

УДК 343.982
DOI <https://doi.org/10.32782/pyuv.v6.2024.22>

В. С. Бондар

orcid.org/0000-0003-1552-4555

*кандидат юридичних наук, професор,
завідувач кафедри кримінального процесу та криміналістики
Навчально-наукового гуманітарного інституту
Національної академії Служби безпеки України*

В. Ю. Парфьонов

orcid.org/0000-0002-0482-853X

*начальник відділу приймання, опрацювання
та аналізу оперативної інформації управління нагляду за додержанням законів
Національною поліцією України та органами, які ведуть боротьбу зі злочинністю
Луганської обласної прокуратури*

ПРО ОСОБЛИВОСТІ ЗАСТОСУВАННЯ НОВІТНІХ ТЕХНОЛОГІЙ У ДОКУМЕНТУВАННІ ТА РОЗСЛІДУВАННІ ОКРЕМИХ ВИДІВ ВОЄННИХ ЗЛОЧИНІВ

Постановка проблеми. Серед злочинів, учинених в період повномасштабного вторгнення РФ до України воєнні злочини взагалі та воєнні злочини зокрема, а саме порушення законів і звичаїв війни, передбачені ст. 438 Кримінального кодексу України (далі – КК України) є найбільш складними в сенсі документування та розслідування. Суттєвим чинником цього є заходи протидії, котрі вживаються фігурантами даних проваджень: приховання зовнішності, припинення катувань за певний період до обміну задля усунення тілесних ушкоджень відповідного характеру тощо, а також певні недоліки документування зазначених кримінально-правових деліктів. Зазначене актуалізує необхідність пошуку співробітниками органів правопорядку нових шляхів документування та розслідування злочинів даної категорії.

Стан дослідження. Питання використання новітніх досягнень науки і техніки під час досудового розслідування кримінальних правопорушень перебували та перебувають у фокусі уваги таких учених: Г.К. Авдеева [1, с. 33–48], Л.І. Аркуша, Д.С. Афонін, О.П. Бабіков [2], Т.В. Будко, А.В. Ватраль, О.І. Дроздов, О.М. Дуфенюк [4], І.В. Гловюк, В.Г. Гончаренко, І.В. Гора, В.А. Журавель, А.В. Іщенко, М.В. Карчевський, А.В. Коваленко, В.В. Коваленко, В.А. Колесник, О.Є. Користін, В.К. Лисиченко, А.В. Мовчан, О.П. Метелев [8, с. 42–53], М.А. Погорецький, М.Я. Сегай, Р.Л. Степанюк, Я.О. Тализіна, О.О. Торбас [11], В.М. Шевчук [13, с. 491–502; 14, с. 356–361], С.О. Шулгін [15; 16, с. 109–116], М.Г. Щербаковський, Д.М. Цехан [6], А.М. Черняк, І.А. Федчак, В.Г. Хахановський та ін. [3, с. 280–283; 12]. Проте дослідниками ще не надано оцінку процесуальної процедури використання даних,

отриманих у контррозвідальній діяльності у кримінальному процесуальному доказуванні (доведенні).

Метою статті є дослідження особливостей застосування новітніх технологій у документуванні та розслідуванні окремих видів воєнних злочинів.

Виклад основного матеріалу. У циклі робіт професора В.М. Шевчука здійснено ґрунтовний аналіз ролі технологій штучного інтелекту у правоохоронній діяльності, у забезпеченні безпеки України та подані оригінальні рекомендації щодо підвищення ефективності такої роботи, які становлять безумовний теоретичний та практичний інтерес, зокрема:

- аналіз супутникових знімків;
- аналіз відео- та фотоматеріалів;
- обробка аудіоматеріалів;
- аналіз соціальних мереж;
- аналіз даних з медичних закладів;
- розпізнавання обличчя;
- аналіз текстової інформації [13, с. 491–502; 14, с. 356–361].

