DOI: https://doi.org/10.26642/sas-2025-6(12)-77-86
УДК 378:344.2:004

Лук'яненко Станіслав
аспірант
Відділ аналізу і діяльності Національної академії Служби безпеки України

Бондар Володимир
кандидат юридичних наук, професор
Навчально-науковий гуманітарний інститут у складі Національної академії Служби безпеки України

Оптимізація моделі підготовки здобувачів освіти та співробітників органів правопорядку для виявлення, документування та досудового розслідування воєнних злочинів із застосуванням високих технологій (OSINT, HUMINT)

Анотація. Цифрові технології кардинально змінюють розслідування воєнних злочинів, розширюючи джерела інформації завдяки «цифровій географії». На сьогодні для встановлення часу, місця та обставин скоєння злочину, розпізнавання, ідентифікації об'єктів, аналізу радіоперехоплень, верифікації даних та деанонімізації осіб активно використовується розвідка з відкритих джерел, цифрові технології та докази, штучний інтелект і великі мовленнєві моделі. Це підвищує ефективність розслідувань, але вимагає підготовки нового покоління фахівців з відповідними цифровими, правовими та аналітичними компетенціями, а також навичками дотримання «цифрової гігієни».

У цьому контексті особливого значення набувають належний збір та автентифікація електронних доказів, перелік яких визначено чинними нормативно-правовими актами, а також дотримання міжнародних стандартів, включно з Протоколом Берклі та рекомендаціями Ради Європи щодо електронних доказів. Формування відповідних цифрових компетентностей здобувачів освіти та співробітників органів правопорядку – зокрема роботи з OSINT, геолокацією, верифікацією даних, техніками цифрової гігієни та інструментами деанонімізації – є необхідною умовою належного опрацювання цифрових матеріалів і підвищення якості доказової бази.

Важливим є розвиток якісних навчальних програм у закладах освіти різних рівнів, забезпечення доступу до спеціалізованих цифрових інструментів, міжвідомча взаємодія з міжнародними організаціями та ІТ-сектором, а також мотивація до безперервного професійного зростання. Штучний інтелект як сучасна технологія створює додаткові можливості для вдосконалення моделі підготовки: автоматизації аналізу цифрових даних, точнішої ідентифікації об'єктів і прискорення окремих криміналістичних процесів, сприяючи формуванню фахівців, здатних ефективно діяти в умовах гібридних загроз та інформаційного протистояння.

Ключові слова: воєнні злочини; цифрові технології; докази; підготовка фахівців.

Актуальність теми дослідження. Сучасне міжнародне право виходить з того, що війна, у випадку її виникнення, не означає нічим не обмеженого взаємного знищення та руйнування, що виключає будь-яке правове регулювання. Водночас, як свідчать результати аналізу слідчої та судової практики, російська федерація систематично та грубим чином порушує закони і звичаї війни, не рахуючись навіть із тим, що вона сама є учасником тих або інших міжнародних конвенцій.

Зазначена акцентована ситуація вимагає адекватного реагування в контексті ефективного розслідування та документування воєнних злочинів, які є унікальними, оскільки посягають на загальнолюдські цінності та принципи гуманізму, спрямовані проти беззахисних цивільних осіб та військовополонених.

Головна мета цієї роботи – напрацювання сучасної моделі підготовки здобувачів освіти та співробітників органів правопорядку для виявлення, документування та досудового розслідування воєнних злочинів із застосуванням високих технологій (OSINT – розвідка з відкритих джерел, HUMINT – розвідка через прямий контакт з людиною) з метою притягнення винних до кримінальної відповідальності та підтримка міжнародних зусиль з розслідування й судового переслідування воєнних злочинців.

Пріоритетом у формуванні доказової бази є збереження актуальної, достовірної інформації щодо часу, фактів і об'єктивних обставин воєнних злочинів, таких як депортація українських дітей, ракетні та інші обстріли критичної та цивільної інфраструктури, позасудові страти українських

військовослужбовців тощо. Також важливо запобігти можливому приховуванню або знищенню цих даних у майбутньому. Зібрані відомості мають слугувати основою для кримінального переслідування винних та гарантувати невідворотність покарання.

На жаль, географія скоєних російською стороною злочинів унаслідок повномасштабного вторгнення є надзвичайно широкою як на території України, так і за її межами. Водночас розвиток цифрових технологій, масове використання мережі «Інтернет», соціальних мереж, месенджерів та інших каналів комунікації, зокрема й безпосередніми виконавцями злочинів, значно розширює можливості збирання інформації та фіксації джерел її надходження.

Актуальність теми постає з обсягів документованих правопорушень у межах статей 437–438 Кримінального кодексу України (далі – КК України), які вчиняються російською стороною. Зокрема, станом на липень 2025 р. загалом розслідувалося 177 745 кримінальних правопорушень, пов'язаних з агресією рф щодо України. 85 % розслідувань здійснюється слідчими Служби безпеки України, 15 % – інших органів правопорядку. На сьогодні слідчими СБ України продовжується досудове розслідування у близько 92 тис. кримінальних провадженнях щодо 143 тис. кримінальних правопорушень, пов'язаних з агресією рф.

Успішне розслідування означених кримінально-правових деліктів насамперед будується на розумінні слідчим та прокурором винятковості цих злочинів. Адже в них йдеться не просто про замах на життя, здоров'я, особисту недоторканність, майно потерпілої особи, вони свідчать про безпорадність та беззахисність неозброєної людини (цивільної особи, військовополоненого) перед представником країни-агресора. Такі злочини посягають на загальнолюдські цінності, принцип гуманізму й викликають тривогу у світової спільноти. Для успіху у розслідуванні зазначених кримінальних проваджень необхідні ґрунтовні знання з теорії та практики міжнародного гуманітарного права та міжнародного кримінального права, особливостей збирання доказової бази та доведення таких злочинів. Особливо важливими на сьогодні постають вміння аналізувати значні обсяги інформації про перебіг збройного протистояння в Україні та уявляти обставини кримінальних правопорушень тощо.

Аналіз останніх досліджень та публікацій. Актуальне питання підготовки здобувачів освіти та співробітників органів правопорядку, зокрема у сфері опанування методів збирання цифрових даних, OSINT тощо для досудового розслідування воєнних злочинів, є предметом активного дискурсу у вітчизняному та зарубіжному науковому полі.

Водночас до початку повномасштабної агресії російської федерації існувала значна прогалина у спеціалізованих криміналістичних та процесуальних дослідженнях, що стосувалися документування воєнних злочинів в Україні, що призводило до необхідності для багатьох фахівців опановувати новітні підходи і технології в умовах певного цейтноту.

