ПОГОРЕЦЬКИЙ М. А.,
доктор юридичних наук, професор,
член-кореспондент Національної
академії правових наук України,
заслужений діяч науки і техніки України,
проректор з науково-педагогічної роботи
*(Київський національний університет
імені Тараса Шевченка)*

МЕЛЕНТІ Є. О.,
кандидат технічних наук, доцент,
перший проректор
*(Національна академія
Служби безпеки України)*

УДК 343.1:343.98:004.056:004.738.5(477)»2022/2025»
DOI https://doi.org/10.32842/2078-3736/2025.4.1.36

ДОКУМЕНТУВАННЯ АТАК ДЕРЖАВИ-АГРЕСОРА НА ОБ'ЄКТИ КРИТИЧНОЇ ІНФРАСТРУКТУРИ УКРАЇНИ: МЕТОДИКА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ МУЛЬТИСЕНСОРНИХ ДАНИХ ТА ВИКОРИСТАННЯ ЙОГО РЕЗУЛЬТАТІВ У КРИМІНАЛЬНОМУ ПРОЦЕСУАЛЬНОМУ ДОКАЗУВАННІ

Стаття присвячена обґрунтуванню та розробці методики інтелектуального аналізу мультисенсорних даних для документування воєнних злочинів і використання результатів такого аналізу у кримінальному процесуальному доказуванні. Запропоновано інтегровану архітектуру програмно-апаратного комплексу (сенсорне ядро, OSINT-ядро, інтегратор даних), що забезпечує повний цикл роботи з даними: від отримання, синхронізації та алгоритмічної обробки до формування доказових пакетів, їх верифікації та стандартизації. Новизна полягає у процесуалізації технічних процедур: методика з самого проєктування «перекладає» сенсорні результати у юридично значимі цифрові докази через фіксацію метаданих, забезпечення автентичності та безперервності ланцюга збереження цифрових доказів, прозорість алгоритмічних процедур та можливість незалежної перевірки. Практичне значення полягає у скороченні часу на опрацювання великих масивів інформації, уніфікації доказових пакетів і формуванні централізованої бази цифрових доказів, що підвищує стійкість матеріалів до процесуального оскарження та полегшує судову оцінку. Методика узгоджується з вимогами кримінального процесуального законодавства України та європейськими стандартами захисту прав людини, а також із технічними настановами щодо цифрових доказів; доведено її спроможність інтегрувати результати мультисенсорного спостереження в систему доказування у справах про атаки на об'єкти критичної інфраструктури. Сформульовано підходи до SOP і валідації (precision/recall/FPR/FNR) та окреслено напрями подальшого розвитку (нейромережеві модулі, математичне моделювання, міжвідомча верифікація).

Ключові слова: *мультисенсорні дані; сенсорна інформація; цифрові докази; інтелектуальний аналіз; OSINT; ланцюг збереження; допустимість доказів; судовий контроль; критична інфраструктура; ЕІО; e-evidence; ЄСПЛ; CJEU, Верховний Суд, досудове розслідування, воєнні злочини.*

Pohoretskyi M. A., Melenti Ye. O. Documentation of the aggressor state's attacks on Ukraine's critical infrastructure: a methodology for the intelligent analysis of multisensor data and the use of its results in criminal evidentiary proceedings

The article substantiates and develops a methodology for the intelligent analysis of multisensor data to document war crimes and to use the results of such analysis in criminal evidentiary proceedings. It proposes an integrated hardware–software architecture (a sensor core, an OSINT core, and a data integrator) that supports the full data lifecycle: from acquisition, synchronization, and algorithmic processing to the creation of evidentiary packages, their verification, and standardization. The novelty lies in the proceduralization of technical operations: from the design stage, the methodology "translates" sensor outputs into legally significant digital evidence through metadata capture, assurance of authenticity and continuity of the chain of custody, transparency of algorithmic procedures, and the possibility of independent verification. The practical value consists in reducing the time required to process large volumes of information, unifying evidentiary packages, and building a centralized repository of digital evidence, which increases the materials' resilience to procedural challenges and facilitates judicial assessment. The methodology is aligned with the requirements of Ukraine's criminal procedure legislation and European human-rights standards, as well as with technical guidelines on digital evidence; its capacity to integrate the results of multisensor observation into the evidentiary system in cases concerning attacks on critical infrastructure has been demonstrated. Approaches to SOPs and validation (precision/recall/FPR/FNR) are articulated, and avenues for further development are outlined (neural-network modules, mathematical modeling, interagency verification).

Key words: *multisensor data; sensor information; digital evidence; intelligent analysis; OSINT; chain of custody; admissibility of evidence; judicial oversight; critical infrastructure; EIO; e-evidence; ECHR; CJEU; Supreme Court; pre-trial investigation, war crimes.*

Вступ. Повномасштабні збройні дії держави-агресора зумовили системні атаки на об'єкти критичної інфраструктури України, що супроводжуються появою великих, різнорідних і високодинамічних масивів даних: оптичних, акустичних, геопросторових, телекомунікаційних, а також матеріалів відкритих джерел. Ефективність досудового розслідування та судового розгляду у таких справах прямо залежить від здатності трансформувати мультисенсорну інформацію у процесуально придатні цифрові докази з дотриманням законності їх одержання, автентичності, безперервності ланцюга збереження цифрових доказів (*chain of custody*) і можливості незалежної перевірки [2; 34–39]. Натомість чинні практики часто залишаються фрагментарними, відомчо роз'єднаними й технологічно неоднорідними, що породжує ризики втрати доказової цінності (втрата/пошкодження метаданих, розсинхронізація часу, дефекти атрибуції джерела, відсутність відтворюваності алгоритмічних процедур) та ускладнює судову оцінку.

Проблемність ситуації посилюється правовими обмеженнями і гарантіями прав людини: будь-яке використання технічних засобів спостереження і доступу до інформації має відповідати стандартам справедливого судового розгляду (ст. 6 Конвенції) і поваги до приватного життя (ст. 8), у тому числі критеріям законної мети, необхідності та пропорційності втручання, наявності дієвих запобіжників від свавілля і забезпечення реальної можливості для змагальної перевірки доказів [22–26]. У національному вимірі ці вимоги кореспондують положенням КПК України щодо предмета доказування, допустимості та належності доказів, процесуальних форм їх одержання і перевірки [2], а також послідовно конкретизуються у практиці Касаційного кримінального суду у складі Верховного Суду (законність джерела, санкціонування доступу, безперервність ланцюга збереження цифрових доказів, технічна цілісність і відтворюваність) [27–30].

Додатковий вимір становить транскордонність цифрових слідів: релевантні дані часто перебувають у володінні провайдерів або сервісів, розміщених поза Україною, що потребує застосування інструментів взаємної правової допомоги та режимів, установлених правом ЄС (Європейський ордер на розслідування; інструменти e-evidence), із дотриманням процесуальних гарантій і меж доступу до даних, визначених судовою практикою CJEU [12–16; 17–21]. Відсутність уніфікованих процедур інтеграції таких даних з національними сенсорними потоками ускладнює їхнє подальше використання у суді.

Методологічно-інженерний розрив проявляється у браку єдиної моделі даних і стандартних операційних процедур: не визначено мінімально необхідні метадані для різних типів сенсорів; не уніфіковано правила синхронізації часу і простору, хешування та підписування; не кодифіковано вимоги до журналювання дій та аудиту; відсутні стандартизовані формати доказових пакетів та вимоги до відтворюваності алгоритмічної обробки (опис моделей/версій/параметрів, контрольні seed, протоколи валідації), що суперечить профільним настановам ISO/NIST/ENFSI та підриває доказову сталість матеріалів [34–39]. Суттєвим є й управлінсько-організаційний компонент: потребуються сталі механізми говернансу (розмежування ролей і доступів, протоколи інцидентів, ретенція/мінімізація даних, DPIA/PIA у світлі GDPR/ePrivacy) та міжвідомчої верифікації результатів [15–16; 34–39].

Отже, дослідницька проблема полягає у відсутності цілісної процесуально-орієнтованої методики, яка б із моменту проєктування забезпечувала «перекладність» технічного результату у юридично значимий цифровий доказ у справах про атаки на критичну інфраструктуру: через уніфікацію архітектури збору й обробки даних, SOP, моделі доказового пакета, прозорість алгоритмів і валідовані метрики якості (precision, recall, F1, FPR, FNR), із гарантіями законності, автентичності та відтворюваності, сумісними з КПК України, практикою ЄСПЛ/CJEU і технічними міжнародними стандартами [2; 12–16; 17–26; 27–30; 34–39]. Саме усунення зазначеного розриву є передумовою для формування доказової бази, здатної витримати судовий контроль у національних та міжнародних юрисдикціях і забезпечити реальну відповідальність за воєнні злочини проти об'єктів критичної інфраструктури.

Аналіз останніх досліджень і публікацій. Проблематика цифрових доказів і технічних засобів їх одержання розвивається у двох взаємопов'язаних напрямах: (а) поглиблення доктрини електронних доказів і процесуальних стандартів їх допустимості та належності; (б) інтенсивна еволюція мультисенсорних і алгоритмічних технологій, що генерують масиви даних, релевантні для кримінального провадження. У фундаментальних працях із цифрової криміналістики сформовано усталений «канон» збирання, фіксації, верифікації та представлення електронної інформації з акцентом на надійність джерела, відтворюваність процедур і документування ланцюга збереження [40; 41]. Доктринальний вимір зазначеного канону розгорнуто в працях під ред. С. Мейсона (S. Mason) і Д. Сенга (D. Seng), де визначено межі та умови використання електронних доказів і електронних підписів у суді, а також наслідки процесуальних дефектів цифрових артефактів [42; 43]. Сучасний порівняльно-правовий контекст системно представлено у виданні «Кембриджський довідник з цифрових доказів у кримінальних розслідуваннях» *(The Cambridge Handbook of Digital Evidence in Criminal Investigations)*, зокрема щодо ролі онлайн-провайдерів, транскордонного доступу до даних та «придатності до суду» цифрових слідів [44], у міждисциплінарній статті про введення цифрових джерел з відкритих ресурсів до судового процесу [45] та іншипрацях зарубіжних та вітчизняних фахівців.

Сукупність суміжних техніко-технологічних досліджень засвідчує перехід від «одноканальних» рішень до мультисенсорних підходів і мультимодальної інтеграції (ф'юзії) даних; узагальнення оглядових та емпіричних праць показує, що належне об'єднання гетерогенних потоків (оптичних, акустичних, геопросторових тощо) підвищує інформативність реконструкції події, однак потребує жорсткої часової синхронізації, уніфікованого нормування метаданих і формалізованих правил кореляції [59].

Паралельно стрімко розвиваються методи атрибуції та протидії маніпуляціям: еталонні дослідження FaceForensics++ і Noiseprint окреслили підходи до виявлення редагувань

і встановлення «відбитка» джерела знімання [47; 48], а узагальнювальні огляди deepfake-форензіки засвідчили зміщення від одномодальних до мультимодальних детекторів і зафіксували «розрив поколінь» між лабораторними датасетами та «польовими» прикладами із соцмереж [46]. Практико-орієнтовані стандарти ENFSI у сфері аутентифікації зображень задають репродуковані протоколи експертиз [39].