Цілком очевидним є те, що відповідна оперативно-розшукова (контррозвідальна) діяльність буде більш ефективною за умови застосування новітніх технологій, у тому числі інформаційних, які базують на штучному інтелекті, зокрема нейромереж для розпізнавання вербальної інформації, соціальної інженерії, а також:

- перевірка достовірності інформації, отриманої з різних джерел, аналіз та підготовка відповідного дослідження (висновку);
- отримання даних про суб'єктів воєнних злочинів, а також осіб, які мають відношення до них, встановлення кримінальних, родинних зв'язків, зв'язків осіб, які разом працюють або навчаються тощо;

розпізнавання ознак зовнішності людини за фото- та відеоматеріалами (@osint_maigret_bot, @the_dark_I_bot, рекламні ідентифікатори, Wi-Fi, бенди);

– пошук за супутниковими знімками (Google Earth Pro, photo-map.ru, tool.geoimgr.com);

– пошук метаданих;

– пошук за позивними;

– гео та хронолокація.

Розповсюдженою практикою є розміщення суб'єктами даних злочинів відео катувань у відповідних групах у месенджері «Телеграм», відеохостінгу YouTube. Ефективність в ідентифікації воєнних злочинців демонструють нейронні мережі, які завдяки відповідній комбінації спеціальних лінгвістичних знань, аналітиків та фахівців у сфері машинного навчання дозволяють визначати ймовірність того, що конкретні ознаки голосу належать певному фігуранту.

Так, у рамках аналізу відео розстрілу військовослужбовці Збройних Сил України, викладеного в мережі було виокремлено аудіо треки для навчання нейромережі та порівняння зі зразками фонограм, досліджених у рамках OSINT-розвідки. Крім того, з відкритих джерел проаналізовано відео, в якому зафіксовано військово-службовця 85-ї бригади «южной группировки войск» із позивним Варяг. Під час аналізу

здійснено порівняння відповідних матеріалів, зафіксованих на відео розстрілу та відео, отриманого під час проведення OSINT-розвідки, в результаті якого встановлено 60% збігу.

Крім того, у теперішній час штучний інтелект використовується для планування розслідування, аналізу матеріалів кримінальних проваджень, а також вибору тактики проведення тієї чи іншої слідчої (розшукової) дії (ресурси на базі Палантір). Наприклад, із урахуванням даних про слідчу ситуацію та психологічні типи підозрюваних штучний інтелект може запропонувати найбільш раціональні прийоми допиту, його тривалість тощо.

Використання інформаційних ресурсів банків даних, колекцій, систем та підсистем має здійснюватися в рамках оперативно-розшукової справи (контррозвідувальної справи) або кримінального провадження і тільки особою, якою заведено оперативно-розшукову справу, або яка входить до складу слідчої групи, створеної для розслідування конкретного кримінального провадження. Інформація про доступ до банку даних повинна фіксуватися та зберігатися в автоматизованій системі обробки даних, включно з інформацією про особу, яка отримала доступ, та про обсяг даних, доступ до яких було отримано. Кожна дія особи щодо отримання інформації

