1. Лисько Т.Д., Левченко А.С. Компетенція правоохоронних органів під час дії правового режиму воєнного стану. *Дніпровський науковий часопис публічного управління, психології, права.* 2023. № 2. С. 121–125.

2. Про Національну поліцію: Закон України від 02.07.2015 р.

3. Муляр Г.В. Діяльність органів Національної поліції України в умовах правового режиму воєнного стану. *Науковий вісник Міжнародного гуманітарного університету.* 2023. № 61. С. 130–133.

4. Звіт Національної поліції України про результати роботи у 2023 році URL: www.npprod/sites/1/Docs/Dialnist/Richni_zvity/zvit_NPU_2023.pdf.

5. Про основи національного спротиву: Закон України (Відомості Верховної Ради (ВВР), 2021, № 41, ст.339) URL: https://zakon.rada.gov.ua/laws/show/1702-20#Text.

Бурнос Олена Олександрівна,
аспірант науково-дослідної лабораторії з проблем криміналістичного забезпечення та судової експертології ННІ № 2 Національної академії внутрішніх справ

ЦИФРОВІ ДЖЕРЕЛА ДОКАЗОВОЇ ІНФОРМАЦІЇ ПІД ЧАС РОЗСЛІДУВАННЯ ВОЄННИХ ЗЛОЧИНІВ

У контексті дослідження особливостей початкового етапу розслідування воєнних злочинів важливого значення набуває аналіз джерел інформації про вчинення таких кримінальних правопорушень, що в подальшому слугуватимуть основою для формування доказової бази даних проваджень.

О. М. Дуфенюк виокремлює чотири основні групи джерел значущої інформації про воєнні злочини: особистісні джерела (показання свідків, потерпілих, підозрюваних (полонених) про обставини події); речові джерела (матеріальна обстановка, місця руйнувань, залишена техніка, речі, зброя, боєприпаси, вибухонебезпечні об’єкти, які не детонували, фрагменти боєприпасів, трупи з ознаками насильницької смерті; сліди біологічного походження у випадках катувань, зґвалтувань; матеріали та речовини (ґрунти, вода тощо), що засвідчують факти застосування забороненої зброї, факти забруднення екосистеми небезпечними речовинами тощо); цифрові джерела (матеріали фото-, відеофіксації подій, дані електронних, комп’ютерних та телекомунікаційних мереж, дані геолокації засобів, оснащених GPS-маяками, дані з відкритих джерел цифрової інформації і т. д.); документальні джерела (протоколи,

розпорядження, накази, розпорядження, плани проведення військових операцій, замовлення на постачання, особисті документи комбатантів, фінансові документи тощо) [1, с. 372].

Необхідно зауважити, що наразі особливого значення набувають цифрові джерела інформації. Дійсно, у воєнних реаліях, коли проблема збирання доказів постала вкрай гостро, центральне місце у формуванні доказової бази, зокрема і у досліджуваних провадженнях, посіли цифрові технології та технології штучного інтелекту (ШІ).

Вчені відзначають, що застосування технологій ШІ може бути корисним для ефективного розслідування воєнних злочинів в Україні та у зборі доказів їх вчинення. Такі сучасні технології можуть допомогти встановити винних і притягти їх до відповідальності. Основними напрямками, в яких може бути використані технології ШІ, виокремлюють наступні:

1) аналіз супутникових знімків та геолокаційних міток. Інструменти ШІ можуть допомагати аналізувати великі обсяги супутникових знімків для виявлення змін у ландшафті, зокрема будівель, доріг, об'єктів інфраструктури, які можуть бути пов'язані з воєнними злочинами. Вони можуть також допомогти в ідентифікації місць, де можуть бути поховані тіла жертв воєнних злочинів;