Водночас актуальний науково-теоретичний дискурс одностайно підкреслює: технічний результат має бути від початку «перекладений» у процесуальні форми. Саме тому методологічні документи: Берклійський протокол з цифрових розслідувань на основі відкритих джерел (Berkeley Protocol on Digital Open Source Investigations); Настанови щодо ідентифікації, збирання, отримання та збереження цифрових доказів (Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence – ISO/IEC 27037); Настанови Національного інституту стандартів і технологій США (*National Institute of Standards and Technology* – NIST) наполягають на вбудованості у ланцюг збереження процедур ідентифікації джерела, хеш-фіксації, часової синхронізації, мінімізації персональних даних і відтворюваності перевірок [34–38]. Європейський правовий контекст – як нормативний: Європейський ордер на розслідування (European Investigation Order – EIO); електронні (цифрові) докази (e-evidence) [12–16], так і прецедентний (Суд Європейського Союзу (Court of Justice of the European Union – CJEU): *M.N. (EncroChat)*, *H.K.*, *La Quadrature*, *SpaceNet*; Європейський суд з прав людини (ЄСПЛ): *Roman Zakharov*, *Big Brother Watch*, *Centrum för Rättvisa*, *Benedik*, *Teixeira de Castro*) [17–26] – задає критерії необхідності/пропорційності, межі зберігання та доступу до даних і процесуальні гарантії, з якими має кореспондувати будь-яка інженерія цифрових доказів. На національному рівні релевантні підходи відображено і в українській судовій практиці Касаційного кримінального суду у складі Верховного Суду (ККС ВС) (допустимість електронних доказів, вимоги до фіксації технічних засобів, ланцюг збереження) [27–30].

В українській науковій доктрині питання теорії кримінального процесуального доказування, критеріїв допустимості та ролі судового контролю у забезпеченні справедливого й належного доказування послідовно розроблені в наукових працях, де висвітлено концептуальне переосмислення доказування, вплив права ЄС на національне судочинство та специфіку використання новітніх технологій у справах про воєнні злочини [53–57].

Прикладні аспекти фіксації наслідків збройної агресії відображені також в українських галузевих публікаціях і методичних рекомендаціях (огляд місця події, використання 3D-сканерів, застосування ГІС/космічних технологій) [49; 50; 58; 59], а технічні класифікації та довідкові матеріали підсилюють ідентифікацію засобів ураження та обстановки події [51].

Узагальнюючи, зазначимо, що у наукових джерелах уже наявні ключові компоненти майбутньої процесуально-орієнтованої системи: (1) доктринальні стандарти допустимості та надійності електронних доказів [42–45]; (2) відтворювані технічні протоколи OSINT/цифрової криміналістики і ланцюга збереження цифрових даних [34–38; 39]; (3) перевірені інструменти мультисенсорної інтеграції й анти-маніпуляційної перевірки [46–48; 59]. Водночас на сьогодні відсутнє уніфіковане атрибуційно-реєстраційне рішення, яке б уже на етапі *проєктування програмно-апаратної архітектури систем фіксації, оброблення та збереження цифрових даних* гарантувало процесуальну легалізацію технічних результатів і їх належне приєднання до матеріалів кримінального провадження: фіксацію походження, хеш-ідентифікацію, часові мітки, процедури мінімізації, міжканальну кореляцію та метадані, придатні для негайного долучення та використання як доказів у кримінальном у провадженні, у тому числі й щодо воєнних злочинів. Запропонована методика спрямована на усунення зазначеної прогалини та поєднує: (1) *мультисенсорний аналіз* різнорідних цифрових потоків і артефактів – відео- та фотозображень (у т. ч. супутникових і з БПЛА), аудіозаписів, геопросторових даних глобальних навігаційних супутникових систем (GNSS), телекомунікаційних і мережевих журналів (CDR, журнали подій/log-files), системних метаданих (EXIF тощо); і (2) *процесуальні фільтри* європейського та національного права – критерії належності, допустимості, достовірності та достатності доказів; перевірку атрибуції

джерела та безперервності ланцюга збереження цифрових даних (chain of custody); забезпечення цілісності й незмінності (хеш-ідентифікація, часові мітки); вимоги пропорційності втручання та мінімізації персональних даних; судовий контроль і можливість незалежної верифікації цифрових даних. Методика призначена для документування атак держави-агресора на об'єкти критичної інфраструктури України, а результати її інтелектуального мультисенсорного аналізу можуть бути використані у кримінальному процесуальному доказуванні воєнних злочинів відповідно до чинного законодавства України та європейських стандартів.

Підсумовуючи, варто зауважити, що наведені в статті та інші авторські праці у цій сфері становлять методологічне підґрунтя дослідження. Доктринальний блок і процесуальні критерії обґрунтовано в низці наукових публікацій [52–57 та ін.], тоді як техніко-аналітичний контур і підходи до оцінювання систем безпеки та національної безпеки – у відповідних працях і колективних дослідженнях [51; 60 та ін.].

Постановка завдання. Мета статті полягає в обґрунтуванні та розробці методики інтелектуального аналізу сенсорної інформації для документування воєнних злочинів і визначенні процесуальних механізмів її використання у кримінальному провадженні з урахуванням критеріїв допустимості, ролі судового контролю та міжнародних стандартів.

Завдання дослідження зводяться до розробки методики інтелектуального аналізу сенсорної інформації для документування воєнних злочинів, визначення процесуальних механізмів її застосування, формулювання критеріїв допустимості та належності отриманих даних, з'ясування ролі судового контролю, узагальнення міжнародних стандартів і підготовки пропозицій щодо вдосконалення національного законодавства та практики розслідування.

Результати дослідження. Сенсорна інформація у широкому розумінні являє собою дані, зафіксовані технічними, цифровими чи біометричними пристроями, що відображають фізичні, хімічні, електронні або інші процеси та можуть бути перетворені у форму, придатну для аналізу й використання у кримінальному провадженні. Її особливістю є об'єктивний характер, оскільки первинна фіксація відбувається автоматизовано, без безпосереднього втручання людини, що мінімізує ризики спотворення. Водночас у процесуальному контексті сенсорні дані не можуть залишатися «сирими»: вони потребують спеціальної обробки, верифікації та інтерпретації, щоб відповідати вимогам належності, допустимості та достовірності доказів [2]. Саме тому в основі методики закладено поняття *мультисенсорного середовища* – інтегрованої системи збору даних із різнорідних джерел (оптичних, акустичних, геолокаційних, цифрових логів, свідчень очевидців та відкритих джерел). Таке середовище дає змогу отримати багатовимірну картину подій, здійснити перехресну перевірку відомостей та забезпечити більшу доказову силу у кримінальному провадженні.

Принципи інтелектуального аналізу даних у межах цієї методики визначаються потребою у стандартизованій та юридично надійній трансформації інформаційних потоків. Першим виступає *принцип інтегративності*, що вимагає узгодженого поєднання даних від різних сенсорів та джерел у єдиній базі. Другим є *принцип синхронізації*, відповідно до якого часові та просторові параметри даних мають бути гармонізовані для створення цілісної реконструкції подій. Третім є *принцип алгоритмічної прозорості*, який передбачає документованість кожного етапу автоматизованої обробки даних та можливість незалежної перевірки результатів судом чи експертами [3; 22–26; 34–39]. Четвертий – *принцип контекстуальності*, що полягає у використанні сенсорних даних лише у взаємозв'язку з іншими доказами, оскільки їх ізольована інтерпретація може призвести до хибних висновків [18]. Нарешті, обов'язковим є *принцип верифікації та автентичності*, який забезпечується через фіксацію ланцюга збереження цифрових доказів, застосування хешування та цифрових підписів, що відповідає сучасним міжнародним підходам до збереження цифрових доказів [23].

Важливою складовою концептуальних засад є роль інтеграції різнорідних сенсорів. Використання фізичних сенсорів (камери, акустичні чи сейсмічні датчики) дозволяє отримати об'єктивні параметри події; цифрові сенсори (системні журнали, телекомунікаційні дані) розкривають цифровий слід злочину; агентурні сенсори (свідчення очевидців,

потерпілих чи інсайдерів) додають якісно новий контекст; OSINT-джерела забезпечують широту охоплення та дають змогу підтвердити чи спростувати інформацію з технічних каналів [12]. Лише у поєднанні ці елементи утворюють цілісну доказову картину, яка відповідає стандартам справедливого судочинства і може бути використана як у національних, так і міжнародних процесах. Таким чином, інтеграція різнорідних сенсорів у межах методики інтелектуального аналізу сенсорної інформації забезпечує перехід від розрізнених сигналів до системно організованих цифрових доказів, здатних витримати процесуальну перевірку та стати основою притягнення винних до відповідальності.

Сенсорне ядро програмно-апаратного комплексу є базовою складовою запропонованої методики інтелектуального аналізу сенсорної інформації для документування воєнних злочинів. Воно виконує функцію первинного збору, фільтрації та синхронізації даних, отриманих від різнорідних сенсорів, забезпечуючи безперервність та достовірність інформаційного потоку. Саме на цьому рівні відбувається формування початкового масиву відомостей, який згодом перетворюється на структуровані цифрові докази.

Архітектурно сенсорне ядро складається з кількох взаємопов'язаних модулів. Першим є модуль *отримання даних*, що акумулює інформацію з оптичних, акустичних, сейсмічних, температурних, геолокаційних, біометричних та цифрових сенсорів. Особливістю є можливість паралельного збирання даних з десятків і навіть сотень сенсорів, що дозволяє максимально повно відобразити обставини події та створити багатовимірну інформаційну модель. Другим модулем є система *попередньої обробки*, яка включає усунення шумів, корекцію технічних похибок і приведення сигналів до уніфікованих форматів, придатних для подальшої інтелектуальної обробки.

Ключовим елементом сенсорного ядра виступає модуль *синхронізації даних.* Його завдання полягає у забезпеченні часової та просторової узгодженості інформації, оскільки лише за умови точного встановлення моменту та місця фіксації події дані можуть мати належну доказову силу [2]. Для цього використовуються системи часових міток (timestamping), геолокаційні протоколи (GPS, Galileo), а також алгоритми зіставлення сигналів з різних сенсорів. Синхронізація дозволяє виявити як підтверджувальні збіги, так і суперечності між даними, що уможливлює їх процесуальну оцінку з позицій достовірності та допустимості [3; ; 22–26; 34–39].

Сенсорне ядро також передбачає застосування *edge-комп'ютерів* і контролерів, які здійснюють локальну обробку та попереднє агрегування даних безпосередньо у місці їх виникнення. Це суттєво скорочує час реакції та знижує ризики втрати інформації через перевантаження каналів зв'язку. Водночас така архітектура підсилює інформаційну безпеку, оскільки дані передаються до центральних вузлів уже у відфільтрованому й зашифрованому вигляді [12].

У підсумку сенсорне ядро забезпечує перетворення фрагментарних і часто хаотичних потоків сенсорної інформації на узгоджений масив, що відповідає процесуальним вимогам і стає основою для подальшої інтеграції з OSINT-даними та агентурними джерелами. Його функціонування гарантує, що доказові матеріали матимуть чітке походження, коректно зафіксовані параметри часу та місця, а також технічно підтверджену цілісність, що унеможливлює маніпуляції та забезпечує їхню придатність для судового розгляду [18].

OSINT-ядро у структурі програмно-апаратного комплексу виконує завдання збирання, систематизації та попередньої обробки даних із відкритих джерел, які мають ключове значення для документування воєнних злочинів. Його роль полягає у доповненні сенсорної інформації цифровими свідченнями, що циркулюють у відкритому інформаційному середовищі, та у створенні умов для перехресної перевірки даних, отриманих від фізичних і цифрових сенсорів.