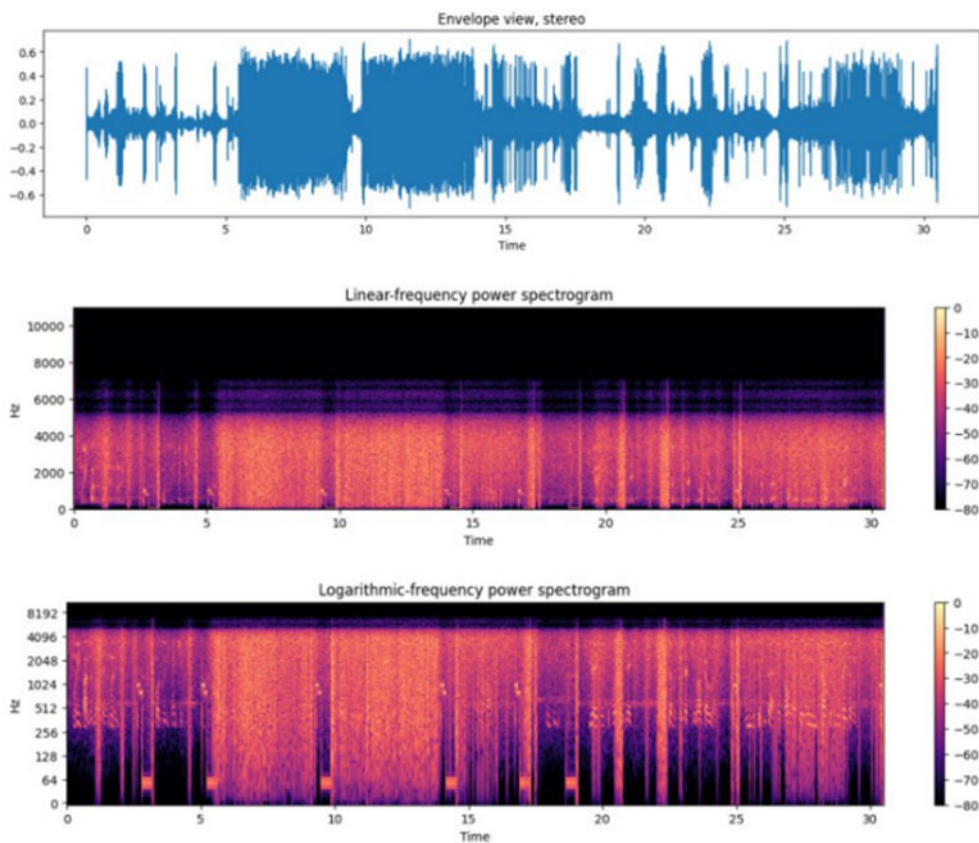


Рис. 1.

з інформаційних ресурсів, фіксується у спеціальному електронному архіві інформаційно-комунікаційної системи, за допомогою якої отримано відомості.

Використання інформації отриманої з банків даних підсистем що містять відомості стосовно осіб, причетних до вчинення воєнних та інших злочинів буде найефективнішою за умови комплексної обробки з інформацією, яка міститься в закритих базах даних органів правопорядку, результатами оперативно-розшукових та оперативно-технічних заходів (у тому числі проведених оперативними службами), контррозвідальних заходів, оброблених та проаналізованих з залученням аналітиків.

Цікавою представляється позиція О.П. Бабікова, який зважаючи на специфіку контррозвідальної діяльності стверджує, що вона «виключає можливість ретельно і достатньо повно опрацювати джерела та спосіб фіксації одержаних доказів. Проте інформація, одержана під час здійснення такої діяльності може бути підставою для внесення відомостей до ЄРДР та початку досудового розслідування» [2, с. 98].

З висловленою тезою погоджуємося частково.

По-перше, згідно з п. 14 ст. 92 Конституції України судоустрій, статус суддів, засади судової експертизи, організація і діяльність прокуратури, нотаріату, органів досудового розслідування, органів і установ виконання покарань, порядок виконання судових рішень, засади організації та діяльності адвокатури визначаються виключно законами України. Серед принципів контррозвідальної діяльності, закріплених ст. 4 Закону України «Про контррозвідальну діяльність» визначено, з-поміж іншого «безперервність» та «адекватність заходів щодо захисту державної безпеки реальним і потенційним загрозам». Згідно п. 1 ч. 2 ст. 6 цього ж Закону підставами для проведення контррозвідальної діяльності є [5]:

здійснення розвідальної діяльності проти України спеціальними службами іноземних держав, а також організаціями, окремими групами та особами, посягання на державний суверенітет, конституційний лад і територіальну цілісність (тобто кримінально-протиправної діяльності, передбаченої ст.ст. 109, 110, 110-2, 111, 111-1, 111-2, 112, 113, 114, 114-1, 114-2 КК України);

терористичні посягання чи терористичну діяльність, кримінальні правопорушення проти миру, безпеки людства та міжнародного правопорядку (тобто кримінально-протиправні делікти, передбачені ст.ст. 258-258-5, 436, 436-2, 437, 438, 439, 440, 441, 442, 443, 444, 446, 447 КК України).

Звідси випливає, що застосування відповідних адекватних заходів протидії вже само

по собі буде відрізнятися від заходів протидії, застосовуваних для нейтралізації протидії так би мовити «традиційній злочинності загально-кримінальної чи іншої подібної спрямованості», яка вчиняється в тому числі в різних формах, нехай і злочинного лідерства, але все ж таки громадянами України. Для протистояння спецслужбам потрібні інші засоби, позиції та заходи. У даному випадку контррозвідального характеру, котрі потребують тривалої кропіткої роботи.