Попри це, вітчизняна наука відреагувала належним чином на сучасні потреби практики. Тільки за останні два роки світ побачив цикл навчально-методичної продукції, яка або повністю присвячена використанню OSINT-аналізу в процесі розкриття та розслідування злочинів, або містить відповідні структурні компоненти чи розділи. Зокрема, серед «класичних» продуктів варто назвати практичний порадник Д.С. Зоренка «Використання інструментів та методів OSINT для отримання пошукової інформації» (Харків, 2023 р.) [1], навчальний посібник Д.В. Ланде «OSINT у кібербезпеці» (Київ, 2024 р.) [7], навчальний посібник Р.Л. Степанюка та В.О. Гусєвої «Сучасні криміналістичні засоби та методи протидії злочинності» (Харків, 2024 р.) [11] та підручник О.О. Торбаса «OSINT при розслідуванні кримінальних правопорушень» (Одеса, 2024 р.) [13].

Окремі питання оптимізації моделі підготовки фахівців висвітлені в науково-практичному посібнику «Розслідування воєнних злочинів і пов'язаних з війною кримінальних правопорушень: кримінально-правові, кримінальні процесуальні та криміналістичні аспекти» колективу авторів Харківського державного університету внутрішніх справ (Харків, 2024 р.). Серед інших, Дуфенюк О.М. акцентує увагу на необхідності стандартизації процесів розслідування, алгоритмізації процесуальних дій та врахування зарубіжного досвіду, а також на доцільності глибокої інтеграції високих технологій, таких як використання дронів, 3D-сканерів та розвідки з відкритих джерел для підвищення якості та швидкості збирання доказів у цифрову епоху.

Таким чином, ці роботи заклали концептуальні засади для формування комплексної та технологічно просунутої програми навчання для співробітників, що займаються розслідуванням воєнних злочинів.

Іноземні джерела інформації з зазначеної проблематики переважно стосуються сфер використання OSINT, напрацювання новітніх стандартів та рекомендацій, проведення тренінгів та курсів, а також обґрунтування застосування зазначених методів збору інформації для її подальшого використання як доказів.

Наприклад, роботи Дж.Девіса у сфері використання розвідки з відкритих джерел є цінним джерелом саме для вирішення вказаних завдань. Його дослідження, що стосуються використання соціальних мереж та супутникових знімків для документування конфліктів, дозволяють встановити причинно-наслідковий зв'язок між діями злочинців та наслідками. Однак у працях не враховуються особливості процесуального

оформлення цифрових доказів відповідно до національного законодавства, що є критично важливим для їх використання в суді.

Крім того, у роботах П.Вагнера аналізуються юридичні аспекти збору та використання електронних доказів у міжнародних судах. Його дослідження щодо Протоколу Берклі та інших міжнародних стандартів (ISO/IEC 27037) надають основу для розробки рекомендацій щодо автентифікації та збереження цифрових даних. Вагнер докладно розглядає питання допустимості та достовірності електронних доказів, що допомагає подолати одну з головних проблем – невизнання таких доказів у суді. Проте його роботи також не можуть повністю вирішити проблему, оскільки не враховують специфіку підготовки та мотивації кадрів, що є однією з ключових цілей статті.

Важливою складовою іноземних досліджень також є вивчення питань швидкого поширення автоматизації, штучного інтелекту, а також проблеми розпорошеності ініціатив, відсутності дієвої координації між суб'єктами освітніх програм, недостатньої інтеграції правової підготовки з технічною, етичних та безпекових питань навчання.

Викладення основного матеріалу. Тенденції зміни кримінальної політики в умовах воєнного стану, структури й ознак кримінально-протиправної діяльності у сфері національної безпеки, воєнних злочинів (ст. 438 КК України), злочину агресії (ст. 437 КК України), злочинів терористичної спрямованості (ст.ст. 258, 258-1, 258-2, 258-3, 258-4, 258-5, 258-6 КК України), трансформація суспільних відносин у цифрову площину, а також ратифікація Україною римського статуту Міжнародного кримінального суду і Кампальських додатків до нього потребують актуальних рекомендацій щодо їх контррозвідувального, оперативно-розшукового та криміналістичного забезпечення.

Зокрема, нині повідомлено про підозру за нанесення ударів по цивільній інфраструктурі 14 командирам підрозділів зс рф, встановлено 224 особи, причетні до жорстокого поводження з військовослужбовцями Сил безпеки та оборони України тощо.

Ефективність цієї діяльності знаходиться у прямій залежності від володіння відповідними суб'єктами, як цифровими компетенціями, так і сучасними методами пошуку, аналізу та оцінки інформації із застосуванням високих технологій для достовірного встановлення осіб, причетних до скоєння позначених кримінально-правових деліктів із урахуванням пізнання системи елементів їх властивостей:

- морфологічних;
- психофізіологічних;
- соціально-психологічних;
- соціально-демографічних.

Відповідні методи базуються на:

- об'єктивних критеріях виокремлення, порівняння та оцінки ідентифікаційних ознак;
- математико-статистичній інтерпретації процесу ідентифікації;
- динаміці ознак зовнішності людини, їх якісних та кількісних характеристик тощо.

Проблема розширення компетенції оперативного співробітника, слідчого, які застосовують технології OSINT та HUMINT через створення нової моделі, стає достатньо актуальною, адже їх знання в області цифрових фотографічних процесів конкурують зі знаннями експертів у галузі комп'ютерних технологій та досліджень фото, експертизи відео та звукозаписів, а також теорії оперативно-розшукової діяльності.

Конкретизуємо лише деякі кримінальні процесуальні та криміналістичні особливості, які рекомендується брати до уваги здобувачам освіти та практичним співробітникам органів правопорядку під час здійснення пошуково-пізнавальної діяльності. Зокрема, усвідомленню підлягають форми відображення слідової інформації, серед якої необхідно виокремити:

1) *інформацію, отриману в результаті радіоперехоплень* (аудіо-, відеоматеріали). Подібна інформація дозволяє виявляти елементи об'єктивної сторони злочину, такі як факт віддання наказів (встановлювати ознаки командної відповідальності), застосування заборонених видів зброї чи засобів ведення війни, катувань та розстрілів військовополонених тощо;

2) *розвідувальну інформацію*. Потенційною проблемою використання цього цінного джерела інформації як доказу є те, що відповідно до українського законодавства розвідувальні дії не можуть проводитися в інтересах слідства;