Насамперед основу OSINT-ядра складає *джерельна база*, яка включає публікації у засобах масової інформації, повідомлення в соціальних мережах, матеріали з відео- та фотофіксацією подій, дані супутникового моніторингу, офіційні повідомлення державних інституцій, бази даних міжнародних організацій і правозахисних ініціатив. Збирання цих

матеріалів має не лише технічний, але й правовий аспект: кожне джерело потребує оцінки на предмет автентичності, достовірності та допустимості для використання у кримінальному провадженні [2].

Другим компонентом є *інструменти збору даних*, які забезпечують автоматизований моніторинг і вилучення інформації з відкритих ресурсів. До них належать системи веб-сканування, парсингу та аналізу соціальних мереж, алгоритми пошуку зображень і відео з функціями геолокації та часової прив'язки, а також спеціалізовані сервіси для відстеження матеріалів у DarkNet. Застосування цих інструментів дозволяє не лише оперативно виявляти повідомлення про ймовірні воєнні злочини, а й співвідносити їх із сенсорними даними, що надходять до сенсорного ядра.

Важливою складовою OSINT-ядра є *модулі попередньої обробки*, завданням яких є очищення, нормалізація та стандартизація отриманих даних. Інформація з відкритих джерел часто містить значний рівень шумів, дублювання та нерелевантних повідомлень. Тому модулі попередньої обробки здійснюють фільтрацію контенту, видалення дублікатів фото- та відеоматеріалів, корекцію метаданих, а також перетворення різнорідних форматів у єдину структуру. Це створює уніфіковану інформаційну базу, придатну для подальшого інтелектуального аналізу і формування доказових пакетів [3; 22–26; 34–39].

OSINT-ядро виконує не лише допоміжну, а й критично важливу функцію для верифікації: співставлення відкритих джерел із сенсорними потоками дозволяє підвищити достовірність доказів та відповідати стандарту сукупності доказів, який закріплений у практиці ЄСПЛ [18]. Таким чином, інтеграція OSINT-ядра у програмно-апаратний комплекс забезпечує широту охоплення інформаційного поля, дозволяє оперативно реагувати на появу нових свідчень воєнних злочинів і формує додатковий рівень захисту від інформаційних маніпуляцій.

Інтегратор даних є завершальною та системоутворювальною ланкою архітектури програмно-апаратного комплексу, що поєднує результати роботи сенсорного та OSINT-ядер у єдину структуру. Його ключове призначення полягає у трансформації різнорідних інформаційних потоків у формалізовані цифрові докази, які відповідають процесуальним критеріям належності, допустимості та достовірності [2].

Функціонування інтегратора передбачає кілька взаємопов'язаних етапів. По-перше, здійснюється *надійне збереження даних*, що включає їх захист від несанкціонованого доступу та забезпечення відмовостійкості системи. При цьому застосовуються криптографічні методи, хешування та цифрові підписи, які унеможливлюють підміну чи модифікацію інформації без залишення сліду [23]. По-друге, відбувається *аналітичне зіставлення та перекласифікація* даних: інформація, отримана від сенсорів і з відкритих джерел, співставляється між собою для виявлення підтверджувальних збігів або суперечностей, а також для уточнення походження та значущості відомостей. По-третє, інтегратор формує *пакети потенційних цифрових доказів*, які проходять процедуру верифікації через порівняння між різними каналами та джерелами. Такий підхід забезпечує багаторівневу перевірку достовірності та підвищує стійкість доказової бази до процесуальних заперечень у суді [18].

Особливу роль відіграє етап *формування попередніх рішень і рекомендацій* для органів досудового розслідування. Алгоритми інтегратора дозволяють не лише структурувати дані, а й генерувати аналітичні висновки – наприклад, про ймовірний тип озброєння, місце запуску ракети чи співвідношення часових параметрів подій. Це істотно скорочує час реагування слідчих підрозділів та оптимізує їхню роботу в умовах масового документування воєнних злочинів [12]. Завершальним етапом є *створення єдиного доказового пакету* – інтегрованого результату багаторівневої обробки даних, який відповідає як технічним, так і процесуальним вимогам, та може бути поданий до судових чи міжнародних інституцій.

Таким чином, інтегратор даних забезпечує завершеність циклу інтелектуального аналізу: від первинної фіксації сигналів різними сенсорами й відкритими джерелами – до формування уніфікованої бази цифрових доказів воєнних злочинів, придатної для судового розгляду. Його роль полягає не лише в технічному поєднанні інформаційних потоків,

а й у створенні гарантій для їх процесуальної використаності, що узгоджується з сучасними стандартами справедливого судочинства та міжнародними зобов'язаннями України [5].

Перелік технічних і процесуальних запобіжників охоплює судове санкціонування доступу, перевірку пропорційності втручання, забезпечення автентичності та цілісності даних (включно з «ланцюгом володіння»), документування алгоритмічних процедур і можливість незалежної перевірки результатів, що відповідає стандартам Конвенції та усталеній практиці ЄСПЛ і CJEU, а також міжнародним методичним настановам щодо цифрових доказів [18; 23; 34–39].

Виходячи з попередньо окреслених передумов – наявних вихідних даних, сформованої логіки обробки, передавання та збереження сенсорних даних, а також визначеного функціонального призначення складових системи – можна побудувати процесно-орієнтовану модель програмно-апаратного комплексу, що становитиме методичне підґрунтя інтелектуального аналізу сенсорної інформації для документування воєнних злочинів (рис. 1).

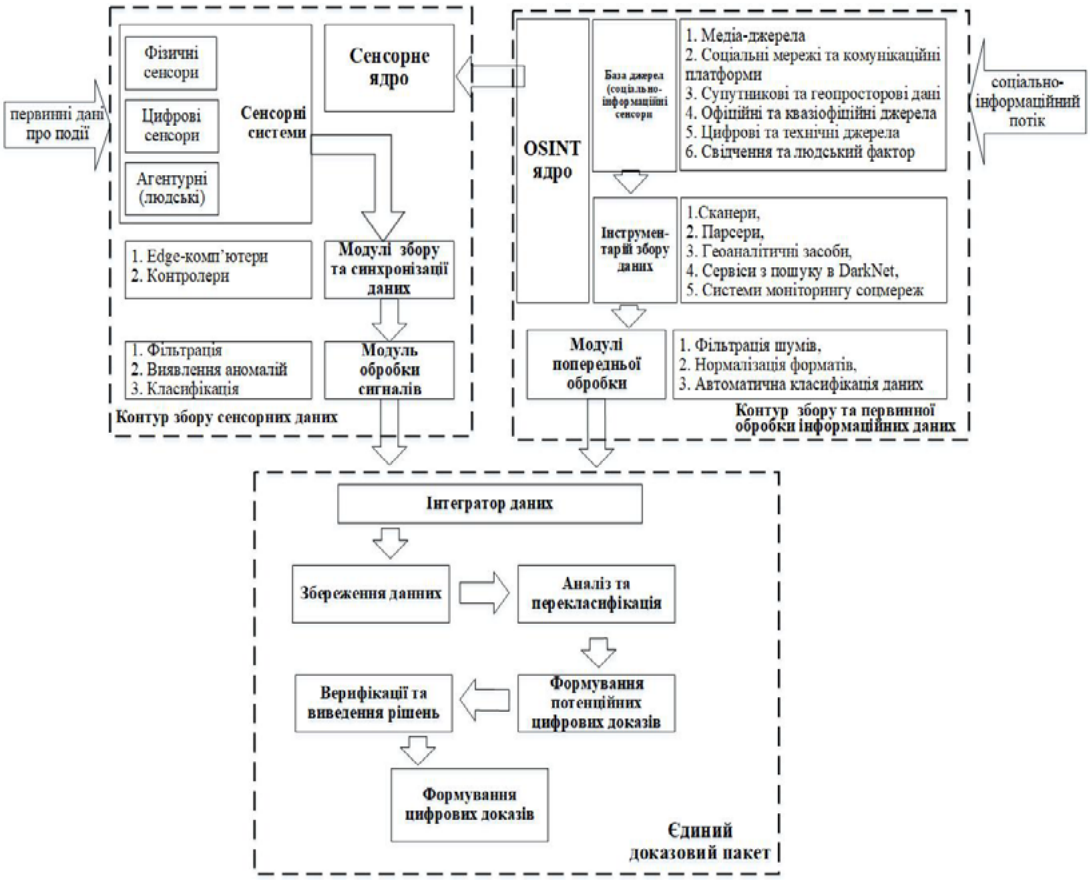

Рис. 1. Модель програмно-апаратного комплексу з інтелектуального аналізу сенсорної інформації для документування воєнних злочинів

Запропонована методика інтегрує тришарову архітектуру (сенсорне ядро, OSINT-ядро, інтегратор), повний цикл опрацювання даних (отримання → синхронізація → алгоритмічна обробка/класифікація → формування доказових пакетів → верифікація/стандартизація) та процесуальні фільтри допустимості використання цих даних як доказів. Усі дії супроводжуються фіксацією метаданих, часовою й геопросторовою узгодженістю, контролем автентичності та ланцюга збереження цифрових доказів, що забезпечує відповідність

вимогам КПК України і міжнародним стандартам ЄСПЛ/CJEU, а також технічним протоколам ISO/NIST/ENFSI [2; 12; 18; 23; 34–39]. Перехресна верифікація між сенсорними й відкритими джерелами мінімізує хибні висновки, а прозорість алгоритмів і можливість незалежної перевірки гарантують процесуальну придатність результатів (*див. також процесуальні положення і європейські стандарти*). Практичний ефект – прискорення кореляції та зіставлення великих масивів даних, уніфікація доказових пакетів і формування централізованої бази цифрових доказів, що розвантажує оперативн та слідчі підрозділи органів правопорядку та полегшує судовий розгляд кримінальних справ про воєнні злочини [2; 12; 18; 23].

Етап отримання інформації становить вихідну й водночас визначальну фазу методики інтелектуального аналізу сенсорної інформації для документування воєнних злочинів. Його завдання полягає у фіксації максимально широкого спектра даних, що відображають обставини вчинення злочину, та створенні умов для їх подальшої систематизації і використання як цифрових доказів.

Джерела інформації на цьому етапі мають комплексний характер і охоплюють кілька категорій. По-перше, це *фізичні сенсори*, до яких належать оптичні пристрої (цифрові камери, тепловізори, прилади нічного бачення), акустичні датчики (мікрофони, ультразвукові сенсори), сейсмічні прилади (геофони, акселерометри), температурні й хімічні датчики. Вони забезпечують первинну реєстрацію подій – вибухів, обстрілів, руйнувань, присутності токсичних речовин тощо, тобто фактично фіксують матеріальні сліди злочину у реальному часі [2].

По-друге, до джерел належать *цифрові сенсори*, які відображають інформаційні процеси у мережевому середовищі: журнали подій у комп'ютерних системах, дані телекомунікаційних операторів, логи мобільних пристроїв, записи систем відеоспостереження, а також інформація з безпілотних літальних апаратів. Ця категорія даних особливо важлива для відтворення цифрового сліду воєнних злочинів та дозволяє ідентифікувати зв'язки між виконавцями, засобами ураження та наслідками їх застосування [3; ; 22–26; 34–39].

Третю групу становлять *агентурні сенсори*, тобто людина як джерело даних: свідки, потерпілі, експерти чи інсайдери. Вони фіксують обставини події в суб'єктивному вимірі, проте їхні показання набувають підвищеної доказової сили, коли підтверджуються матеріалами з фізичних і цифрових сенсорів.