2) аналіз відео- та фотоматеріалів. Застосування технологій ШІ можуть бути використані для аналізу великого обсягу відео- та фотоматеріалів, які були зняті на місці воєнних злочинів. Такі технології можуть допомогти в ідентифікації потерпілих та свідків, а також встановити, чи були зображені деякі об'єкти, які можуть мати важливість для розслідування; можуть ідентифікувати воєнних злочинців;

3) обробка аудіоматеріалів. ШІ може допомогти в обробці аудіоматеріалів, наприклад, записів телефонних розмов, які можуть мати важливість для розслідування воєнних злочинів. Застосування таких технологій може допомогти в ідентифікації голосів та визначенні місць, де були здійснені розмови;

4) аналіз соціальних мереж. Технології ШІ можуть допомогти в аналізі соціальних мереж для виявлення зв'язків між підозрюваними та іншими особами, які можуть бути пов'язані з воєнними злочинами. Він може також допомогти в ідентифікації осіб, які можуть бути свідками воєнних злочинів або мати інформацію про них;

5) аналіз даних з медичних закладів. Інструменти цифрової криміналістики і ШІ можуть допомогти в ідентифікації тіл жертв воєнних злочинів, встановленні причини смерті, ідентифікації

військовополонених, військових злочинців та їх пошук за даними про хворобу та відомостями про їх ідентифікаційні ознаки, які допомагають встановленню конкретної особи;

6) розпізнавання облич. Технології ШІ можуть бути використані для розпізнавання облич на фото та відео з місць вчинення воєнних злочинів. Це може допомогти в ідентифікації підозрюваних, причетних до вчинення таких злочинів, та встановленню свідків, які можуть повідомити важливу інформацію про розслідувану подію воєнного злочину;

7) використання безпілотних літальних апаратів (квадрокоптерів). Враховуючи специфіку місця події таких злочинів, застосування квадрокоптерів для аерофото-відеозйомки у небезпечних або важкодоступних місцях, на великих площах території, стає сучасним технічним засобом фіксації слідів злочинної діяльності;

8) аналіз текстової інформації. ШІ може бути використаний для аналізу текстової інформації, наприклад, повідомлень в соціальних мережах та інших джерелах, що можуть бути пов'язані з воєнними злочинами. Він може допомогти в ідентифікації підозрюваних та свідків, а також встановленні криміналістично значущої інформації про воєнні злочини, які розслідуються [2, с. 34–35].

Докладний перелік джерел отримання доказової інформації про воєнні злочини пропонується у посібнику, підготовленому фахівцями НАВС. У виданні, зокрема, розглядаються наступні джерела:

– запити (ГШ ЗСУ, оперативно-тактичному угрупованню (командуванню) ЗСУ, командуванню Повітряних сил ЗСУ, штабу ООС, ГУР МОУ, СБУ, СЗРУ, ДПСУ, НГУ) щодо відомостей про: персональні дані осіб, які входять до підрозділів збройних сил та інших військових формувань рф; підрозділи збройних сил та інших військових формувань рф, які перебували на певній місцевості під час бойових дій; інформації щодо полонених ЗС та інших військових формувань рф; інформації щодо полонених військовослужбовців ЗСУ та інших осіб, які беруть участь у протидії збройній агресії рф, а також цивільних осіб, яких незаконно утримують тощо;

– тематичні телеграм-боти, а також мобільні додатки **(**STOP Russian War (@stop_russian_war_bot, Народний месник (@ukraine_avanger_bot, єВорог (@evorog_bot, Знайти зрадника (@Traitor_Search_bot, мобільний додаток BACHU та ін.*)*;

– підсистеми інформаційно-телекомунікаційної системи «Інформаційний портал Національної поліції України» (ІПНП), зокрема інформаційні підсистеми «АРМ 102», «Єдиний облік», «Особа», «Гарпун», «Воєнний злочинець» та ін.;

– вивчення відкритих джерел (OSINT), завдяки яким є можливість знаходити фотозображення осіб, причетних до злочинної діяльності, для подальшого їх впізнання очевидцями, встановлювати власників абонентських номерів мобільного зв'язку, які були зафіксовані на певних територіях, виявляти фото- та відеодокази протиправної діяльності, встановлювати повні анкетні відомості особи, якій повідомляють про підозру [3, с. 189–193].