3) *використання можливостей штучного інтелекту та великих мовленнєвих моделей (скорочення AI або Artificial intelligence – штучний інтелект).* Станом на сьогодні застосування можливостей штучного інтелекту на основі нейронних мереж використовується слідчими органів безпеки (програмні оболонки Palantir, Paliscope) [16], співробітниками уповноважених оперативних підрозділів для оцінки вихідної інформації, виявлення ознак серійності в умовах інформаційної недостатності та формулювання пропозицій щодо перевірки слідчих версій; виявлення прихованих закономірностей у способі вчинення злочинів; роботи з соціальними мережами, вебкешем, індексом пошукових систем; перехоплення й дешифрування повідомлень, переданих технічними каналами зв'язку; транскрування аудіо- та відеофайлів; візуалізації великих масивів даних для спрощення аналітичного процесу; розпізнавання та ідентифікації («офізичування») суб'єктів вчинення воєнних

злочинів, військової техніки, ознак місцевості, будівель та інших військових об'єктів за такими ознаками (штучними ідентифікаторами):

- вивчення зображень облич, розміщених на акаунтах у месенджерах, на відеохостингу YouTube тощо, фотозображень облич, надісланих через месенджери чи електронну пошту, шляхом порівняння із зображеннями облич осіб, отриманих з різних видів обліків, баз даних («Clearview AI»), санкційних списків тощо;
- пошук недоступних програмному забезпеченню комп'ютерних файлів, прихованих за допомогою стеганографії або альтернативних потоків даних, встановлення первинного джерела інформації в мережі «Інтернет» у процесі проведення комп'ютерно-технічних експертиз;
- аналізу фонограм, розміщених на різноманітних ресурсах шляхом порівняння з фонограмами, що містяться у відповідних базах даних, за допомогою об'єктно орієнтованої скриптової мови програмування Python з відповідними пакетами для обробки зображень: Artellence, NumPy, Matplotlib, IPython Jupyter, Pillow, OpenCV, SciPy, Scikit-learn [6; 8; 9; 14; 16], а також програмних продуктів Сил оборони України та СБ України.

Використання таких технологій дозволяє здійснювати моніторинг та автоматизовану ідентифікацію у відкритих джерелах осіб, об'єктів та ознак місцевості, а також підвищує точність верифікації отриманих даних.

Наведені фактори та особливості слугують підставою диференціації проблем використання методів OSINT, HUMINT як самостійного напряму в підготовці фахівців. Предметом цього напряму є закономірності:

1) розсіювання фото-, відео- та аудіоінформації (відкритих даних) про особу (об'єкт пошуку) в інформаційних системах, колекціях, базах і банках даних незалежно від їх цільового призначення та відомчої належності, соціальних мережах, медіа (новинний та інший контент), геоінформаційних системах, яке має об'єктивний характер;
2) *формування* та відображення властивостей особи і предметів навколишнього середовища з метою ідентифікації й розпізнавання відповідних властивостей.

Активне використання цифрових технологій потребує врахування закономірності відображення ознак зовнішності, елементів місцевості, отриманих за допомогою цифрової фото- та відеозйомки, застосування програмно-апаратних засобів обробки отриманих зображень. Це вочевидь підтверджує необхідність розробки нової моделі підготовки фахівців.

Принципами відповідних OSINT-досліджень є:

1) особа як об'єкт ідентифікації становить соціальне та біологічне ціле – складну функціональну систему, яка володіє стійкою та неповторною внутрішньою та зовнішньою структурою;
2) тотожність особи (предмета) встановлюється правовими засобами: кримінальними процесуальними – під час досудового розслідування та судового розгляду (в порядку, визначеному ст.ст. 93, 159–166, 263, 264 Кримінального процесуального кодексу України (далі – КПК України), адміністративно-правовими та оперативними – під час оперативно-розшукової (контррозвідувальної) діяльності [4; 9, с. 984].

У такому разі цікавим видається такий приклад судової практики. *12.05.2023 близько 09:00 год ОСОБА_5, ІНФОРМАЦІЯ_1, діючи в умовах міжнародного збройного конфлікту, перебуваючи на тимчасово окупованій території прибережної частини річки Дніпро Каховського району Херсонської області (точне місце досудовим розслідуванням не встановлено), здійснюючи дистанційне керування безпілотним літальним апаратом моделі «Mavic», спеціально облаштованим для здійснення керованого скидання боєприпасів типу «ВОГ-17», усвідомлюючи суспільно небезпечний характер своїх дій, тяжкі наслідки у вигляді загибелі або поранення цивільних осіб та бажаючи їх настання, за допомогою пульта керування квадрокоптером та отримання від останнього зображення в режимі реального часу визначив для себе як ціль для ураження двох цивільних осіб (чоловіка та жінку, одягнутих у цивільний одяг, неозброєних, без будь-яких ознак приналежності до комбатантів), які йшли пішки на розі вулиці Виноградної та провулку Спартаківського у с. Одрадокам'янка Бериславського району Херсонської області, а саме за координатами: 46°47'11.7"№ 33°17'39.3"E (46.786582, 33.294239), після чого умисно дистанційно здійснив прицільне скидання бойового припасу моделі «ВОГ-17» на останніх. У результаті розриву бойового припасу ОСОБА_6, ІНФОРМАЦІЯ_2, отримав мінно-вибухову травму: непроникаюче осколкове поранення передньої черевної стінки, осколкові поранення III та IV пальців правої кисті, правої гомілки та правої стопи.*

Отже, військовослужбовець рф ОСОБА_5, ІНФОРМАЦІЯ_1, діючи в умовах міжнародного збройного конфлікту та у зв'язку з ним, вчинив порушення законів та звичаїв війни, які полягали у здійсненні нападу на цивільних осіб, що не беруть безпосередньої участі у воєнних діях, чим порушив вимоги ст.ст. 48, 51, 57, 85 ДП I.

Дії обвинуваченого ОСОБА_5 суд кваліфікує за ч. 1 ст. 438 КК України як порушення законів та звичаїв війни, що передбачені міжнародними договорами, згода на обов'язковість яких надана Верховною Радою України.