Згідно з ч. 3 ст. 7 Закону України «Про контррозвідальну діяльність» відповідні підрозділи мають право: «... здійснювати заходи, визначені частиною третьою статті 8 Закону України «Про оперативно-розшукову діяльність», – лише за ухвалою слідчого судді, постановленою за клопотанням керівника відповідного оперативного підрозділу або його заступника, погодженим із прокурором. Нагляд за додержанням законів під час проведення контррозвідальної діяльності здійснюється Генеральним прокурором, виконувачем його обов'язків або уповноваженим наказом Генерального прокурора заступниками Генерального прокурора» [5]. Тобто, мова про відсутність контролю, у тому числі судового взагалі не йдеться.

Далі. Відповідно, згідно п. 7 ст. 7 Закону України «Про контррозвідальну діяльність» органи, підрозділи та співробітники Служби безпеки України, що здійснюють контррозвідальну діяльність мають право «затримувати і тримати у спеціально відведених для цього місцях: осіб, підозрюваних у підготовці чи проведенні розвідально-підривної, терористичної діяльності та вчиненні інших кримінальних правопорушень, розслідування яких віднесено до компетенції органів Служби безпеки України, – на строки і в порядку, що передбачені законами України» [5]. Своєю чергою, згідно з п. 6 ч. 11 ст. 8 цього ж закону «контррозвідальна справа повинна бути закрита у разі притягнення особи до кримінальної відповідальності, в тому числі і за кордоном, за дії, що були підставами для заведення контррозвідальної справи» [5]. Відповідно до п. 14 ч. 1 ст. 3 КПК України «притягнення до кримінальної відповідальності – стадія кримінального провадження, яка починається з моменту повідомлення особі про підозру у вчиненні кримінального правопорушення (п. 14 ч. 1 ст. 3 КПК України) [7]. В свою чергу, «у разі виявлення ознак злочину оперативний підрозділ, який здійснює оперативно-розшукову і контррозвідальну діяльність, зобов'язаний невідкладно направити зібрані матеріали... до органу досудового розслідування для початку та здійснення досудового розслідування» (ч. 2 ст. 7 Закону України «Про оперативно-розшукову діяльність») [9]. Тобто ризики протиправного

посягання на права і свободи особи зняті й таким запобіжником.

По-друге, однозначно, що матеріали:

а) фото-, аудіо-, відеозаписів, зафіксованих:

– безпілотними літальними апаратами Сил оборони України;

– безпілотними літальними апаратами аеророзвідки (військової повітряної розвідки), підрозділами ударних безпілотних авіаційних комплексів;

б) перехоплень, насамперед на об'єктах контррозвідувального забезпечення, потребують використання під час розслідування зазначених деліктів як приводи і підстави початку досудового розслідування, для отримання доказів, для попередження, виявлення, припинення і розслідування злочинів вищезазначеної категорії.

Можемо виокремити види матеріалів контррозвідувальної діяльності за функціональним призначенням (критерієм):

а) матеріали, в яких зафіксовано результати організаційної роботи з проведення відповідної діяльності (постанова про заведення справи, продовження строків її проведення тощо);

б) матеріали, в яких зафіксовано результати контррозвідувальної діяльності, тобто фактичні дані, відомості щодо протиправних, суспільно небезпечних діянь осіб, або груп осіб, відповідальність за які передбачена зазначеними вище кримінально-правовими заборонами.

По-третє. Обов'язковим критерієм для врахування, з метою подальшого не допущення хибних внесень відомостей до Єдиного реєстру досудових розслідувань (далі – ЄРДР), а також у випадках достовірних внесень відомостей до ЄРДР, однак при цьому подальшого встановлення початкових хибних обставин кримінального правопорушення, зокрема щодо об'єкту злочину та потерпілого, за ч. 2 ст. 438 КК України, є детальна невідкладна перевірка на об'єктах контррозвідувального забезпечення відомостей про обставини, які передували кримінальному правопорушенню, тобто відомості з бойових розпоряджень, підсумкових бойових донесень, журналів ведення бойових дій, анкетних даних на військовослужбовців, у тому числі фото- відео матеріалів з ними, безпосередньо щодо військовослужбовців Сил Оборони України, які виконували бойові (спеціальні) завдання на лінії бойового зіткнення чи в тилу ворога, оскільки наявні непоодинокі випадки в зонах діяльності оперативно-тактичних угруповань, коли виникають первинні ситуації, за яких надаються відомості щодо військовослужбовців Сил Оборони України, які не є об'єктом злочину та не є потерпілими, а кримінальне правопорушення представниками російських окупаційних військ вчинено відносно інших військових. Отже, дана обставина біль-

шою мірою впливає і на первинну ідентифікацію суб'єкту злочину.