Четвертою групою виступають *OSINT-джерела*, що формуються у відкритому інформаційному просторі: повідомлення у соціальних мережах, публікації в ЗМІ, супутникові знімки, бази даних міжнародних організацій. Такі матеріали особливо цінні для верифікації подій, які відбувалися поза зоною доступу офіційних структур, і дозволяють підкріпити сенсорні дані незалежними свідченнями [18].

Важливо підкреслити, що етап отримання інформації передбачає одночасне дотримання двох взаємопов'язаних вимог: *технічної достовірності* (точність фіксації, відсутність спотворень, збереження метаданих) та *процесуальної придатності* (законність отримання, документованість джерела, можливість перевірки й відтворюваності). Лише поєднання цих умов робить зібрані дані придатними для подальшої обробки й використання у кримінальному процесі.

Таким чином, перший етап методики створює фундамент для всього подальшого інтелектуального аналізу: саме якість, повнота й автентичність зібраної сенсорної та відкритої інформації визначає перспективу її використання як цифрового доказу у національному та міжнародному судочинстві.

Етап алгоритмічної обробки та класифікації є центральним у методиці інтелектуального аналізу сенсорної інформації, оскільки саме тут відбувається перетворення попередньо синхронізованих і стандартизованих потоків даних у структуровані інформаційні блоки, які мають процесуальне значення. Завдання цього етапу полягає у виявленні закономірностей, відсіканні нерелевантних відомостей та формуванні узгодженої системи ознак події, що може бути використана для доведення складу воєнного злочину.

Алгоритмічна обробка передбачає застосування методів *сигнальної та контентної фільтрації*, що дають змогу усунути залишкові шуми, спотворення чи дублювання даних. На цьому рівні використовуються також алгоритми розпізнавання образів, акустичного аналізу, виявлення аномальних подій, які дозволяють відокремити звичайні фонтові сигнали від подій, що мають ознаки злочину. Наприклад, автоматизовані системи можуть розпізнавати характерні звуки вибухів чи пострілів, визначати тип озброєння за акустичним або візуальним слідом, а також виявляти факти застосування заборонених методів ведення війни [2; 12].

Класифікація даних здійснюється шляхом їх розподілу за визначеними категоріями: тип воєнного злочину, місце і час його вчинення, спосіб реалізації, наслідки для цивільних чи об'єктів критичної інфраструктури. У цьому процесі застосовуються *нейромережеві та машинно-навчальні алгоритми*, які забезпечують здатність системи до самоудосконалення та підвищення точності класифікації на основі накопиченого масиву даних. Особливу увагу приділено прозорості алгоритмічних процедур: усі кроки мають бути задокументовані й відтворювані, що є передумовою їх допустимості у кримінальному провадженні [3; 23].

Правовий контекст допустимості результатів алгоритмічної обробки та їх оцінювання у сукупності з іншими доказами визначається стандартами Конвенції (статті 6 і 8) і практикою ЄСПЛ, а також вимогами до прозорості процедур, автентичності та збереження ланцюга цифрових доказів, відображеними у рішеннях CJEU та технічних/методичних настановах (ISO/IEC 27037, NIST, ENFSI) [18; 23; 34–39].

Таким чином, етап алгоритмічної обробки та класифікації виконує подвійну функцію: з одного боку, він оптимізує роботу слідчих органів через автоматизацію рутинних процесів, а з іншого – створює процесуально придатний масив доказів, який здатний витримати судовий контроль і сприяти притягненню до відповідальності за воєнні злочини.

Етап формування доказових пакетів є логічним завершенням алгоритмічної обробки та класифікації сенсорної інформації, оскільки саме тут результати інтелектуального аналізу набувають процесуально завершеної форми й стають придатними для використання у кримінальному провадженні. Його завдання полягає у поєднанні відфільтрованих, класифікованих і верифікованих даних у цілісні інформаційні блоки, що відповідають вимогам належності, допустимості та достовірності [2].

Формування доказового пакета передбачає кілька ключових дій. По-перше, здійснюється *структурування даних* за категоріями воєнних злочинів: атаки на цивільних осіб, обстріли критичної інфраструктури, застосування заборонених засобів ведення війни тощо. Це дозволяє вибудувати логіку події відповідно до кваліфікаційних ознак, визначених КК України та міжнародним гуманітарним правом [12]. По-друге, здійснюється атрибуція джерел і обставин: до пакета включають не лише результати сенсорних вимірювань, а й відомості про спосіб і час їх одержання, технічні характеристики засобів фіксації, а також інформацію про документування та забезпечення безперервності ланцюга збереження цифрових доказів *(chain of custody).* [23].

Важливою складовою є *верифікація та підтвердження автентичності:* кожен доказовий пакет проходить процедуру зіставлення між різними джерелами – сенсорними даними, матеріалами OSINT, свідченнями очевидців чи потерпілих. Така багаторівнева перевірка підвищує достовірність доказів і відповідає стандарту оцінки сукупності доказів, що послідовно застосовується в практиці ЄСПЛ [18]. У випадках, коли дані підтверджуються декількома незалежними каналами, їхня доказова сила істотно зростає.

Таким чином, формування а збереження доказових пакетів здійснюються відповідно до стандартизованих протоколів опису метаданих і криптографічного захисту із забезпеченням безперервності ланцюга збереження цифрових доказів; вимоги щодо автентичності, цілісності та відтворюваності закріплені в профільних міжнародних методичних настановах (ISO/IEC 27037, публікації NIST, ENFSI) та підтверджені практикою міжнародних судових інституцій [23; 34–39].

Етап верифікації та стандартизації є завершальною ланкою методики інтелектуального аналізу сенсорної інформації, що забезпечує надійність та процесуальну придатність

отриманих цифрових доказів. Його головне завдання полягає у підтвердженні автентичності даних, перевірці їх цілісності та приведенні у форму, яка відповідає міжнародним і національним стандартам доказування.

Верифікація передбачає багаторівневу перевірку походження та достовірності даних. Насамперед здійснюється підтвердження автентичності файлів через фіксацію метаданих, застосування хеш-функцій та електронних цифрових підписів. Важливим є також збереження безперервного ланцюга збереження цифрових доказів, що дозволяє відстежити кожен етап руху інформації – від моменту її отримання сенсорами чи з відкритих джерел до інтеграції в доказовий пакет [23]. Крім того, верифікація включає співставлення даних між різними каналами: фотозображення з камер можуть підтверджуватися відео- чи акустичними матеріалами, а дані з соціальних мереж – незалежними сенсорними записами. Така кореляція відповідає принципу оцінки доказів у сукупності, який закріплений у практиці ЄСПЛ [18].

Стандартизація спрямована на уніфікацію структури й формату даних для їх подальшого використання у національному та міжнародному кримінальному процесі. Вона охоплює нормалізацію форматів файлів, уніфікацію метаданих, присвоєння унікальних ідентифікаторів кожному доказу, а також застосування міжнародних протоколів зберігання та передачі цифрових доказів (зокрема стандартів, що імплементовані у вітчизняне законодавство [2; 3]). Це дозволяє не лише гарантувати сумісність системи з іноземними юрисдикціями, але й знизити ризики відхилення доказів через формальні процесуальні підстави.

Поєднання верифікації та стандартизації формує кінцевий результат у вигляді *уніфікованого цифрового доказу,* який має чітко визначене походження, підтверджену автентичність і закріплений у стандартизованому форматі. Такий доказ не лише відповідає вимогам кримінального процесуального законодавства України, але й узгоджується з європейськими стандартами доказування та практикою міжнародних трибуналів [12].

У підсумку етап верифікації та стандартизації створює основу для довгострокового використання цифрових доказів у кримінальному провадженні. Він забезпечує їхню інтегрованість, відтворюваність і захист від маніпуляцій, що є критично важливим у процесах документування воєнних злочинів і представлення доказової бази в міжнародних судових інституціях.

Застосування методики передбачає узгоджені стандартні операційні процедури (SOP), які забезпечують належність, допустимість та відтворюваність цифрових матеріалів. Для всіх типів даних фіксуються обов'язкові метадані (унікальний ідентифікатор, дата і час у форматі ISO 8601/UTC, геолокація WGS-84 із зазначенням точності, опис пристрою/ПЗ та версії, умови фіксації, формат файлу, первинні хеш-значення), здійснюється синхронізація часу (GNSS/NTP) і просторової прив'язки, а також забезпечуються автентичність і цілісність через хешування (SHA-256/512), кваліфіковані електронні підписи/мітки часу, журналювання дій у режимі append-only і безперервність ланцюга збереження цифрових доказів від моменту отримання до подання. Оригінали зберігаються у незміненому вигляді (RAW/без втрат, якщо можливо) поряд із форензійними копіями з контрольними сумами; під час будь-яких перетворень зберігаються логи обробки. Такі вимоги відповідають профільним методичним настановам і практикам (Berkeley Protocol; ISO/IEC 27037; NIST SP 800-86, 800-101; ENFSI Best Practice Manual) [34–39].

Для відео- та фотоматеріалів фіксуються нативні контейнери/RAW і повні EXIF/XMP-метадані (модель і серійний номер сенсора, оптика, експозиційні параметри, геомітки, узгоджені таймкоди). Після зняття обчислюються хеші, накладаються е-підписи і мітки часу; будь-які операції редагування заборонені на оригіналах і виконуються лише на копіях із протоколюванням. Автентичність перевіряється методами судово-технічної аутентифікації зображень за керівництвами ENFSI/NIST із фіксацією слідів рекомпресії й редагування [34–39].

Для акустичних записів застосовуються безвтратні формати (напр., WAV 48/96 kHz, 24-bit), фіксуються координати/висота/орієнтація мікрофонів і параметри калібрування. Синхронізація каналів забезпечується опорним імпульсом та GNSS/NTP; первинні доріжки

хешуються і підписуються до будь-якої фільтрації, а «сирі» файли зберігаються для незалежної перевірки [34–38].

Для телекомунікаційних журналів (дані операторів/мережеві логи) обов'язково документуються правові підстави доступу, отримуються первинні формати провайдера разом із підписаними експортами (CSV/JSON), а часові мітки узгоджуються до UTC з фіксацією джерела часу і можливого дрейфу. Набори даних хешуються пакетно, підписуються провайдером і приймаючою стороною, а приймання-передавання відображається у chain of custody [34–38].

Для супутникових знімків та матеріалів UAV фіксуються параметри платформи і сенсора, час (UTC), координати WGS-84, роздільність/GSD та метеоумови; для БпЛА додатково – телеметрія (трек польоту, висота, швидкість, курс). Обробка (ортокорекція, мозаїкування) виконується з повним логуванням і збереженням сирих даних; усі продукти хешуються і підписуються [34–39].

Для OSINT-матеріалів зберігаються первинні джерела (URL, дата/час доступу, веб-архів/скріншот, оригінальні медіафайли за наявності), технічні атрибути (тип платформи, ідентифікатори акаунтів, EXIF/MIME, розмір), здійснюється часово-просторова верифікація (геолокація за орієнтирами, тінями, метеоумовами), а також крос-перевірка з іншими каналами (сенсорні записи, телеком-дані). Кожен крок фіксується у журналі OSINT-дій для забезпечення відтворюваності й незалежної перевірки [34–39].