Винуватість обвинуваченого ОСОБА_5 у скоєнні зазначеного кримінального правопорушення підтверджується:

- довідкою оперативного підрозділу та фотозображенням до неї від 29.02.2024 року про встановлення особи ОСОБА_5 з зазначенням повних анкетних даних, засобів зв'язку, місця проживання, соціальних та родинних зв'язків;

- відповіддю на виконання доручення в порядку ст.ст. 36, 41 КПК України від 19.03.2024, відповідно до якої встановлено окремі групи військовослужбовців спеціальних бойових підрозділів зс рф, які після деокупації правого берега р. Дніпро Херсонської області діють на тимчасово окупованій території, серед яких НОМЕР_5 обрСпП гу гш зс рф, в/ч НОМЕР_4. Встановлено повні анкетні дані ОСОБА_5, засоби зв'язку, коло осіб, які можуть бути причетні до вчинення воєнних злочинів;

- протоколом проведення негласної слідчої (розшукової) дії від 24.04.2024, передбачених ст. 264 КПК України (зняття інформації з електронних інформаційних систем) з роздруківкою вказаного документа з фотозображеннями до нього та мультимедійним оптичним носієм інформації формату DVD-R, зі збереженими на ньому в електронному вигляді файлами, відповідно до якого здійснено зняття інформації з електронної інформаційної системи інтернет-месенджера «Telegram», а саме з акаунту зареєстрованого за допомогою мобільного термінала НОМЕР_6, яким користується ОСОБА_5. У протоколі зафіксовано листування ОСОБА_5 з абонентом, який підписаний «Витя», ідентифікований як брат ОСОБА_5 – ОСОБА_8, в ході аналізу листування встановлено наступне: 12.05.2023 у листуванні ОСОБА_5 з братом надсилав останньому фото з зображенням безпілотного літального апарата марки «Mavic», переобладнаного з закріпленням у нижній частині 2 боєприпасів. Крім того, 12.05.2023 ОСОБА_5 у листуванні з братом детально описує, що за результатами скидання ним боєприпасу з квадрокоптер було поранено 3 осіб (вказане зазначено у голосовому повідомленні). Також у звукозаписі ОСОБА_5 хвалиться брату, що це саме його особиста робота, коли він за наведенням «колег» здійснив ураження визначеної цілі. У голосовому повідомленні ОСОБА_5 повідомляє брату, що після скидання ним боєприпасу з'явилась інформація з ресурсів мережі «Інтернет» про одного пораненого та надає посилання на фрагмент відповідної публікації керівника Бериславської РВА ОСОБА_9 щодо поранення скинутим з дрона осколковим боєприпасом особи у с. Одрадокам'янка Тягинської територіальної громади Херсонської області (надається пересланий фрагмент публікації). Крім того, на питання брата «Так это вы по мирным жителям скинули, или по кому?», ОСОБА_5 зазначає, що йому неважливо, чи були вказані поранені особами військовими, чи просто мирне населення. Для нього ціллю є будь-яка особа чоловічої статі. Також у протоколі зафіксовано листування ОСОБА_5 з абонентом, який підписаний «ОСОБА_10» (ідентифікований як командир групи розвідки 1-го загону 2-ї роти 4-ї групи – ОСОБА_11), в ході аналізу листування встановлено наступне: 12.05.2023 ОСОБА_5 доповідає щодо нанесення вогневого ураження по трьом особам на території с. Одрадокам'янка Тягинської територіальної громади Херсонської області, з використанням дрона, спорядженого боєприпасом ВОГ-17 о 08.05 (російський час) з зазначенням координат Х та У. Крім того, при переписці ОСОБА_5 зазначає, що цілі ховались у кущах. Також ОСОБА_5 відправляв особі абоненту «Одесса» фрагмент публікації Бериславської РВА про поранення однієї особи у с. Одрадокам'янка. Крім того, у протоколі зафіксовано листування ОСОБА_5 з абонентом, який підписаний «ОСОБА_12», аналізом якого встановлено наступне: 11.01.2023 ОСОБА_5 на адресу вказаного вище абонента відправив фото власного паспорта та військового квитка (фото додаються). Відповідно до фото військового квитка ОСОБА_5 з 22.07.2022 проходить службу у в/ч НОМЕР_4. Також 26.06.2023 у листуванні ОСОБА_5 зафіксовано запис відеозвернення, в ході якого запис проводився на фронтальну камеру, під час якого зафіксовано обличчя особи, яка записує. Одночасно у листуванні наявні групові фото з ідентифікованими військовослужбовцями НОМЕР_3 окремої бригади спеціального призначення гу гш зс рф, що підтверджують перебування ОСОБА_5 на островах в районі н.п. Одрадокам'янка. Крім того, зафіксовано листування ОСОБА_5 з абонентом «мама», в ході якого останній висловлює невдоволення щодо опублікованої 15.03.2023 року в російському друкованому та електронному виданні (газеті) «Комсомольская правда», статті, через яку ОСОБА_5 може мати неприємності, в якій описується, що останній проходить службу в зс рф та бере участь у «сво» на території України;

- протоколом проведення негласної слідчої (розшукової) дії від 24.04.2024, передбачених ст. 264 КПК України (зняття інформації з електронних інформаційних систем) з роздруківкою вказаного документа з фотозображеннями до нього та мультимедійним оптичним носієм інформації формату DVD-R, зі збереженими на ньому в електронному вигляді файлами, відповідно до якого здійснено зняття інформації з електронної інформаційної системи інтернет-месенджера «Te1egram», а саме з акаунту, зареєстрованого за допомогою мобільного термінала НОМЕР_7, яким користується ОСОБА_13 (ідентифікована як військовослужбовець кадрового апарата в/ч НОМЕР_4 рф). У протоколі

зафіксовано листування ОСОБА_13 з абонентом, якого ідентифіковано як «ОСОБА_14», в ході аналізу листування отримано списки військовослужбовців трьох рот 1-го загону в/ч НОМЕР_4 з періодами їх перебування у так званій зоні «сво», а також список відпусток за 2023 рік. Відповідно до зазначених списків міститься інформація про період перебування у так званій зоні «сво» ОСОБА_5 (1 період – 24.08.22–03.12.2022,2 період – 17.12.2022–20.05.2023, 3 період – 27.05.2023-21.06.2023, 4 період – 28.06.2023– 11.08.2023, 5 період – 06.12.2023 по т.ч.). Крім того, отримано рапорт ОСОБА_5 про надання йому відпустки за 2024 рік (підписаний як командир відділу в/ч ОСОБА_15) [2].