На сьогодні в Україні та в інших країнах функціонують декілька платформ для фіксації злочинів, скоєних російськими військовими в Україні. Зокрема, база даних «Книга катів українського народу», інформаційний ресурс Української Гельсінської Спілки з прав людини, база даних «T4P (Трибунал для Путіна)», створена Офісом Генерального прокурора України спільно з компанією «IT Defends», національна платформа WarCrimes.gov.ua, аналітична база даних «Воєнні злочинці рф», створена Агентством Європейського Союзу з питань судового співробітництва (Євроюстом), міжнародна централізована база доказів міжнародних злочинів (CICED) та ін. Для захисту та представництва України в Європейському суді з прав людини та Міжнародному суді ООН функціонує міжурядова платформа для збирання та аналізу інформації про порушення прав людини військовими рф. Однак варто пам'ятати, що накопичена в базах даних цифрова інформація не завжди може використовуватися в кримінальному провадженні як доказ навіть у випадках, коли в ній зафіксований факт вчинення злочину [4, с. 34].

Найбільш поширеним та втім не менш важливим джерелом інформації про досліджувані злочини є дані з мобільних телефонів. Однак, слід враховувати, що така інформація може бути включена до доказової бази лише за умови її виявлення, вилучення, дослідження і процесуального закріплення відповідно до встановлених законодавством вимог. Для якісного виконання цих завдань залучаються спеціалісти в IT-сфері, які за допомогою сучасних портативних апаратно-програмних комплексів «Cellebrite UFED Touch 2 Ultimate» та «Cellebrite UFED 4 PC PhysicalAnalyzer» виявляють, декодують і аналізують цифрові дані, отримані з мобільних телефонів. Зокрема, 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 месенджерівViber, 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 [5, с. 71]. Аби дослідити цю інформацію і трансформувати її в процесуальні джерела доказів необхідно залучати судового експерта відповідно до ч. 1 ст. 243 КПК України.

Таким чином, для забезпечення ефективного розслідування воєнних злочинів в умовах сучасного технологічного середовища виняткового значення набуває використання здобутків так званої цифрової криміналістики, предметом якої є розроблення та застосування інноваційних засобів, прийомів і методів, що уможливлюють ефективний збір, дослідження, використання під час досудового розслідування й судового розгляду цифрових доказів.

Список використаних джерел

1. Дуфенюк О. М. Розслідування воєнних злочинів: логістичні, криміналістичні та судово-медичні питання. *Юридичний науковий електронний журнал*. 2022. № 4. С. 369–374.

2. Матуєлене С., Шевчук В., Балтрунене Ю. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. *Теорія та практика судової експертизи і криміналістики.* 2022. Вип. 4 (29). С. 12–46. URL: https://khrife-journal.org/index.php/journal/article/
view/547/617

3. Кваліфікація та розслідування порушення законів і звичаїв війни : наук.-практ. посіб. / А. А. Вознюк, І. В. Жук, О. В. Таран, С. С. Чернявський та ін.; за заг. ред. В. В. Чернєя, М. С. Цуцкірідзе, А. А. Вознюка. Київ : Норма права, 2023. 326 с.

4. Авдєєва Г. К. Проблеми визначення достовірності цифрових доказів у кримінальному провадженні. *Вісник Луганського навчально-наукового інституту імені Е.О. Дідоренка.* № 1. 2024. С. 33–48. DOI: https://doi.org/10.33766/2786-9156.105.33-48.

5. Кобець М. В. Апаратно-програмний комплекс «CellebriteUfed» 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.) / редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін. Київ : Нац. акад. внутр. справ, 2023. С. 70–73.