На первинному етапі важливим є саме детальний, чіткий підхід у встановленні обставин означеного кримінального правопорушення, достовірні відомості про яке, у даному випадку, можуть бути отримані за результатами наданих первинних пояснень (в подальшому допитів) військовослужбовців Сил Оборони України, зокрема командирів, військових, які вийшли з «оточення» ворога, чи перебували на суміжних позиціях та виконували бойові (спеціальні) завдання, а також іншими військовими. Не треба й нехтувати відомостями, отриманими від полонених (в даному випадку маються на увазі представники російських окупаційних військ). Під час відібрання пояснень та проведення допитів необхідно слід звернути увагу на ідентифікацію суб'єктів злочину, поведінку, одяг, окремі ознаки наявні на їх одязі, шеврони, наліпки, тощо, озброєння та військову техніку які використовуються ворогом, інше військове майно, крім того, індивідуальні ознаки на тілі суб'єкта злочину, татування, оздоблення тощо.

Окрім того, важливу роль відіграє попередній аналіз обставин вчинення кримінального правопорушення, зокрема під час збирання відповідних документальних матеріалів перед внесенням відомостей до ЄРДР, а саме часу, місця, обставин перебування військових Сил Оборони України на лінії бойового зіткнення чи в тилу ворога, таких фактів та факторів як останніх з'єднань радіозв'язку, напрямків просування ворога, задіяних останніми підрозділів, тощо.

Слід попередньо враховувати та аналізувати отримані за інших обставин відомості, у тому числі від ворога, через агентурну мережу, від полонених (в даному випадку маються на увазі представники російських окупаційних військ), тощо, щодо можливих списків їх військових підрозділів, інших відомостей, у тому числі з мобільних гаджетів, як під час потрапляння в полон так і за інших обставин, під час проведення контррозвідувального забезпечення.

По-четверте. Пунктами 5, 6 Закону України «Про судоустрій і статус суддів» передбачена обов'язковість судових рішень, зокрема «Висновків щодо застосування норм права, викладених у постановках Верховного Суду» [10]. З-поміж іншого станом на сьогодні маємо відповідні правові позиції, викладені в таких постановках:

– постанова від 03.03.2020 (справа №221/2901/15-к; провадження № 51-3070 км 18);

– постанова від 06.12.2021 (справа № 756/4855/17; провадження № 51-7121 км 18);

– постанова від 11.01.2022 (справа №942/1889/19; провадження № 51-3806 км 21).

По-н'яте (і в рамках даної публікації останнє). Чи достатньо врегульовано використання матеріалів контррозвідувальної діяльності в доказуванні (доведенні)? Дійсно, на жаль у сучасному кримінальному процесі продовжують виходити з поділу процесу доказування (доведення) та принципів (засад), котрі регулюють цей процес, виокремлюючи збирання доказів від їх оцінки. Збирання доказів залишається максимально деталізованим, тобто таким, що базується на теорії формальних доказів; оцінка доказів – вільною, тобто такою, що базується на теорії вільної оцінки доказів за внутрішнім переконанням. «Неозброєним оком» видно, що оцінка доказів за КПК України здійснюється вільно, без тиску з боку закону, за внутрішньою волею правозастосовця, але при тому законом встановлені суворі процесуальні рамки відносно збирання доказів.

Позаяк не можна заперечувати і того факту, що вітчизняна теорія доказів має багато загального з англосаксонською. В якості прикладу можна навести фундаментальні для доказового права поняття належності та допустимості доказів, які є невідомими іншим континентальним правовим системам і мають, очевидно, британське походження.

Таким чином, слід визнати той факт, що особливість вітчизняного кримінального процесу полягає в суворому дотриманні принципу свободи доказування (доведення) за внутрішнім переконанням, але тільки відносно оцінки доказів. Збирання доказів базується на принципі формалізації процедури.

Висновки. Тому, перспективними напрямками подальших наукових розвідок у цій сфері вважаємо:

- подальше машинне навчання нейромереж;
- залучення до процесу відповідного ідентифікаційного пошуку фахівців у галузі семантико-текстуальної експертизи;
- створення єдиної бази даних (картотеки) фотogram воєнних злочинців;
- врегулювання (створення) процесуального механізму звернення з клопотанням до прокурора під час ведення контррозвідувальних заходів (у рамках контррозвідувального пошуку) з метою створення можливості використання матеріалів контррозвідувальної діяльності як джерел судових доказів – документів.

