямовані на протидію воєнним злочинам, пов'язаним із військовою агресією РФ проти України та процесів цифровізації суспільства. Окремо необхідно розробляти системи криміналістичних методик розслідування, удосконалювати техніко-криміналістичне забезпечення, застосування спеціальних знань, захист інформаційних джерел та інформаційну безпеку в еру цифровізації під час війни. Можна констатувати, що сьогодні формуються нові наукові криміналістичні напрями – воєнна криміналістика та цифрова криміналістика [6, с. 795–822] .

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, розкриття та 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.

Отже, криміналістика в сучасних реаліях, інтегруючи сучасні досягнення науки й техніки, спрямовує свій науковий потенціал на створення ефективної системи криміналістичних засобів, прийомів і технологій, застосування яких покликано розв'язати складні практичні завдання [7], серед яких особливо значення набувають можливості застосування криміналістичних знань у протидії злочинності в реаліях війни. Відтак, розв'язання означених завдань передбачає запровадження ефективної системи протидії воєнним злочинам, пов'язаних із військовою агресією РФ проти України, активізації застосування цифрових технологій у кримінальному провадженні. При цьому важливого значення набуває реформування кримінального і кримінального процесу-

ального законодавства з врахуванням процесів цифровізації та на цій підставі вжиття системних заходів, спрямованих на удосконалення слідчої, детективної, експертної та судової практики в умовах сучасних євроінтеграційних процесів під час війни.

Список використаних джерел:

1. Богуцький П. П. Військова юстиція як правова система: міжнародні стандарти та національні особливості. *Діяльність військової юстиції в умовах збройного конфлікту. Досвід української прокуратури* : мат. міжнар. наук.-практ. конф. (Харків, 28.10.2021). Київ ; Одеса, 2021. С. 19–26.

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. 631–669.

3. Konovalova V. O., Shevchuk V. M. Digital criminalistics as a strategic direction of formation of criminalistic knowledge. *Advanced discoveries of modern science: experience, approaches and innovations*: collection of scientific papers «SCIENTIA» III International Scientific Conference. Amsterdam, 2023. Pp. 73–77.

4. Matulienė, S., Shevchuk, V., & Baltrūnienė, J. Artificial Intelligence in Law Enforcement and Justice Bodies: Domestic and European Experience. *Theory and Practice of Forensic Science and Criminalistics*, 29(4), 2023, 12–46.

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

6. Shevchuk V. M. Criminalistics support for the investigation of military criminal offenses and war crimes: digitalization, innovations, prospects. *Military offences and war crimes: background, theory and practice*: collective monograph. Ed. by V. M. Stratonov. Riga, Latvia: «Baltija Publishing», 2023. Pp. 795–822.

7. Шепітько В. Ю., Коновалова В. О., Шевчук В. М. та ін. Науково-технічне забезпечення слідчої діяльності в умовах змагального кримінального процесу. *Питання боротьби зі злочинністю.* 2021. Вип. 42. С. 92–102.

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

ВИКОРИСТАННЯ ІННОВАЦІЙНИХ ЗАСОБІВ ТА ЦИФРОВИХ ТЕХНОЛОГІЙ У КРИМІНАЛЬНОМУ ПРОВАДЖЕННІ

На сьогодні розвиток криміналістики та судової експертизи обумовлений науково-технічним прогресом світового співтовариства, впровадженням новітніх технологій у практику органів правопорядку та суду. У сучасних умовах воєнного стану в Україні та здійснення розслідування воєнних та інших злочинів міжнародного характеру важливого значення набуває використання інноваційних науково-технічних засобів, техніко-криміналістичних методів, прийомів та технологій. У цей період існує необхідність застосування найсучаснішої криміналістичної техніки (систем оптичної візуалізації, 3D сканерів, БпЛА (дронів, квадрокоптерів, мультікоптерів), мобільних ДНК-лабораторій), звернення до інформаційно-аналітичного та програмного забезпечення, автоматизованих робочих місць співробітників органів досудового розслідування та суду (наприклад, АРМ слідчого, АРМ прокурора, АРМ судді, АРМ експерта та ін.), автоматизованих інформаційно-пошукових систем та баз даних («Слідча практика», «Слідчий прецедент» та ін.) [1, с. 39–46], а також впровадження штучного інтелекту в діяльність правозастосовних органів.