Також в одному з судових рішень зазначено: *«Згідно з рапортом ВКП ЧРУП ОСОБА_23 від 02.06.2022 року, вбачається, що в ході проведення оперативно-розшукових заходів було встановлено, що до злочину можливо причетний гр. рф ОСОБА_4, ІНФОРМАЦІЯ_1, уродженець рф, Челябінська область, Чебаркульський район, с. Варламово, вул. Леніна, 11 та фотоілюстрацією до нього, де зазначені анкетні дані ОСОБА_4. Відповідно до протоколів огляду web-ресурсу від 02.06.2022 року та від 07.03.2023 року за допомогою браузера «ОСОБА_24», було оглянуто сторінки у соціальній мережі «ВК» та «ОК», де наявні фотозображення ОСОБА_4, які було скопійовано для проведення подальших слідчих дій. Згідно з інформацією ВКА ГУНП в Чернігівській області встановлені анкетні дані ОСОБА_4: дата та місце народження, адреси проживання, номери мобільних телефонів, якими користується останній та номер військової частини. Відповідно до протоколу за результатами проведення негласної слідчої (розшукової) дії зняття інформації з електронних інформаційних систем від 19.10.2023 року, вбачається, що було отримано «Форму-1» громадянина росії – ОСОБА_4, ІНФОРМАЦІЯ_1, яка долучена до протоколу. Крім того, в ході проведення слідчих (розшукових) дій встановлено, що ОСОБА_4, ІНФОРМАЦІЯ_1 є громадянином російської федерації та військовослужбовцем в/ч НОМЕР_3 (НОМЕР_4 самохідно-артилерійський полк, що входить до складу НОМЕР_5 танкової дивізії) з місцем дислокації в м. Чебаркуль, Челябинської області, російської федерації. ОСОБА_4, ІНФОРМАЦІЯ_1, станом на березень 2022 року перебував на території Чернігівської області та проходив військову службу в складі 400-го самохідно-артилерійського полку 90 танкової дивізії на посаді командира взводу у військовому званні старший лейтенант. Згідно з листом заступника командира в/ч НОМЕР_6 вбачається, що за результатами опрацювання наявні дані на військовослужбовця зс рф ОСОБА_4 з посиланням на фото. Відповідно до картографічного матеріалу вбачається, що один з номерів телефонів ОСОБА_4 (НОМЕР_7) було вперше зафіксовано 24.02.2022 року вежею стільникового зв'язку Українського мобільного оператора при перетині кордону з Україною на ділянці автомобільного пункту пропуску Грем'яч, після чого номер було помічено у Чернігівській та Київській областях. На території Новобілоуської ОТГ номер ОСОБА_4 фіксувався у період 07-12.03.2022, остання фіксація на території України 29.03.2022 в районі с. Зарубка Прилуцького району Чернігівської області. Згідно з матеріалами тимчасового доступу до інформації, яка містить охоронювану законом таємницю, а саме мобільних операторів ПрАТ «Київстар», ПрАТ «ВФ Україна», ТОВ «Лайфселл», вбачається, що працівниками УОТЗ ГУНП в Чернігівській області проведено опрацювання технічної інформації та під час аналізу було встановлено, що на час вчинення злочину за період часу з 08.03.2022 року по 13.03.2022 року військовослужбовець зс рф ОСОБА_4 перебував в зоні дії вишок мобільного зв'язку та безпосередньо у місці вчинення злочину (с. Деснянка, с. Шестовиця Чернігівського району Чернігівської області) разом із іншими військовослужбовцями зс рф. Як вбачається з листа УСБУ в Чернігівській області від 02.05.2024 року, встановлено, що громадянин російської федерації – ОСОБА_4, ІНФОРМАЦІЯ_1, на даний час постійно знаходиться на території російської федерації, а саме в с. Варламове Челябінського району Челябінської області рф»* [3];

3) умовою виокремлення конкретної людини з заданої сукупності (множинності) інших осіб є неповторність комплексу його стійких властивостей чи ознак, відображених у навколишньому середовищі, які збігаються з відповідними ознаками особи, які перевіряються.

Важливе значення у фіксації та розслідуванні воєнних злочинів в умовах збройного конфлікту має впровадження найкращих практик збирання доказової бази, зокрема тієї, що наявна у електронному вигляді, а також використання інноваційних цифрових технологій.

Частиною першою статті 99 КПК України визначено поняття та види електронних доказів. Зокрема, до них належать документи – матеріальні об'єкти, спеціально створені для збереження інформації, які містять зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості. Це можуть бути матеріали фотозйомки, звукозапису, відеозапису, а також інші носії інформації, зокрема комп'ютерні дані, зафіксовані технічними засобами [10].

Електронний документ або електронний доказ, згідно з вимогами законодавства, є відображенням оригінального документа і має юридичну силу за умови відповідності встановленим технічним та процесуальним вимогам. У контексті документування воєнних злочинів це положення відіграє важливу роль, оскільки дозволяє включати цифрові матеріали до переліку допустимих доказів у кримінальному провадженні. Саме тому критично важливим є дотримання процедур автентифікації, етапності зберігання доказів та підтвердження їх достовірності.

Крім створення баз даних та онлайн-платформ для збирання та обробки інформації, з метою збирання зазначеної категорії доказів на сьогодні широко використовується Протокол Берклі, який у 2020 році був представлений Центром прав людини Університету Берклі в Каліфорнії та Офісом Верховного комісара ООН з прав людини [5; 17]. Зазначений документ визначає мінімальні стандарти для пошуку, зберігання, аналізу та перевірки відкритих джерел інформації та фіксації воєнних злочинів. Водночас, незважаючи на те, що Протокол Берклі не є частиною національного законодавства, дотримання стандартів його використання спільно з вимогами кримінального процесу забезпечує визнання доказів допустимими у вітчизняних та міжнародних судових інстанціях.

В той же час він не єдиний, оскільки варто також враховувати норми та положення, викладені в «Керівних принципах щодо електронних доказів», представлених Радою Європи, а також міжнародний стандарт ISO/IEC 27037:2017 та його національний відповідник ДСТУ ISO/IEC 27037:2017 [5].

З метою оптимізації системи розслідувань в умовах повномасштабного вторгнення російської федерації в Україну дедалі більшої ваги набуває навчальна підготовка здобувачів освіти та співробітників органів правопорядку. На сьогодні актуальним питанням є необхідність підготовки кадрів нової формації, оскільки виклики та потреби сьогодення вимагають від співробітників правоохоронного блоку ефективного та швидкого культивування навичок та вмінь, в тому числі володіння цифровими компетенціями, які забезпечать найкращий результат роботи під час документування та розслідування воєнних злочинів з використанням новітніх технологій. Додатково в умовах сучасної війни це надасть можливість реагувати на потенційні та реальні виклики не конвенційно, а використовуючи весь набір інноваційних та асиметричних підходів та практик.

Традиційна класична модель підготовки кадрів, орієнтована переважно на юридичну базу та загальні вимоги досудового розслідування, на сьогодні вже не відповідає сучасним викликам і загрозам. Наявна потреба підготовки фахівців нового типу – проактивних, міждисциплінарних, технічно грамотних та гнучких у питанні використання цифрових інструментів, а також здатних орієнтуватися у складних умовах гібридної інформаційної війни.