Література

1. Авдеева Г.К. Проблеми визначення достовірності цифрових доказів у кримінальному провадженні. *Вісник Луганського навчально-наукового інституту імені Е.О. Дідоренка*. № 1 (2024). С. 33–48.
2. Бабіков О.П. Теоретико-прикладні засади негласних слідчих (розшукових) дій: генеза та перспек-

тиви розвитку: монографія; Наук.-досл. ін-т публічного права. Київ: Норма права, 2024. 446 с.

3. Бондар В.С. Використання експертних технологій в інформаційно-аналітичному забезпеченні розслідування злочинів проти основ національної безпеки України. *СБУ в умовах війни в Україні: сучасні реалії та інноваційні стратегії забезпечення національної безпеки*: мат. міжн. наук.-практ. конференції 4–5 липня 2024 року. Київ: Алерта, 2024. С. 280–283.

4. Дуфенюк О.М. Концептуальна модель балансу в кримінальному провадженні: інституційний, правозастосовний, особистісний рівні. дис. ... докт. юрид. наук : 12.00.01; 12.00.09; Львівський державний університет внутрішніх справ. Львів, 2024. 568 с.

5. Закони України: «Про розвідку», «Про контррозвідувальну діяльність», «Про Службу зовнішньої розвідки України»: чинне законодавство зі змінами та допов. станом на 2 травня 2023 р.: Київ: ПАЛІВОДА А.В., 2023. 68 с. (Закони України).

6. Кіберзлочинність та електронні докази = Cybercrime and digital evidence: навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д.М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельцер. Електрон. вид. Львів : ЛНУ ім. Івана Франка, 2022. 298 с.

7. Кримінальний процесуальний кодекс України від 13.04.2012 № 4651-VI (зі змін. та допов.). URL: <https://zakon.rada.gov.ua/laws/show/4651-17#Text>.

8. Метелев, О. (2024). Цифрові докази у кримінальному процесі: видова характеристика. *Вісник кримінального судочинства*, (1-2), 42–53.

9. Про оперативно-розшукову діяльність: Закон України від 18 лютого 1992 року № 2135-XII у редакції від 18.07.2024. URL: <https://zakon.rada.gov.ua/laws/show/2135-12#Text> (дата звернення: 29.11.2024).

10. Про судоустрій і статус суддів: Закон України від 02 червня 2016 року № 1402-VIII у редакції від 09.12.2023. URL: <https://zakon.rada.gov.ua/laws/show/1402-19#Text> (дата звернення: 29.11.2024).

11. Торбас О. О. OSINT при розслідуванні кримінальних правопорушень : підручник. Одеса, 2024. 180 с.

12. Шевчишена К.П. Розслідування воєнних злочинів в Україні: дис. ... канд. юрид. наук (докт. філос.): 12.00.09 (081 – Право); Національна академія внутрішніх справ. Київ, 2024. 330 с.

13. Шевчук В.М. Використання технологій штучного інтелекту та спеціальних знань у розслідуванні воєнних злочинів. *Правнична наука та законодавство України: європейський вектор розвитку в умовах воєнного стану: монографія / редкол.: В.А. Журавель (співголова), Н.С. Кузнецова (співголова), О.М. Бандурка та ін.; Нац. акад. прав. наук України. Харків: Право, 2023. С. 491–502.*

14. Шевчук В.М. Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України. *Юридичний науковий електронний журнал*. 2024. № 6. С. 356–361.

15. Шульгін С. О. Оцінка слідчим і прокурором доказів при прийнятті процесуальних рішень на стадії досудового розслідування : дис. ... канд. юрид. наук : 12.00.09 ; Науково-дослідний інститут публічного права ; Дніпропетровський державний університет внутрішніх справ МВС України. Київ, 2021. 260 с.

16. Шульгін С.О. Достатність доказів як підстава прийняття процесуальних рішень слідчим та прокурором. *Право та державне управління*. 2019. № 2 (35). Т. 2. С. 109–116.

Анотація

Бондар В. С., Парфьонов В. Ю. Про особливості застосування новітніх технологій у документуванні та розслідуванні окремих видів воєнних злочинів. – Стаття.