У межах запропонованої методики застосовується система метрик та процедур валідації, спрямована на забезпечення відтворюваності результатів і контрольованої якості обробки. Узагальнювальна таблиця *«Показники якості алгоритмічної обробки»* охоплює щонайменше три типові завдання: (1) класифікацію типу ураження за відеозаписами; (2) класифікацію типу ураження за акустичними слідами; (3) кореляцію телекомунікаційних журналів із сенсорними подіями. Для кожного завдання фіксуються: опис наборів даних та умов (походження, баланс класів, критерії відбору, розподіл train/validation/test); показники точності *precision, recall* та інтегральний *F1*; показники помилок *FPR* (false positive rate) і *FNR* (false negative rate); середні значення з 95% довірчими інтервалами й порогові критерії прийнятності; застереження щодо ризиків хибних спрацьовувань і пропусків. Окремо документуються процедура маркування (джерела істини), міжрозмічувальна узгодженість (*к Коена*), а також параметри відтворення (версії програмного забезпечення та моделей, контрольні seed, конфігурації апаратури). Розрахунки здійснюються на відкладених наборах; усі проміжні артефакти (скрипти, журнали, контрольні суми) включаються до пакета валідації. Вимоги до структури таблиці, метаданих і документування узгоджуються з профільними методичними настановами та найкращими практиками (*Berkeley Protocol; ISO/IEC 27037; NIST SP 800-86, 800-101; ENFSI Best Practice Manual*) [34–39].

Міжвідомча верифікація передбачає незалежне відтворення результатів щонайменше двома уповноваженими суб'єктами у «засліпленому» режимі на репрезентативній вибірці з фіксованими правилами доступу та мінімізації даних; процедура включає формування вибірки й протокол анотування, відтворення обробки відповідно до SOP із повною фіксацією параметрів, перехресне зіставлення обчислених *precision/recall/F1* та *FPR/FNR* з визначенням допустимого діапазону розбіжностей, аудит журналів і первинних хешів для підтвердження автентичності, підписання результатів кваліфікованими електронними підписами з часовими мітками та внесенням до реєстру ланцюга дій; у разі перевищення порогових значень – повторне калібрування та повторна валідація. Такий підхід забезпечує перевірюваність і змагальність у сенсі статті 6 Конвенції, дотримання принципів необхідності/пропорційності та мінімізації втручання у приватне життя за статтею 8 (практика ЄСПЛ і позиції CJEU), а також підсилює аргументацію процесуальної допустимості цифрових доказів відповідно до вимог КПК України [22–26; 34–39; 2].

У кримінальному процесі результат інтелектуального аналізу сенсорної інформації може набути статусу доказу лише за умови дотримання критеріїв допустимості, які

є фундаментальними гарантіями справедливого судочинства. Відповідно до положень Кримінального процесуального кодексу України, доказами визнаються фактичні дані, отримані в передбаченому законом порядку, які підлягають перевірці та оцінці судом [2; 22–26; 34–39]. Це правило однаковою мірою поширюється і на цифрові докази, включно із сенсорними даними.

Першим і базовим критерієм є *законність джерела походження*. Сенсорна інформація повинна бути зібрана уповноваженим суб'єктом із дотриманням процесуальних норм, що визначають порядок проведення слідчих та негласних слідчих (розшукових) дій. Порушення цього правила (наприклад, використання даних, здобутих без ухвали слідчого судді чи поза межами визначених законом повноважень) автоматично позбавляє такий матеріал статусу допустимого доказу [3; 22–26; 34–39].

Другим критерієм є *збереження автентичності й цілісності даних.* Для сенсорної інформації, яка зазвичай існує у цифровій формі, це означає необхідність забезпечення ланцюга збереження цифрових доказів та застосування технічних засобів перевірки незмінності (хешування, електронні підписи, блокчейн-рішення). Лише у випадку, коли автентичність даних може бути підтверджена й відтворена, вони здатні витримати судовий контроль [23].

Третій критерій – *належність і релевантність*. Сенсорні дані повинні мати безпосередній зв'язок із предметом доказування, визначеним статтею 91 КПК України, тобто підтверджувати обставини вчинення злочину, особу винного, форму його вини, наслідки діяння тощо. Використання випадкових або не пов'язаних із предметом доказування відомостей суперечить засадам процесуальної економії та порушує право на справедливий розгляд справи [2].

Четвертим критерієм є *надійність та достовірність джерела*. У практиці ЄСПЛ неодноразово підкреслювалося, що використання цифрових доказів можливе лише за умови доведеної автентичності й можливості перевірки (наприклад, рішення у справах *Bykov v. Russia* та *Roman Zakharov v. Russia*). Це положення прямо кореспондує з національним принципом оцінки доказів на основі внутрішнього переконання суду при обов'язковому врахуванні їх достовірності [18].

П'ятий критерій – *можливість незалежної перевірки*. Алгоритмічні результати аналізу сенсорних даних повинні бути відтворюваними, тобто інший суб'єкт із належною кваліфікацією має мати змогу перевірити застосовані методи та підтвердити отримані результати. Це особливо важливо в умовах використання штучного інтелекту та машинного навчання, де «чорні скриньки» без пояснення логіки прийняття рішень несуть загрозу для процесуальної допустимості доказів [5].

Національна практика Касаційного кримінального суду у складі Верховного Суду послідовно конкретизує ці вимоги до електронних (сенсорних) доказів: наголошується на законності джерела та санкціонуванні доступу, належному процесуальному оформленні, фіксації походження й безперервності ланцюга збереження цифрових доказів, технічній цілісності матеріалів і можливості їх незалежної перевірки; пор. постанови від 20.02.2018 у справі № 750/4139/15-к (ЄДРСР № 72460327), від 30.09.2020 у справі № 563/1118/16-к (ЄДРСР № 91998609), від 04.09.2019 у справі № 369/3713/18 (ЄДРСР № 84120855), від 04.06.2025 у справі № 686/20198/22 (ЄДРСР № 128309294) [27–30]. Зазначений підхід кореспондує тестам ЄСПЛ за статтями 6 і 8 Конвенції щодо справедливого судового розгляду та необхідності/пропорційності втручання у приватне життя (забезпечення законної мети, достатніх і дієвих процесуальних гарантій, відтворюваності й перевірюваності цифрових матеріалів) [22–26].

Отже, сенсорна інформація набуває статусу цифрового доказу лише за одночасного виконання всіх зазначених критеріїв: законність отримання, автентичність і цілісність, належність і релевантність, достовірність та відтворюваність. Дотримання цих умов гарантує не лише процесуальну придатність матеріалів, але й їхню стійкість до оскарження у суді, у тому числі в міжнародних юрисдикціях.

Судовий контроль у кримінальному провадженні є ключовим інструментом забезпечення законності, справедливості та дотримання прав людини, особливо коли йдеться про використання новітніх технологій і сенсорних даних як цифрових доказів. В умовах воєнного стану, коли масштабність і терміновість документування воєнних злочинів значно зростає, саме судовий контроль стає гарантією того, що інтелектуальний аналіз сенсорної інформації застосовується не довільно, а в межах процесуальних приписів та з дотриманням міжнародних стандартів [2; 3].

Передусім судовий контроль проявляється у формі *санкціонування доступу до даних*, що отримуються через сенсорні системи, зокрема телекомунікаційні мережі, інформаційні системи чи пристрої спостереження. Встановлення таких обмежень є виявом балансу між інтересами держави у сфері безпеки та правами людини на приватність і захист персональних даних. Суддя повинен перевіряти наявність законних підстав, достатність обґрунтувань і пропорційність втручання у права особи, що повністю узгоджується з практикою ЄСПЛ щодо застосування заходів таємного стеження (*Roman Zakharov v. Russia*, *Big Brother Watch and Others v. the United Kingdom*) [18].

Другим важливим аспектом є *контроль за дотриманням критеріїв допустимості* цифрових доказів. Суд, розглядаючи клопотання сторін чи вирішуючи питання про допустимість матеріалів у процесі, має оцінювати, чи було забезпечено автентичність даних, чи збережено «ланцюг володіння» (chain of custody), чи задокументовані всі етапи збору та обробки інформації, зокрема алгоритмічні процедури [23]. Такий підхід не лише гарантує прозорість використання новітніх технологій, а й мінімізує ризики маніпуляцій або підміни даних.

З урахуванням цього ККС ВС підкреслює, що судовий контроль охоплює не лише попереднє санкціонування доступу до даних, а й наступну перевірку дотримання умов їх одержання й обробки, включно з підтвердженням технічної цілісності, належної атрибуції джерела та релевантності до предмета доказування; пор. постанови від 20.02.2018 у справі № 750/4139/15-к, від 30.09.2020 у справі № 563/1118/16-к, від 04.09.2019 у справі № 369/3713/18, від 04.06.2025 у справі № 686/20198/22 [27–30]. Такий підхід узгоджується з практикою ЄСПЛ щодо тесту «необхідності й пропорційності» та вимоги ефективних запобіжників від свавільного втручання (статті 6 і 8 Конвенції) [22–26].

Третім напрямом судового контролю є *оцінка пропорційності та релевантності використання методики.* Суд має перевіряти, чи справді обраний спосіб аналізу відповідав меті доказування у конкретному провадженні, чи не призвів він до надмірного збору нерелевантної інформації, яка може порушувати права сторонніх осіб. У цьому контексті суд виконує роль арбітра між інтересами безпеки та індивідуальними свободами, запобігаючи перетворенню інтелектуальних технологій на інструмент масового стеження.

Зрештою, судовий контроль гарантує, що результати інтелектуального аналізу сенсорної інформації мають не лише технічну, але й процесуальну легітимність. Він забезпечує інтеграцію цієї методики у систему доказування відповідно до засад верховенства права та справедливого судочинства. В умовах воєнного стану це набуває особливого значення, адже дозволяє поєднати ефективність реагування на воєнні злочини з дотриманням прав людини та міжнародних зобов'язань України [5].

Використання методики інтелектуального аналізу сенсорної інформації у кримінальному провадженні має безпосереднє значення для забезпечення прав людини, оскільки воно поєднує два ключові вектори: ефективність розслідування воєнних злочинів та гарантії справедливого судочинства. З одного боку, методика дозволяє оперативно збирати, систематизувати й аналізувати великі масиви даних про злочини агресора, створюючи основу для притягнення винних до відповідальності; з іншого – вона закладає процесуальні запобіжники, що унеможливлюють свавільне чи непропорційне втручання у права особи.

По-перше, застосування сенсорної інформації, здобутої у мультисенсорному середовищі, сприяє *реалізації права потерпілих на ефективне розслідування.* Воно гарантує, що злочини проти цивільного населення чи критичної інфраструктури не залишаться безкарними, а зібрані матеріали відповідатимуть стандартам доказування у міжнародних судах,

зокрема в Міжнародному кримінальному суді. Так забезпечується право на справедливість, відновлення порушених прав і репарацію шкоди [12].

По-друге, методика інтелектуального аналізу забезпечує *пропорційність втручання у приватне життя.* Вона побудована на принципах синхронізації, автентифікації та алгоритмічної прозорості, що дозволяє уникати надмірного збору нерелевантних даних, а також гарантувати, що кожне втручання має чітку правову підставу та обґрунтовану мету. Цей підхід узгоджується з практикою ЄСПЛ, яка вимагає, аби будь-які заходи спостереження чи збору інформації мали законну мету, були необхідними в демократичному суспільстві та супроводжувалися належними гарантіями від зловживань (*Klass v. Germany*, *Roman Zakharov v. Russia*) [18].

По-третє, методика створює умови для *забезпечення права на захист.* Оскільки алгоритмічна обробка даних супроводжується документуванням кожного етапу, сторона захисту має можливість ознайомитися з методами збору та аналізу, перевірити їх відтворюваність і ставити під сумнів достовірність чи релевантність отриманих результатів. Це відповідає засаді змагальності процесу й гарантує баланс між обвинуваченням і захистом [2; 22–26; 34–39].