Основу загальних компетентностей майбутніх спеціалістів у зазначеній галузі має становити поєднання цифрової, інформаційної, правової та аналітичної освіченості, а також критичної оцінки та інтерпретацію даних / інформації. До основоположних умінь та навичок у зазначених умовах мають належати: вміння налагоджувати дієву взаємодію (комунікацію), працювати з відкритими джерелами інформації (OSINT), перевіряти їх надійність та забезпечувати захищеність та автентичність отриманих результатів, оперувати цифровими доказами, застосовувати інструменти ідентифікації та верифікації зображень і відео (геометричні, амплітудні, частотні), геолокації, пошуку ідентифікаторів у джерелах даних, а також знання основ кримінального та міжнародного гуманітарного права, що забезпечує правову класифікацію зафіксованих фактів і розуміння механізмів подальшої правової кваліфікації дій в умовах збройного конфлікту.

Разом з цим не менш важливими є навички дотримання заходів безпеки при роботі з вказаною інформацією (так звана «цифрова гігієна» – використання VPN, анонімайзерів, фейкових акаунтів у пошуковій роботі, а також віртуальних активів для анонімізації розрахунків у межах пошуково-пізнавальної діяльності тощо), її етичної оцінки та виявлення упередженості при аналізі, доказового (перехресного) підтвердження даних з відкритих джерел, дотримання стандартів захисту прав та свобод людини і громадянина, персональних даних, а також здатність ефективно використовувати результати розслідувань у національному та міжнародному контекстах.

Також наявна потреба у розвитку вмінь та навичок спілкування в мережі «Інтернет» з об’єктами зацікавленості (HUMINT) із забезпеченням заходів конспірації, конфіденційності тощо.

Водночас проблемами, що заважають ефективній підготовці сучасних фахівців, залишаються обмежений доступ до ліцензованих інноваційних інструментів та програмних продуктів у процесі навчання, ефективної практики їх використання на конкретних кейсах та практичних прикладах, а також відсутність тренерів або інструкторів з практичним досвідом застосування цих технологій. Матеріально-технічна база часто не відповідає потребам сучасного цифрового слідства, а навчальні програми не синхронізовані з актуальними запитами правоохоронної сфери. Враховуючи значну вартість окремих програмних продуктів (зокрема, для розпізнавання облич ClearView, Artellence, роботи з великими обсягами інформації Maltego та NexusExplore тощо), наявна потреба тісної взаємодії з практичними підрозділами, які мають на озброєнні вказані спеціалізовані платформи обробки інформації та оперують ними.

Крім цього, проблемою, яка потребує розв’язання, є підвищення мотивації здобувачів освіти та співробітників органів правопорядку до опанування нових знань та навичок, зокрема й понаднормового вивчення навчальної літератури, посібників та презентацій, практичного використання отриманих знань поза основною сферою щоденної службової діяльності. Додатковою складовою підготовки є заохочення розвитку до креативного та інноваційного мислення слухачів, зокрема формування здатності генерувати нестандартні рішення, застосовувати прогностичне мислення та комплексний аналіз інформації.

Консерватизм окремих напрямів службової практики не сприяє виконанню вказаних завдань, тому керівний підхід до впровадження та застосування новітніх тенденцій є одним з найважливіших факторів ефективності у визначеній сфері.

Надзвичайно важлива роль у реалізації новітніх освітніх проєктів належить закладам вищої освіти зі специфічними умовами навчання, які здійснюють підготовку правоохоронців та інших спеціалістів за різними напрямами навчальних програм. Вищі військові навчальні заклади мають стати осередками підготовки нового покоління фахівців, здатних працювати на перетині права, інформаційних технологій та аналітики. З цією метою доцільно оновити навчальні програми, впровадити міждисциплінарні курси, а також регулярно залучати до освітнього процесу фахівців-практиків. Окремо варто розглянути можливість запровадження короткострокових спеціалізованих освітніх програм у закладах середньої освіти з метою формування базових знань у відповідних сферах у молодого покоління.

Важливою складовою також є взаємодія з правоохоронними органами, вітчизняними та міжнародними урядовими і позаурядовими організаціями (Міжнародний кримінальний суд, Організація з безпеки і співробітництва в Європі, Агентство Європейського Союзу з підготовки співробітників правоохоронних органів (CEPOL), Фонд «Safe Ukraine 2030» (Асоціація професіоналів корпоративної безпеки), Centre for information resilience (Центр інформаційної стійкості), TruthHounds тощо) та ІТ-сектором. Вказана взаємодія дозволить здобувачам освіти та співробітникам органів правопорядку отримати доступ до реальних кейсів, технологій та досвіду, а також сформувати практичні навички, що відповідатимуть реальним запитам сьогодення.

Додатково наявна потреба у запровадженні дієвої системи постійного підвищення кваліфікації співробітників, що має враховувати: тренінги з використання спеціалізованих платформ, виконання практичних завдань у межах різноманітних існуючих кейсів, спільних навчальних розслідувань, співпрацю з OSINT-компаніями, міжнародними організаціями та установами, які працюють за подібними напрямами.

Не менш важливою складовою сучасної підготовки є вивчення питань використання штучного інтелекту та машинного навчання у сфері розслідувань воєнних злочинів. Технології штучного інтелекту досить активно застосовуються в секторі безпеки і оборони. Передусім це система органів державної влади, Збройних Сил України, інших утворених відповідно до законів України військових формувань, правоохоронних та розвідувальних органів, державних органів спеціального призначення з правоохоронними функціями, сил цивільного захисту, оборонно-промислового комплексу України, діяльність яких перебуває під демократичним цивільним контролем і відповідно до Конституції та законів України за функціональним призначенням спрямована на захист національних інтересів України від загроз, а також громадяни та громадські об'єднання, які добровільно беруть участь у забезпеченні національної безпеки і оборони України [8, с. 166; 15, с. 356].

Зазначені технології відкривають нові можливості для обробки великих обсягів даних, автоматизації рутинних процесів і підвищення якості аналізу. Зокрема, штучний інтелект застосовується для автоматичного перекладу текстів з іноземних мов, транскрибування аудіо- та відеозаписів, ідентифікації облич за морфологічними ознаками та об'єктів на зображеннях, класифікації контенту, що публікується особами, які становлять оперативну зацікавленість тощо. Додатково здійснюється верифікація матеріалів із відкритих джерел, включно з виявленням монтажу, підміни артефактів файлів (метаданих і сигнатур) та геолокації. Інтеграція таких інструментів у практику правоохоронної діяльності дозволяє значно скоротити час розслідувань воєнних злочинів, підвищити достовірність зібраних доказів та оперативно реагувати на реальні та потенційні загрози. Обов'язковим компонентом відповідних компетенцій має стати оволодіння техніками деанонімізації:

- аналізом метаданих: час активності, мовленнєві шаблони, IP-адреси, user-agent;
- кореляцією поведінки: звички, стилістика повідомлень;
- збиранням технічних характеристик (браузерних сигнатур);
- аналізом DNS-запитів (процес перетворення зрозумілого для людини доменного імені на числову IP-адресу);
- аналізом WebRTC-витоків (розкриття IP-адрес);
- пошуком витоків через акаунти в соцмережах (одночасне використання браузера Tor і реального акаунту).