У статті розглядаються можливості застосування новітніх технологій у документуванні та розслідуванні окремих видів воєнних злочинів, зокрема штучного інтелекту. Подаються приклади використання програмних продуктів під час документування конкретних злочинів, передбачених ст. 438 КК України.

Класифіковано види матеріалів контррозвідувальної діяльності за функціональним призначенням (критерієм):

а) матеріали, в яких зафіксовано результати організаційної роботи з проведення відповідної діяльності (постанова про заведення справи, продовження строків її проведення тощо);

б) матеріали, в яких зафіксовано результати контррозвідувальної діяльності, тобто фактичні дані, відомості щодо протиправних, суспільно небезпечних діянь осіб, або груп осіб, відповідальність за які передбачена ст.ст. 109, 110, 110-2, 111, 111-1, 111-2, 112, 113, 114, 114-1, 114-2, 258-258-5, 436, 436-2, 437, 438, 439, 440, 441, 442, 443, 444, 446, 447 КК України (матеріали радіоперехоплень, відомості з бойових розпоряджень, підсумкових бойових донесень, журналів ведення бойових дій, анкетних даних на військовослужбовців, у тому числі фото-відео матеріалів з ними, безпосередньо щодо військовослужбовців Сил Оборони України, які виконували бойові (спеціальні) завдання на лінії бойового зіткнення чи в тилу ворога тощо).

Наведені правові позиції Верхового Суду щодо використання результатів контррозвідувальної діяльності у кримінальному провадженні.

Сформульовані пропозиції щодо подальших наукових розвідок у цьому напрямі з метою використання відповідних матеріалів у якості судових доказів, які обіймають:

- подальше машинне навчання нейромереж;
- залучення до процесу відповідного ідентифікаційного пошуку фахівців у галузі семантико-текстуальної експертизи;
- створення єдиної бази даних (картотеки) фонограм воєнних злочинців;
- врегулювання (створення) процесуального механізму звернення з клопотанням до прокурора під час ведення контррозвідувальних заходів (у рамках контррозвідувального пошуку) з метою створення можливості використання матеріалів контррозвідувальної діяльності як джерел судових доказів – документів.

Ключові слова: воєнні злочини, державна безпека, доказування, документування, контррозвідувальна діяльність, OSINT-розслідування, ідентифікація, інформаційна система, нейронна мережа, штучний інтелект.

Summary

Bondar V. S., Parfyonov V. Yu. On the peculiarities of the application of the latest technologies in the documentation and investigation of certain types of war crimes. – Article.

The article considers the possibilities of using the latest technologies in documenting and investigating certain types of war crimes, in particular artificial intelligence. Examples of using software products in documenting specific crimes stipulated in Art. 438 of the Criminal Code of Ukraine are given.

Types of counterintelligence materials are classified by functional purpose (criterion):

a) materials that record the results of organizational work on the implementation of the relevant activity (resolution on the initiation of a case, extension of the terms of its implementation, etc.);

b) materials that record the results of counterintelligence activities, i.e. factual data, information on illegal, socially dangerous acts of individuals or groups of individuals, liability for which is provided for in Art. 109, 110, 110-2, 111, 111-1, 111-2, 112, 113, 114, 114-1, 114-2, 258-258-5, 436, 436-2, 437, 438, 439, 440, 441, 442, 443, 444, 446, 447 of the Criminal Code of Ukraine (radio interception materials, information from combat orders, summary combat reports, combat logs, personal data on servicemen, including photo and video materials with them, directly concerning servicemen of the Defense Forces of Ukraine who performed combat (special) tasks on the front line or behind enemy lines, etc.).

The legal positions of the Supreme Court on the use of counterintelligence results in criminal proceedings are presented.

Proposals have been formulated for further scientific research in this direction in order to use relevant materials as judicial evidence, which include:

- further machine learning of neural networks;
- involvement of specialists in the field of semantic and textual examination in the process of the relevant identification search;
- creation of a single database (card index) of phonograms of war criminals;
- regulation (creation) of a procedural mechanism for applying to the prosecutor during counterintelligence measures (within the framework of a counterintelligence search) in order to create the possibility of using materials of counterintelligence activities as sources of judicial evidence – documents.

Key words: war crimes, state security, evidence, documentation, counterintelligence, OSINT investigation, identification, information system, neural network, artificial intelligence.