Таким чином, методика інтелектуального аналізу сенсорної інформації не лише посилює ефективність документування воєнних злочинів, а й виступає процесуальним інструментом забезпечення прав людини. Її застосування у воєнних провадженнях гарантує поєднання інтересів національної безпеки з міжнародними стандартами верховенства права, що є критично важливим для довіри до українського правосуддя як всередині держави, так і на міжнародному рівні [5; 23].

Європейські стандарти становлять нормативну та практичну основу, без урахування якої неможливо оцінювати допустимість і належність сенсорних даних як цифрових доказів у кримінальному провадженні. Їх джерелами виступають право Європейського Союзу, практика Європейського суду з прав людини та позиції Суду Європейського Союзу, що у своїй сукупності формують багаторівневу систему гарантій прав людини у сфері збирання й використання інформації.

Право Європейського Союзу регулює питання цифрових доказів через кілька ключових актів. Насамперед ідеться про Директиву 2014/41/ЄС щодо Європейського ордера на розслідування (ЕІО), яка передбачає можливість транскордонного доступу до цифрових даних і встановлює вимогу їхнього збору та передачі виключно у законний спосіб із гарантіями захисту прав особи. Додаткове значення має пропонований Регламент ЄС про електронні докази (e-evidence), який закріплює правила прямого доступу правоохоронних органів держав-членів до інформації, що зберігається у провайдерів послуг, але водночас зобов'язує забезпечувати принципи пропорційності, судового контролю та захисту персональних даних [2; 22–26; 34–39].

Європейський суд з прав людини (ЄСПЛ) у своїй практиці неодноразово наголошував, що використання цифрових даних у кримінальному провадженні повинно відповідати стандартам статей 6 і 8 Конвенції про захист прав людини і основоположних свобод. Це означає, що держава зобов'язана забезпечити, по-перше, право на справедливий судовий розгляд, зокрема можливість сторони захисту перевіряти достовірність і допустимість цифрових доказів, а по-друге – право на повагу до приватного життя, що передбачає наявність належних гарантій від свавільного чи непропорційного втручання у сферу персональних даних. У рішеннях *Roman Zakharov v. Russia*, *Bykov v. Russia*, *Big Brother Watch and Others v. the United Kingdom* Суд прямо вказав, що будь-яке масове чи непрозоре використання технічних засобів збору інформації суперечить принципу верховенства права [18].

Суд Європейського Союзу (CJEU) у низці рішень сформулював підхід до допустимості та пропорційності збору цифрових даних. У справі *Digital Rights Ireland* він визнав несумісним із правом ЄС масове зберігання телекомунікаційних даних без належних процесуальних гарантій. У справі *La Quadrature du Net* Суд підкреслив, що навіть в умовах загроз національній безпеці держави-члени повинні забезпечувати чіткі межі втручання у приватне життя та дотримуватися принципу пропорційності. Ці позиції безпосередньо стосуються

використання сенсорних технологій, оскільки підкреслюють: цифрові дані можуть застосовуватися у кримінальному процесі лише тоді, коли забезпечені гарантії їхнього законного походження, автентичності та перевірюваності [23].

У сукупності право ЄС, практика ЄСПЛ та CJEU створюють багаторівневий стандарт: збирання й використання сенсорних даних можливе лише за наявності законних підстав, пропорційності обмежень, ефективного судового контролю та забезпечення права сторін на перевірку доказів. Ці вимоги мають бути інтегровані у національне кримінальне судочинство України для того, щоб результати інтелектуального аналізу сенсорної інформації визнавалися не лише в українських судах, але й у міжнародних юрисдикціях.

Міжнародні кримінальні трибунали сформували важливий прецедентний досвід у використанні цифрових і сенсорних даних як доказів, що має безпосереднє значення для розробки національної методики інтелектуального аналізу. Застосування новітніх технологій у цих юрисдикціях відбувалося у відповідь на виклики документування масових порушень міжнародного гуманітарного права, які супроводжувалися масштабними руйнуваннями та численними жертвами серед цивільного населення.

Найяскравішим прикладом є практика *Міжнародного кримінального трибуналу для колишньої Югославії (ICTY),* де активно застосовувалися супутникові знімки, матеріали авіаційної розвідки та цифрові записи переговорів. Суд у справі *Prosecutor v. Karadžić* визнав такі матеріали допустимими доказами, за умови підтвердження їхнього походження, автентичності та достовірності. Вони дозволили довести факти масових обстрілів цивільних об'єктів і знищення населених пунктів, що кваліфікувалося як воєнні злочини.

У практиці *Міжнародного кримінального трибуналу для Руанди (ICTR)* значну роль відігравали відео- та аудіоматеріали, які документували злочини геноциду. Важливим процесуальним стандартом стало підтвердження ланцюга збереження цифрових доказів такими матеріалами: суд вимагав детально описувати шлях кожного файлу від моменту його фіксації до подання у судовому засіданні. Це гарантувало їхню допустимість і захищало від маніпуляцій.

Особливе значення має досвід *Міжнародного кримінального суду (МКС).* В умовах сучасних конфліктів він активно використовує цифрові та OSINT-джерела – супутникові знімки, матеріали соціальних мереж, мобільні додатки для збору свідчень. Наприклад, у справах, що стосуються злочинів у Дарфурі та Малі, МКС визнавав дані з цифрових платформ доказами за умови їхньої ретельної перевірки на автентичність та відтворюваність. При цьому Суд наголошував на необхідності незалежної експертної оцінки алгоритмів аналізу, що використовувалися для обробки масивів даних.

Сьогодні дедалі більшого значення набуває застосування *Берклійського протоколу щодо цифрових відкритих джерел розслідувань*, розробленого під егідою ООН. Його положення активно використовуються міжнародними правозахисними організаціями та слідчими органами МКС для документування злочинів в Україні. Протокол визначає стандарти перевірки автентичності цифрових доказів з відкритих джерел, їхньої збереженості та належної верифікації, що унеможливлює їхню відмову на стадії судового розгляду.

Таким чином, міжнародні трибунали виробили універсальні підходи, які мають стати орієнтиром і для національної практики: (1) забезпечення автентичності та цілісності даних через «ланцюг володіння»; (2) незалежна перевірка алгоритмів обробки; (3) документування кожного етапу збору й аналізу; (4) обов'язкове співставлення цифрових матеріалів з іншими доказами у справі. Інтеграція цих стандартів у вітчизняне кримінальне судочинство є передумовою визнання українських матеріалів на рівні міжнародних юрисдикцій.

Імплементація міжнародних підходів до використання цифрових і сенсорних доказів у національну практику передбачає поєднання нормативної гармонізації, процесуальної стандартизації та технологічної уніфікації інструментів документування воєнних злочинів. Насамперед йдеться про адаптацію вимог права ЄС та практики ЄСПЛ щодо законності джерела, пропорційності втручання та ефективного судового контролю, аби результати

інтелектуального аналізу сенсорної інформації відповідали критеріям належності, допустимості, достовірності та достатності доказів у кримінальному провадженні України [2; 18]. На законодавчому рівні доцільно деталізувати порядок одержання, зберігання та оцінки цифрових доказів сенсорного походження, зокрема закріпивши вимоги до фіксації метаданих, часової та геопросторової синхронізації, а також до процедур підтвердження автентичності, включно з фіксацією ланцюга збереження цифрових доказів (hash-ідентифікатори, кваліфіковані електронні підписи, протоколи незмінності) [3; 23]. Процесуальною опорою імплементації має стати запровадження уніфікованих стандартних операційних процедур (SOP) для слідчих і прокурорів: від моменту отримання даних із фізичних, цифрових, агентурних і OSINT-сенсорів – до формування доказових пакетів та їх подання до суду, із чітким розмежуванням ролі судового контролю на етапах доступу до інформації, перевірки пропорційності заходів і оцінки допустимості результатів алгоритмічної обробки [2; 18; 23]. Технологічна складова імплементації охоплює створення сумісних із міжнародними юрисдикціями форматів і реєстрів цифрових доказів, уніфікацію сховищ і протоколів передачі даних, а також використання сертифікованих інструментів для аудиту алгоритмів, що забезпечує відтворюваність і незалежну перевірку висновків інтелектуального аналізу [23]. У воєнних провадженнях необхідно синхронізувати класифікацію подій і ознак складів злочинів із міжнародними стандартами, щоб забезпечити відповідність доказової бази вимогам як національних судів, так і потенційних міжнародних процесів щодо злочинів, пов'язаних з атаками на цивільних і об'єкти критичної інфраструктури [12]. Науково-методичну основу імплементації становлять напрацьовані вітчизняною доктриною підходи до кримінального процесуального доказування та використання новітніх технологій, які пропонують логіку інтеграції мультисенсорних даних у систему доказів і моделі їх процесуальної легітимації в судах України [51; 52–57; 60]. У підсумку, послідовна гармонізація норм, процедуралізація практик та уніфікація технічних рішень забезпечують те, що сенсорні дані, оброблені за методикою інтелектуального аналізу, визнаються процесуально придатними й стійкими до оскарження як у національному, так і міжнародному вимірі [2; 18; 23].

Впровадження методики інтелектуального аналізу сенсорної інформації у практику документування воєнних злочинів матиме комплексний вплив на діяльність слідчих органів та судів. Насамперед очікується суттєве *скорочення часу на збирання й обробку даних.* Умови воєнного стану характеризуються надзвичайно великими масивами інформації – від супутникових знімків і даних БПЛА до цифрових логів та повідомлень у соціальних мережах. Використання інтелектуальних алгоритмів дозволить автоматизувати первинну фільтрацію, синхронізацію та класифікацію цих потоків, зменшуючи навантаження на слідчих підрозділів і підвищуючи оперативність реагування [2; 12].

Другим очікуваним результатом є *підвищення достовірності та стійкості доказової бази до процесуального оскарження*. Завдяки запровадженню процедур автентифікації, збереженню ланцюга цифрових доказів та стандартизації даних, кожен цифровий доказ матиме підтверджене походження та чітко задокументовану історію обробки [23]. Це мінімізує ризики відхилення доказів у судах та забезпечує їх відповідність як національним, так і міжнародним стандартам допустимості [18].

Для судів ключовим ефектом стане *можливість роботи з більш структурованими та зрозумілими доказовими матеріалами*. Інтелектуальний аналіз сенсорної інформації дозволяє перетворювати хаотичні потоки сигналів на доказові пакети, де чітко визначені час, місце, спосіб та наслідки воєнного злочину. Це полегшує оцінку доказів на основі їх сукупності й підвищує обґрунтованість судових рішень, що особливо важливо з огляду на вимогу до мотивованості судових актів у практиці ЄСПЛ [18].

Крім того, впровадження методики сприятиме *уніфікації стандартів документування воєнних злочинів* на рівні органів досудового розслідування, прокуратури та судів. Це забезпечить узгодженість практики, скорочення кількості процесуальних помилок і створить підґрунтя для міжнародного визнання зібраних матеріалів. Для України, яка вже перебуває

у фокусі міжнародних розслідувань злочину агресії та воєнних злочинів, така уніфікація має особливу вагу, адже дозволяє подавати докази до міжнародних інституцій у форматі, сумісному з їхніми процесуальними вимогами [12].

Сукупний ефект упровадження методики полягає у підвищенні оперативності роботи органів досудового розслідування, у стійкості та процесуальній легітимності цифрових доказів завдяки забезпеченню законного походження, автентичності та безперервності ланцюга збереження цифрових доказів, а також в узгодженні практики слідства і суду з європейськими стандартами EIO/e-evidence та критеріями оцінки доказів у практиці ЄСПЛ і CJEU [2; 12; 18; 23].