Інформатизація, алгоритмізація та технологізація органів правопорядку та суду відбувається за допомогою впровадження інноваційних та цифрових технологій, 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 рі-

шень, 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.) [2, с. 126–133].

Значним досягненням є те, що в Україні запроваджуються інформаційно-телекомунікаційні системи: Єдина судова інформаційно-телекомунікаційна система (ЄСІТС) та Інформаційно-телекомунікаційна система досудового розслідування («іКейс»).

У сучасних літературних джерелах окремі науковці вказують, що «у національному правовому просторі виникли передумови та достатні підстави для впровадження концепції електронного кримінального провадження у реальну діяльність органів прокуратури та слідчих підрозділів органів Національної поліції України, а також поступової відмови від паперового документообігу у кримінальному процесі» [3, с. 159]. При цьому, у ч. 1 ст. 106–1 КПК України передбачено, що «інформаційно-телекомунікаційна система досудового розслідування – це система, яка забезпечує створення, збирання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні». Окрім того, у Положенні «Про інформаційно-телекомунікаційну систему досудового розслідування «іКейс»», затвердженому наказом Національного антикорупційного бюро України, Офісу Генерального прокурора, Ради суддів України, Вищого антикорупційного суду від 15 грудня 2021 р. №175/390/57/72 вказано, що метою Системи є автоматизація процесів досудового розслідування, включаючи створення, збирання, зберігання, пошук, оброблення і передачу матеріалів та інформації (відомостей) у кримінальному провадженні, а також процесів, які забезпечують організаційні, управлінські, аналітичні, інформаційно-телекомунікаційні та інші потреби користувачів Системи [4].

Під час розслідування можуть використовуватися також різного роду єдині реєстри (наприклад, єдиний реєстр судових рішень, єдиний реєстр юридичних осіб, фізичних осіб – підприємців та громадських формувань, реєстр методик проведення судових експертиз та ін.). Певним брендом цифрової держави в Україні («держава в смартфоні») визнано мобільний застосунок, веб-портал – «Дію».

Окремої уваги заслуговує розгляд питання щодо використання цифрової інформації у кримінальному провадженні (інформації, яка створена за допомогою високих інформаційних технологій). Така інформація

може створюватися, передаватися, зберігатися тощо не лише за допомогою комп'ютерної техніки, а й з використанням іншої апаратури (диктофонів, цифрових фотоапаратів, відеокамер, смартфонів та ін.) [5, с. 49].

У спеціальних джерелах широкого застосування набув термін цифрові докази («digital evidence»), під якими розуміють будь-які збережені дані або дані, що передаються з використанням комп'ютерної чи іншої техніки. Цифрові докази – це фактичні дані, що подані у цифровій формі та зафіксовані на будь-якому типі носія інформації [6, с. 259]. Цифровий доказ – інформація в електронній (цифровій) формі, що має значення для досудового розслідування та судового розгляду й надається стороною провадження (справи) для її оцінки слідчим, прокурором або судом. Для прийняття такої інформації у вигляді цифрового доказу можуть ставитися нормативні вимоги, передбачені законодавством (форма та зміст) [7, с. 129].

Необхідно звернути увагу на те, що у різних джерелах поряд із терміном «цифрові докази» використовуються й інші, наприклад: «електронні докази», «електронні сліди», «цифрові джерела інформації», «комп'ютерна інформація», «електронні документи» тощо. При цьому, зазначені терміни у більшості випадків використовуються як синоніми. Тому, окремі дослідники справедливо зазначають, що «за своєю суттю електронний доказ є цифровим об'єктом, який був засобом чи знаряддям вчинення кримінального правопорушення, зберіг електронно-цифрові сліди кримінального правопорушення, був предметом або об'єктом вчинення кримінального правопорушення або містить інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюються під час кримінального провадження» [8].