Висновки та перспективи подальших досліджень. Таким чином, підготовка спеціалістів, здатних здійснювати документування воєнних злочинів, є невід'ємним елементом встановлення правди та забезпечення прав жертв російської агресії на відшкодування завданої шкоди.

У історичній перспективі процес фіксації воєнних злочинів дозволить вшанувати пам'ять жертв конфлікту та посприяє формуванню «історичної правди». Також систематизовані відомості допоможуть у міжнародних трибуналах та національних судах віднайти істину, що у подальшому стане частиною національної пам'яті.

Відомо, що людина, її права і свободи становлять у сучасній державі найвищу соціальну цінність, саме на їхнє забезпечення й найповнішу реалізацію у суспільному житті має бути спрямована уся державна діяльність і насамперед діяльність у сфері державного управління [12, с. 193]. Процес документування важливий і з позиції планування глобальних безпекових стратегій, адже дозволяє детально визначити характер порушення прав людини та системність насильства, яке застосовується державою-агресором в Україні. Це необхідно робити і для напрацювання механізмів попередження воєнних злочинів у майбутньому. По суті йдеться про певний внесок в узагальнений світовий історичний досвід, який дасть змогу уникнути помилок іншим країнам світу [14].

Таким чином, оновлення моделі підготовки фахівців для виявлення та розслідування воєнних злочинів потребує глибокої переорієнтації з теоретично-правового підходу до практично-технологічного, що передбачає інтеграцію права, цифрових технологій, криміналістики та аналітики даних. Стаття акцентує увагу на нагальній потребі трансформації освітнього процесу для підготовки фахівців, здатних ефективно протидіяти воєнним злочинам у сучасних умовах гібридної війни, використовуючи передові цифрові технології. Провідну роль у цьому процесі мають відігравати заклади вищої освіти у тісній взаємодії з правоохоронними органами, громадськими організаціями та об’єднаннями, ІТ-сектором та міжнародними партнерами. Такий комплексний підхід вимагає системного оновлення знань, впровадження міждисциплінарних курсів, залучення практиків до навчального процесу, а також формування серед здобувачів мотивації до самостійного навчання, розвитку креативного та інноваційного мислення. Лише за умови синергії освіти, практики та інновацій можлива підготовка фахівців, здатних ефективно документувати воєнні злочини та застосовувати цифрові інструменти в інтересах правосуддя.

Список використаних джерел:

1. Використання інструментів та методів OSINT для отримання пошукової інформації : практ. порадник / Д.С. Зоренко та ін.. ; СБУ, Ін-т підгот. юрид. кадрів для СБУ НЮУ ім. Ярослава Мудрого. – 4-е вид. – Харків : ІПЮК для СБ України, 2023. – 36 с.
2. Вирок Великоолександрівського районного суду Херсонської області / Єдиний державний реєстр судових рішень. – 2025. – Спр. 650/3777/24 [Електронний ресурс]. – Режим доступу : https://reyestr.court.gov.ua /Review/128058801.
3. Вирок Чернігівського районного суду Чернігівської області / Єдиний державний реєстр судових рішень. – 2025. – Провадження 1-кп/748/85/25 [Електронний ресурс]. – Режим доступу : https://reyestr.court.gov.ua /Review/127524899.
4. Впровадження найкращих практик здійснення правосуддя / Вища ради правосуддя [Електронний ресурс]. – Режим доступу : https://hcj.gov.ua/news /u-vyshchiy-radi-pravosuddya-obgovoryly-vprovadzhennya-pravyl-organizaciyi-efektyvnogo.
5. Документування воєнних злочинів: як працює протокол Берклі? / Експертний центр з прав людини [Електронний ресурс]. – Режим доступу : https://ecpl.com.ua/news /dokumentuvannia-voiennykh-zlochyniv-iak-pratsiuie-protokol-berkli/.
6. *Кульчицька Л.О.* Матеріали OSINT як джерела доказів у кримінальних провадженнях за ознаками злочину агресії та воєнних злочинів / *Л.О. Кульчицька* // Цифровізація кримінального провадження: стан та перспективи : матеріали наук.-практ. круглого столу, 19 вересня – Харків, 2024. – С. 97–101.
7. *Ланде Д.В.* OSINT у кібербезпеці : навч. посіб. / *Д.В. Ланде*. – Київ : Інжиніринг, 2024. – 522 с.
8. *Оніщенко С.* Використання штучного інтелекту для розпізнавання терористичних та ворожих військових об’єктів / *С.Оніщенко, О.Лактіонов, А.Глушко* // Вісник Хмельницького національного університету. – 2024 – №3, Т. 1. – С. 166–171.
9. *Пашковський М.* Обставини, що мають значення для кримінального провадження, та належність цифрових доказів з відкритих джерел / *М.Пашковський* // Наукові перспективи. – Листопад 2024. – С. 984–998. DOI: 10.52058/2708-7530-2024-10(52)-984-998.
10. Кримінальний процесуальний кодекс України : документ № 4651-VI від 13.04.2012 [Електронний ресурс]. – Режим доступу : https://kodeksy.com.ua/kriminal_no-protsesual_ nij_kodeks_ukraini/statja-99.htm.
11. *Степанюк Р.Л.* Сучасні криміналістичні засоби та методи протидії злочинності : навч. посіб. / *Р.Л. Степанюк, В.О. Гусєва.* – Харків : ХНУВС, 2024. – 232 с.
12. Теорія держави і права : навчальний посібник/ *Н.М. Крестовська, Л.Г. Матвєєва, Я.О. Тицька та ін.* – Міжнародний гуманітарний ун-т., 2021. – 193 с.
13. *Торбас О.О.* OSINT при розслідуванні кримінальних правопорушень : підручник / *О.О. Торбас*. – Одеса : Юридика, 2024. – 180 с.
14. Чому важливо документувати воєнні злочини рф в Україні? / Правозахисна група «СІЧ» [Електронний ресурс]. – Режим доступу : https://sich-pravo.org/chomu-vazhlyvo-dokumentuvaty-voienni-zlochyny-rf-v-ukraini/.
15. *Шевчук В.М.* Роль технологій штучного інтелекту у правоохоронній діяльності та забезпеченні безпеки та обороноздатності України / *В.М. Шевчук* // Юридичний науковий електронний журнал. – 2024. – № 6. – С. 356–361.
16. AI-Powered Operations / Palantir [Electronic resource]. – Access mode : https:// www.palantir.com/.
17. Berkeley Protocol on Digital Open-Source Investigations / United Nations. DOI: 10.18356/9789210053433.