Одним із ключових очікуваних результатів упровадження методики інтелектуального аналізу сенсорної інформації є розвантаження слідчих підрозділів, які у воєнний час працюють в умовах критичного перевантаження. Масштаби злочинів, вчинених державою-агресором, щодня формують тисячі інформаційних одиниць – від уламків боєприпасів і цифрових слідів у мережі до свідчень потерпілих та даних із відкритих джерел. Без належної автоматизації їх обробка вимагає значних людських і часових ресурсів, що знижує ефективність розслідувань та створює ризики втрати доказової інформації.

Методика дозволяє інтегрувати різнорідні потоки даних у єдину систему та автоматизувати їхнє попереднє сортування, класифікацію й синхронізацію. Це означає, що значна частина рутинних завдань – від перевірки автентичності цифрових файлів до формування метаданих і створення попередніх доказових пакетів – виконується безпосередньо програмно-апаратним комплексом [2; 23]. У такий спосіб слідчі звільняються від технічно трудомісткої роботи й можуть зосередитися на аналітичній та процесуальній діяльності: допитах, формуванні версій, координації з прокурором та підготовці матеріалів до суду.

Крім того, застосування методики створює передумови для *оптимізації кадрового потенціалу* органів досудового розслідування. Оскільки частина завдань виконується автоматично, зменшується потреба у значній кількості технічних фахівців, а натомість зростає роль спеціалістів, здатних оцінювати результати інтелектуальної обробки з процесуальної точки зору. Це сприяє підвищенню якості доказування та відповідності зібраних матеріалів вимогам кримінального процесу [3; ; 22–26; 34–39].

Важливим наслідком є також *зменшення ризиків професійного вигорання та помилок* серед слідчих. Постійне перевантаження справами та обсягами інформації призводить до зниження уважності, що може стати підставою для втрати чи спотворення доказів. Автоматизовані алгоритми, що працюють за принципами прозорості та відтворюваності, знижують ці ризики, одночасно підвищуючи довіру до результатів розслідувань [18].

Застосування методики раціоналізує розподіл ресурсів у слідчих підрозділах: автоматизує попереднє сортування, синхронізацію та верифікацію даних, зменшує частку ручних операцій, вивільняє час для процесуальних дій і підвищує якість доказування завдяки стандартизованим доказовим пакетам та контрольованому «ланцюгу володіння» [2; 23].

Формування уніфікованої бази цифрових доказів воєнних злочинів є одним із найважливіших практичних результатів упровадження методики інтелектуального аналізу сенсорної інформації. Умови воєнного стану та масовість злочинів агресора зумовлюють необхідність переходу від фрагментарного збирання матеріалів до створення централізованої системи, яка забезпечує їх повноту, автентичність і доступність для перевірки.

Уніфікована база виконує кілька ключових функцій. Насамперед вона забезпечує *систематизацію доказів*, отриманих із різнорідних сенсорів, OSINT-джерел та агентурної інформації, у єдиному цифровому просторі. Завдяки цьому створюється цілісна картина подій, що дозволяє простежити хронологію та причинно-наслідкові зв'язки між окремими злочинами [2; 22–26; 34–39]. Другою функцією є *верифікація даних:* зберігання у базі відбувається з фіксацією метаданих, електронними підписами та хеш-ідентифікаторами, що забезпечує збереження ланцюга цифрових доказів та виключає можливість несанкціонованої модифікації інформації [23].

Особливе значення має *стандартизація доказових матеріалів,* що уможливлює їх використання не лише у національному судочинстві, але й у міжнародних кримінальних процесах. Уніфікація форматів файлів, протоколів збереження й передачі даних відповідає сучасним вимогам практики ЄСПЛ і міжнародних трибуналів, які визнають лише ті цифрові докази, що можуть бути перевірені та відтворені незалежними експертами [18].

Крім того, база цифрових доказів виконує функцію *оперативного доступу для уповноважених органів* – слідчих, прокурорів, експертів і суддів. Це скорочує час на пошук і аналіз матеріалів, сприяє узгодженості процесуальних дій і створює умови для спільної роботи з міжнародними партнерами. Така база може стати важливим елементом інтеграції України до європейського простору правосуддя, де питання доказування злочинів проти людяності та воєнних злочинів мають надзвичайну актуальність [12].

Уніфікована база цифрових доказів виконує функції централізованого зберігання та стандартизації метаданих, забезпечує автентичність і цілісність інформації (через криптографічний контроль і безперервність ланцюга збереження цифрових доказів), надає оперативний доступ уповноваженим суб'єктам і гарантує міжнародну сумісність доказових матеріалів відповідно до підходів ЄСПЛ і CJEU та профільних методичних настанов (ISO/IEC 27037, NIST, ENFSI) [18; 23; 34–39].

Подальший розвиток методики інтелектуального аналізу сенсорної інформації для документування воєнних злочинів нерозривно пов'язаний із впровадженням передових технологій обробки даних, серед яких провідне місце посідають алгоритмічні комплекси, штучні нейронні мережі та математичне моделювання. Вони здатні суттєво розширити аналітичні можливості програмно-апаратного комплексу, підвищити точність класифікації подій і зменшити ризик помилкових інтерпретацій.

Алгоритмічні комплекси забезпечують автоматизацію обробки великих масивів даних у реальному часі. Йдеться про розпізнавання вибухів за акустичними слідами, ідентифікацію типів озброєння за візуальними характеристиками уламків, виявлення аномалій у поведінці мережевих систем чи аналіз траєкторій обстрілів. Їхня інтеграція у процес доказування дає змогу значно скоротити час між подією та формуванням доказового пакета, що критично важливо для воєнних проваджень [2; 22–26; 34–39].

Нейромережі відкривають нові можливості для виявлення прихованих закономірностей у сенсорних даних. Вони здатні навчатися на великих масивах уже задокументованих злочинів і в подальшому з високою точністю ідентифікувати аналогічні випадки. Наприклад, нейромережі можуть автоматично відрізняти наслідки ударів ракетного чи артилерійського озброєння, співвідносити часові й просторові параметри атак, а також прогнозувати подальші сценарії злочинних дій. Використання таких технологій повинно супроводжуватися процедурою алгоритмічної прозорості та можливістю незалежної перевірки результатів, щоб гарантувати їхню процесуальну допустимість [18].

Математичне моделювання дозволяє реконструювати події воєнних злочинів, виходячи з неповних або фрагментарних даних. Створення моделей траєкторій ракет, сейсмічних карт ударів чи теплових полів руйнувань дає змогу відтворити механізм події та визначити ймовірних виконавців. Такий підхід підсилює доказову базу, особливо коли безпосередні сенсорні дані є частковими або пошкодженими [23].

У перспективі подальші дослідження мають бути спрямовані на інтеграцію цих технологій у єдину систему, яка дозволить не лише документувати вже вчинені злочини, а й виконувати **прогностичні функції**: виявляти підготовку нових атак, аналізувати вразливість об'єктів критичної інфраструктури та формувати попереджувальні сигнали для органів безпеки. Таким чином, удосконалення методики через алгоритмічні комплекси, нейромережі та математичне моделювання не лише посилить ефективність доказування, але й сприятиме розбудові комплексної системи національної безпеки [12].

Розроблена методика інтелектуального аналізу сенсорної інформації для документування воєнних злочинів має багатовимірний практичний ефект. Її впровадження забезпечує істотне підвищення ефективності діяльності органів досудового розслідування, оскільки

дозволяє скоротити час на обробку масових потоків даних, автоматизувати рутинні процеси та розвантажити слідчих підрозділів для виконання аналітичних і процесуальних завдань [2; 12]. Водночас ця методика створює умови для формування уніфікованої бази цифрових доказів воєнних злочинів, яка відповідає міжнародним стандартам допустимості та автентичності, забезпечує збереження ланцюга цифрових доказів й підвищує стійкість доказів до процесуального оскарження [23].

Завдяки структурованості та прозорості аналітичних процедур, результати інтелектуальної обробки сенсорних даних стають зрозумілими й доступними для перевірки судами, що сприяє зміцненню принципу змагальності й гарантує справедливість судових рішень у воєнних провадженнях [18]. Крім того, методика закладає основу для довгострокового розвитку кримінального процесуального доказування в умовах гібридних загроз: використання алгоритмічних комплексів, нейромереж і математичного моделювання відкриває нові перспективи як у частині підвищення точності реконструкції подій, так і в аспекті превентивного прогнозування злочинів.

Узагальнюючи, можна констатувати, що впровадження методики забезпечує системний прорив у документуванні воєнних злочинів: вона одночасно посилює ефективність слідства, підвищує процесуальну стійкість доказів і зміцнює довіру до українського правосуддя як на національному, так і на міжнародному рівні [2; 12; 18; 23].

Проведене дослідження дозволило сформувати комплексне бачення методики інтелектуального аналізу сенсорної інформації як інноваційного інструменту документування воєнних злочинів. На першому етапі було обґрунтовано актуальність проблеми: сенсорні й цифрові дані, що продукуються у воєнних умовах, набувають вирішального значення для доведення складів злочинів проти миру та безпеки людства. Саме тому потреба у формуванні єдиної методики їх інтеграції та процесуальної легітимації є невідкладною [2; 22–26; 34–39].

У концептуальних засадах методики визначено сутність сенсорної інформації, принципи її аналізу (інтегративність, синхронізація, алгоритмічна прозорість, контекстуальність, автентичність) та роль мультисенсорного середовища, яке поєднує фізичні, цифрові, агентурні й OSINT-джерела. Запропонована архітектура програмно-апаратного комплексу (сенсорне ядро, OSINT-ядро, інтегратор даних) забезпечує безперервний цикл від первинної фіксації сигналів до формування уніфікованих доказових пакетів [12].

Основні етапи методики – отримання, синхронізація, алгоритмічна обробка, класифікація, формування доказових пакетів, верифікація й стандартизація – створюють багаторівневу систему, що гарантує достовірність, відтворюваність та процесуальну придатність сенсорних даних [23]. У процесуальному вимірі методика відповідає критеріям допустимості цифрових доказів, інтегрує судовий контроль як гарантію пропорційності й законності та забезпечує баланс між ефективністю розслідування і захистом прав людини, що узгоджується з практикою ЄСПЛ [18].

У міжнародному контексті вона спирається на стандарти права ЄС, рішення CJEU та ЄСПЛ, а також на досвід міжнародних трибуналів, що підтвердили можливість використання цифрових і сенсорних доказів за умови автентичності, збереження ланцюга цифрових доказів та незалежної перевірки алгоритмів. Це створює передумови для гармонізації української практики з міжнародними стандартами та підвищує легітимність доказів у міжнародних юрисдикціях [2; 18; 23].

Практичне значення методики полягає у підвищенні ефективності роботи слідчих органів, розвантаженні підрозділів, формуванні уніфікованої бази цифрових доказів і створенні умов для впровадження сучасних алгоритмічних комплексів, нейромереж та математичного моделювання. Це забезпечує не лише належне документування вже вчинених злочинів, але й відкриває перспективи для прогнозування майбутніх загроз [12].

Узагальнюючи, розроблена методика поєднує технічний і процесуальний виміри, створюючи умови для ефективного й легітимного використання сенсорних даних як цифрових доказів. Вона зміцнює національну систему доказування воєнних злочинів і водночас

інтегрує її у міжнародний правовий простір, що має вирішальне значення для подальшого притягнення винних до відповідальності.