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

Цифрові докази вимагають новітніх підходів до їх збирання, зберігання, використання та дослідження під час доказування у кримінальному провадженні. Особливого значення цифрова інформація набуває під час розслідування воєнних злочинів і використання технологій розвідки на підставі відкритих джерел (Open Source Intelligence, OSINT). Прикладом можуть слугувати й положення «Протоколу Берклі» [9], які містять поради щодо фіксації цифрових доказів (цифрової інформації). При цьому, «інформація у відкритому доступі може надавати підказки, підтримувати результати розвідки та служити прямим доказом у судах» [10].

Список використаних джерел :

1. Шепітько В. Ю., Журавель В. А., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю:* зб. наук. праць. Харків: Право, 2011. Вип. 21. С. 39–46.
2. Шепітько В. Ю. Місце цифрових доказів та інституту доказування в доктрині криміналістики та судової експертизи. Інформаційне забезпечення розслідування злочинів: матеріали IX Міжнародного круглого столу (4 червня 2021 р.). Одеса: Вид. дім «Гельветика», 2022. С. 126–133.
3. Мазурик Р. В. Актуальні питання реалізації концепції електронного кримінального провадження у діяльності органів прокуратури: адміністративно-правовий аспект. *Право і суспільство.* 2022. № 1. С. 156–163.
4. Положення «Про інформаційно-телекомунікаційну систему досудового розслідування «iКейс»». URL: https://zakon.rada.gov/laws/ahow/v0390886-21#Text
5. Семко М. О., Крахмальов О. В. Електронна інформація як докази. *Вісник Національного технічного університету «ХПІ». Серія: Актуальні проблеми розвитку українського суспільства.* 2021. № 1. С. 48–51.
6. Цехан Д. М. Цифрові докази: поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Юрипруденція.* 2013. Вип. 5. С. 256–260.
7. Шепітько В., Шепітько М. Кримінальне право, криміналістика та судові науки: енциклопедія. Харків: Право, 2021. 508 с.
8. Козицька О. Г. Щодо поняття електронних доказів у кримінальному провадженні. *Юридичний науковий електронний журнал.* 2020. № 8. URL: https://lsej.org.ua/8_2020/105.pdf
9. ООН. Права человека. Управление Верховного Комиссара. *Протокол Беркли по ведению расследований с использованием открытых цифровых*

данных. Практическое руководство по эффективному использованию открытых цифровых данных при расследовании нарушений международного уголовного права прав человека и международного гуманитарного права. URL: https://www.ohchr.org/ru/publications/policy-and-methodological-publications/berkeley-protocol-digital-open-source

10. Протокол Берклі з ведення розслідування з використанням відкритих цифрових даних. URL: https://www.law.berkeley.edu/wp-content/uploads/2022/03/Berkeley-Protocol-Ukrainian.pdf

Вікторія Яремчук
кандидатка юридичних наук, старший науковий співробітник,
Науково-дослідний інститут вивчення проблем злочинності
імені академіка В. В. Сташиса НАПрН України, м. Харків, Україна

ДОСЛІДЖЕННЯ ЦИФРОВОЇ ІНФОРМАЦІЇ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

В світі сьогодні поширеним видом інформації є цифрова інформація. Усе більше даних зберігається в цифровому форматі. З'явилися нові види кримінальних правопорушень, що мають умовну назву «кіберзлочини». Тому актуальними є проблеми щодо використання цифрової інформації як доказів у кримінальному процесі [1, с. 568].

Невирішеними на сьогодні залишається низка практичних проблем, пов'язаних із поводженням з електронною слідовою інформацією, призначенням комп'ютерно-технічної експертизи, використанням її результатів у розслідуванні. З огляду на особливості інформації, що зберігається на електронних носіях має бути гарантоване її збереження під час усього кримінального провадження, в тому числі у випадках, коли електронний носій залишається у законних власників [2, с. 22].