References:

1. Zorenko, D.S. and oth. (2023), *Vykorystannia instrumentiv ta metodov OSINT dlia otrymannia poshukovoi informatsii*, prakt. poradnyk SBU, 4-e vyd, IPIuK dlia SB Ukrainy, Kharkiv, 36 p.
2. Yedynyi derzhavnyi reiestr sudovykh rishen (2025), *Vyrok Velykooleksandrivskoho raionnoho sudu Khersonskoi oblasti*, No. 650/3777/24, [Online], available at: https://reyestr.court.gov.ua /Review/128058801
3. Yedynyi derzhavnyi reiestr sudovykh rishen (2025), *Vyrok Chernihivskoho raionnoho sudu Chernihivskoi oblasti*, Provadzhennia No. 1-kp/748/85/25, [Online], available at: https://reyestr.court.gov.ua /Review/127524899
4. «Vprovadzhennia naikrashchykh praktyk zdiisnennia pravosuddia», *Vyshcha rady pravosuddia*, [Online], available at: https://hcj.gov.ua/news /u-vyshchiy-radi-pravosuddya-obgovoryly-vprovadzhennya-pravyl-organizaciyi-efektyvnogo
5. «Dokumentuvannia voiennykh zlochyniv: yak pratsiuie protokol Berkli?», *Ekspertnyi Tsentr z Prav Liudyny*, [Online], available at: https://ecpl. com.ua/news/dokumentuvannia-voiennykh-zlochyniv-iak-pratsiuie-protokol-berkli/
6. Kulchytska, L. O. (2024) «Materialy OSINT yak dzherela dokaziv u kryminalnykh provadzhenniakh za oznakamy zlochynu ahresii ta voiennykh zlochyniv», *Tsyfrovizatsiia kryminalnoho provadzhennia: stan ta perspektyvy, materialy nauk.-prakt. kruhloho stolu,* 19 veres, Kharkiv, pp. 97–101.
7. Lande, D.V. (2024), *OSINT u kiberbezpetsi*, navch. pos., Inzhynirynh, Kyiv, 522 p.
8. Onishchenko, S., Laktionov, O. and Hlushko, A. (2024), «Vykorystannia shtuchnoho intelektu dlia rozpiznavannia terorystychnykh ta vorozhykh viiskovykh obiektiv», *Visnyk Khmelnytskoho natsionalnoho universytetu*, No. 3, Vol. 1, Iss. 335, pp. 166–171.
9. Pashkovskyi, M. (2024), «Obstavyny, shcho maiut znachennia dlia kryminalnoho provadzhennia, ta nalezhnist tsyfrovykh dokaziv z vidkrytykh dzherel», *Naukovi perspektyvy*, Lystopad 2024, pp. 984–998, doi: 10.52058/2708-7530-2024-10(52)-984-998.
10. Verkhovna Rada Ukrainy (2012), *Kryminalnyi protsesualnyi kodeks Ukrainy*, dokument 4651-VI vid 13.04.2012 r., [Online], available at: https://kodeksy. com.ua/kriminal_no-protsesual_ nij_kodeks_ukraini/statja-99.htm
11. Stepaniuk, R.L. and Husieva, V.O. (2024), *Suchasni kryminalistychni zasoby ta metody protydii zlochynnosti*, navch. posib, KhNUVS, Kharkiv, 232 p.
12. Krestovska, N.M., Matvieieva, L.H., Tytska, Ya. and oth. (2021), *Teoriia derzhavy i prava*, navchalnyi posibnyk, Mizhnarodnyi humanitarnyi un-t., 193 p.
13. Torbas, O.O. (2024), *OSINT pry rozsliduvanni kryminalnykh pravoporushen*, pidruchnyk, Yurydyka, Odesa, 180 p.
14. «Chomu vazhlyvo dokumentuvaty voienni zlochyny rf v ukraini?», *Pravozakhysna hrupa «SICh»*, [Online], available at: https://sich-pravo.org/chomu-vazhlyvo-dokumentuvaty-voienni-zlochyny-rf-v-ukraini/
15. Shevchuk, V.M. (2024), «Rol tekhnolohii shtuchnoho intelektu u pravookhoronnii diialnosti ta zabezpechenni bezpeky ta oboronozdatnosti Ukrainy», *Yurydychnyi naukovyi elektronnyi zhurnal*, No 6, pp. 356–361.
16. «AI-Powered Operations», Palantir, [Online], available at: https://www. palantir.com/
17. «Berkeley Protocol on Digital Open-Source Investigations», United Nations, doi: 10.18356/9789210053433.

Lukianenko S., Bondar V.

Optimisation of the training model for learners and law enforcement personnel in the detection, documentation, and pre-trial investigation of war crimes using advanced technologies (osint, humint)

Abstact. Digital technologies profoundly reshape the investigation of war crimes, broadening the spectrum of available sources of information through the development of «digital geography». At present, open-source intelligence, digital tools and evidence, artificial intelligence, and large language models are extensively employed to establish the time, location, and circumstances of crimes; to detect and identify objects; to analyze radio intercepts; to verify information; and to de-anonymize individuals. These technologies enhance the effectiveness of investigations, yet simultaneously necessitate the training of a new generation of specialists equipped with advanced digital, legal, and analytical competencies.

In this context, the proper collection and authentication of electronic evidence – as defined by current regulatory acts – acquire particular importance, as does adherence to international standards, including the Berkeley Protocol and the Council of Europe's recommendations on electronic evidence. Developing the relevant digital competencies among students and law enforcement personnel, such as OSINT skills, geolocation, data verification, digital hygiene techniques, and de-anonymization tools, is essential for the proper handling of digital materials and for improving the overall quality of the evidence base.

Equally important are the development of high-quality educational programs across different levels of education, the provision of access to specialized digital tools, interagency cooperation with international organizations and the IT sector, as well as motivation for continuous professional development. Artificial intelligence, as a modern technology, offers additional opportunities to enhance training models – particularly through the automation of digital data analysis, more accurate object identification, and the acceleration of certain forensic processes – thus contributing to the formation of specialists capable of operating effectively amid hybrid threats and information confrontation.

Keywords: war crimes; training of specialists; evidence.

Стаття надійшла до редакції 27.10.2025.