До проведення огляду комп'ютерних носіїв необхідно запрошувати спеціалістів. Вони нададуть слідчому допомогу у вилученні саме необхідної електронної інформації. На практиці при проведенні слідчих (розшукових) дійй слідчими вилучаються значні обсяги інформації, всі електронні документи, які є на комп'ютері. Надалі при проведенні комп'ютерно-технічної експертизи експерту необхідно витратити велику кількість часу, щоб продивитися всі вилучені файли, та з них обрати невелику кількість необхідних для проведення судової експертизи. Особливо це відбувається при дослідженні відеозаписів, коли судовому експерту необхідно на відео виділити лише декільна хвилин відеозапису для проведення судової експертизи. Як зазначено в «інформаційному листі про підготовчі заходи та алгоритм дій при призначенні комп'ютерно-технічної експертизи» під час залучення експерта для проведення комп'ютерно-технічної експертизи допускаються такі помилки: експерту надаються об'єкти, які не містять електронної інформації; однією постановою призначається судова експертиза щодо різних видів об'єктів, таких як сервери, планшети, мобільні телефони тощо; призначаються

експертизи з великим обсягом досліджуваних даних і великою кількістю об'єктів, що потрібно одночасно досліджувати; експертові надаться об'єкти, щодо яких неможливе дослідження – відсутніми відповідними програмами для дослідження-драйверами, без елементів живлення [3, с. 2]. Таким чином, дослідження електронної інформації нині є поширеним видом судових експертиз. Необхідне залучення відповідних спеціалістів для виявлення, фіксації, вилучення електронної інформації при проведенні слідчих (розшукових) та негласних слідчих (розшукових) дій. На практиці є типові помилки , що допускаються при підготовці матеріалів для даного виду судової експертизи. Тому необхідно отримувати консультації спеціаліста при залученні судового експерта для проведення комп'ютерно-технічної експертизи.

Список використаних джерел :

1. Кириченко А. І. Актуальні проблеми використання цифрової інформації як доказу в кримінальному процесі. Юридичний науковий електронний журнал. Вип. 4. 2023. С. 567–569.

2. Климчук М. П., Комісарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп'ютерно-технічна експертиза у кримінальному провадженні : навч. посіб. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с. URL : https://dspace.lvduvs.edu.ua/bitstream/1234567890/4399/1/Судова%20к-т%20експертиза…%20--верстка.pdf

3. Інформаційний лист про підготовчі заходи та алгоритм дій при призначенні комп'ютерно-технічної експертизи. Київ, 2017. URL : file:///C:/Users/LG/Downloads/Інформ.лист_підготовчі-дії-КТЕ-2017.pdf

Наукове видання

ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ У КРИМІНАЛІСТИЦІ ТА СУДОВІЙ ЕКСПЕРТИЗІ

Збірник матеріалів міжнародного науково-практичного круглого столу

м. Харків, 11 грудня 2023 року

Електронне наукове видання

Видається в авторській редакції

Комп'ютерна верстка *А. Т. Гринченка*

Підписано до поширення через мережу Інтернет 22.02.2024.
Відповідає формату друкованого видання 60×84/16.
Обл.-вид. арк. 7. Об'єм даних 3,1 Мб

ТОВ «Видавничий дім «Право»,
вул. Харківських Дивізій, 11/2, м. Харків, Україна
Для кореспонденції: а/с 822, м. Харків, 61023, Україна
Тел.: (050) 409-08-69, (067) 574-81-20, (063) 254-50-84
Вебсайт: https://pravo-izdat.com.ua
E-mail для замовників послуг: verstka@pravo-izdat.com.ua
E-mail для покупців: sales@pravo-izdat.com.ua
Свідоцтво суб'єкта видавничої справи ДК № 8024 від 05.12.2023