Висновки. Методика інтелектуального аналізу мультисенсорних даних для документування воєнних злочинів являє собою цілісну процесуально орієнтовану рамку, що поєднує інженерні рішення зі строгими вимогами кримінального процесу. Триєдина архітектура (сенсорне ядро – OSINT-ядро – інтегратор даних) забезпечує безперервний цикл опрацювання: отримання даних, часово-просторову синхронізацію, алгоритмічну обробку та класифікацію, формування доказових пакетів, їх верифікацію й стандартизацію.

Унікальність методики полягає в *процесуалізації технічних процедур*: результати сенсорного спостереження з моменту проєктування переводяться у юридично значимі цифрові докази через фіксацію повних метаданих; забезпечення автентичності та безперервності ланцюга збереження цифрових доказів; прозорість алгоритмів і можливість незалежної перевірки на всіх етапах; уніфіковані SOP для різних каналів даних; стандартизовані формати доказових пакетів і механізми валідації (у т.ч. precision/recall/F1, FPR/FNR). Методика відповідає критеріям допустимості доказів за КПК України (законність одержання, належність, достовірність, достатність і перевірюваність) та узгоджується з європейськими стандартами справедливого судового розгляду і поваги до приватного життя (ст. 6 і 8 Конвенції, практика ЄСПЛ) і підходами CJEU щодо законної мети, необхідності/пропорційності доступу до даних і наявності ефективних запобіжників від свавілля.

Запропоновані техніко-процесуальні рішення кореспондують національній судовій практиці ККС ВС (санкціонування доступу, атрибуція джерела, фіксація та збереження технічних характеристик, безперервність ланцюга збереження цифрових доказів, можливість незалежної перевірки) і узгоджуються з профільними міжнародними настановами ISO/NIST/ENFSI щодо ідентифікації, збирання, збереження та аутентифікації цифрових доказів.

Практичний ефект методики проявляється у *скороченні часу* на опрацювання великих масивів даних, *уніфікації доказових пакетів* і *формуванні централізованої бази цифрових доказів*, що підвищує стійкість матеріалів до процесуального оскарження, полегшує судову оцінку та сприяє міжвідомчій і транскордонній кооперації (EIO/e-evidence).

Впровадження SOP для різних каналів даних (відео/фото, акустика, телеком-логи, супутникові знімки/UAV, OSINT) у поєднанні з вимогами до хешування, підписування й журналювання дій створює стандартизовану «дорогу доказу» від моменту фіксації до судового розгляду.

Запропонований блок *метрик та валідації* (precision, recall, F1, FPR, FNR із довірчими інтервалами) і процедура *міжвідомчої верифікації* підсилюють відтворюваність результатів та їхню доказову надійність, уможливлюючи змагальну перевірку стороною захисту відповідно до вимог ст. 6 Конвенції.

Разом із тим окреслено ключові *умови практичної імплементації*: гармонізація внутрішніх процедур із актами ЄС щодо електронних доказів (у т. ч. щодо меж і механізмів доступу, обсягу даних і контролю суду); запровадження єдиних форматів доказових пакетів і реєстрів; політика управління доказовими даними (ролі/доступи, ретенція/мінімізація, аудит, реагування на інциденти); регулярні DPIA/PIA з огляду на вимоги ePrivacy/GDPR. Для органів досудового розслідування очікуваними є *раціоналізація ресурсів* і зниження частки ручних операцій, для судів – підвищення структурованості матеріалів і якості мотивування рішень, для міжнародної взаємодії – *сумісність* форматів і процедур з вимогами міжнародних юрисдикцій.

Подальші напрями роботи полягають у розгортанні *нейромережевих і математичних модулів* реконструкції подій (за неповними даними), розширенні відкаліброваних бенчмарків для типових задач (класифікація типів ураження за відео/акустикою, кореляція телеком-логів із сенсорними подіями), удосконаленні процедур аудиту алгоритмів і міжвідомчої верифікації, а також у доопрацюванні законодавчих і відомчих актів для повномасштабної інтеграції SOP і реєстрів цифрових доказів.

Методика створює цілісну рамку легітимного використання результатів мультисенсорного спостереження у доказуванні воєнних злочинів, забезпечує узгодженість національної практики з європейськими стандартами та підвищує шанси на ефективне притягнення винних до відповідальності на національному й міжнародному рівнях.

Список використаних джерел:

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: https://zakon.rada.gov.ua/go/254к/96-вр
2. Кримінальний процесуальний кодекс України: Закон України від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/go/4651-17
3. Кримінальний кодекс України: Закон України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/go/2341-14
4. Про правовий режим воєнного стану: Закон України від 12.05.2015 № 389-VIII. URL: https://zakon.rada.gov.ua/go/389-19
5. Про введення воєнного стану в Україні: Указ Президента України від 24.02.2022 № 64/2022. URL: https://zakon.rada.gov.ua/go/64/2022
6. Про затвердження Указу Президента «Про введення воєнного стану в Україні»: Закон України від 24.02.2022 № 2102-IX. URL: https://zakon.rada.gov.ua/go/2102-20
7. Rome Statute of the International Criminal Court, 17.07.1998. URL: https://zakon.rada.gov.ua/go/995_588
8. Convention (IV) respecting the Laws and Customs of War on Land (Hague), 18.10.1907. URL: https://zakon.rada.gov.ua/go/995_222
9. Geneva Convention (IV) relative to the Protection of Civilian Persons in Time of War, 12.08.1949. URL: https://zakon.rada.gov.ua/go/995_154
10. Additional Protocol I to the Geneva Conventions, 08.06.1977. URL: https://zakon.rada.gov.ua/go/995_199
11. Additional Protocol II to the Geneva Conventions, 08.06.1977. URL: https://zakon.rada.gov.ua/go/995_200
12. Directive 2014/41/EU regarding the European Investigation Order in criminal matters. OJ L 130, 01.05.2014, p. 1–36. URL: https://eur-lex.europa.eu/eli/dir/2014/41/oj/eng
13. Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence. OJ L 191, 28.07.2023, p. 118–180. URL: https://eur-lex.europa.eu/eli/reg/2023/1543/oj/eng
14. Directive (EU) 2023/1544 on designated establishments and legal representatives for gathering electronic evidence in criminal proceedings. OJ L 191, 28.07.2023, p. 181–190. URL: https://eur-lex.europa.eu/eli/dir/2023/1544/oj/eng
15. Directive 2002/58/EC (ePrivacy). OJ L 201, 31.07.2002, p. 37–47. URL: https://eur-lex.europa.eu/eli/dir/2002/58/oj/eng
16. Regulation (EU) 2016/679 (GDPR). OJ L 119, 04.05.2016, p. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng
17. Court of Justice of the EU, Case C-670/22, M.N. (EncroChat), Grand Chamber, 30.04.2024. URL: https://curia.europa.eu/juris/liste.jsf?num=C-670/22
18. CJEU, Case C-746/18, H.K. v Prokuratuur, Grand Chamber, 02.03.2021. URL: https://curia.europa.eu/juris/liste.jsf?num=C-746/18
19. CJEU, Joined Cases C-511/18, C-512/18, C-520/18, La Quadrature du Net and Others, Grand Chamber, 06.10.2020. URL: https://curia.europa.eu/juris/document/document.jsf?docid=232084&doclang=en
20. CJEU, Joined Cases C-793/19 & C-794/19, SpaceNet AG; Telekom Deutschland GmbH, Grand Chamber, 20.09.2022. URL: https://curia.europa.eu/juris/liste.jsf?num=C-793/19
21. CJEU, Case C-140/20, G.D. v Commissioner of the Garda Síochána, Grand Chamber, 05.04.2022. URL: https://curia.europa.eu/juris/liste.jsf?num=C-140/20
22. ECtHR [GC]. Roman Zakharov v. Russia, no. 47143/06, 04.12.2015. HUDOC: https://hudoc.echr.coe.int/eng?i=001-159324
23. ECtHR [GC]. Big Brother Watch and Others v. the United Kingdom, nos. 58170/13, 62322/14, 24960/15, 25.05.2021. HUDOC: https://hudoc.echr.coe.int/eng?i=001-210077

24. ECtHR [GC]. Centrum för Rättvisa v. Sweden, no. 35252/08, 25.05.2021. HUDOC: https://hudoc.echr.coe.int/eng?i=001-210078

25. ECtHR. Benedik v. Slovenia, no. 62357/14, 24.04.2018. HUDOC: https://hudoc.echr.coe.int/eng?i=001-182455

26. ECtHR. Teixeira de Castro v. Portugal, no. 25829/94, 09.06.1998. HUDOC: h ttps://hudoc.echr.coe.int/eng?i=001-58193

27. Верховний Суд (ККС). Постанова від 20.02.2018 у справі № 750/4139/15-к. ЄДРСР № 72460327. URL: https://reyestr.court.gov.ua/Review/72460327

28. Верховний Суд (ККС). Постанова від 30.09.2020 у справі № 563/1118/16-к. ЄДРСР № 91998609. URL: https://reyestr.court.gov.ua/Review/91998609

29. Верховний Суд (ККС). Постанова від 04.06.2025 у справі № 686/20198/22. ЄДРСР № 128309294. URL: https://reyestr.court.gov.ua/Review/128309294

30. Верховний Суд (ККС). Постанова від 04.09.2019 у справі № 369/3713/18. ЄДРСР № 84120855. URL: https://reyestr.court.gov.ua/Review/84120855

31. Deutschland. Strafprozessordnung, § 100b – Online-Durchsuchung. URL: https://dejure.org/gesetze/StPO/100b.html

32. Code de procédure pénale (France), art. 706-102-1 (De la captation des données informatiques). URL: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624

33. España. Ley Orgánica 13/2015, de 5 de octubre (modificación de la LECrim). BOE núm. 239, 06/10/2015. URL: https://www.boe.es/buscar/act.php?id=BOE-A-2015-10725

34. OHCHR. The Berkeley Protocol on Digital Open Source Investigations. URL: https://www.ohchr.org/sites/default/files/2024-01/OHCHR_BerkeleyProtocol.pdf

35. ISO/IEC 27037:2012. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. URL: https://www.iso.org/standard/44381.html

36. ДСТУ ISO/IEC 27037:2017 (IDT). Інформаційні технології. Методи захисту. Настанови щодо ідентифікації, збирання, одержання та збереження цифрових доказів. Набув чинності 01.01.2019. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=74978

37. NIST Special Publication 800-101 Rev. 1. Guidelines on Mobile Device Forensics. 2014. URL: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-101r1.pdf

38. NIST Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response. 2006. URL: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-86.pdf ; Card: https://csrc.nist.gov/pubs/sp/800/86/final

39. ENFSI. Best Practice Manual for Digital Image Authentication. ENFSI-BPM-DI-003-1, 2021. URL: https://enfsi.eu/wp-content/uploads/2021/10/BPM_Image-Authentication_ENFSI-BPM-DI-003-1.pdf

40. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Waltham, MA: Academic Press. 2011. 840 p.URL: https://www.oreilly.com/library/view/digital-evidence-and/9780123742681/

41. Casey, E. (ed.). Handbook of Digital Forensics and Investigation. Amsterdam–Boston: Academic Press, 2009. xxvi, 567 p. URL: https://archive.org/details/handbookofdigita0000case

42. Mason, S.; Seng, D. (eds.). Electronic Evidence. 4th ed. London: University of London Press/IALS, 2017. 422 p. URL: https://library.oapen.org/handle/20.500.12657/39391

43. Mason, S.; Seng, D. (eds.). Electronic Evidence and Electronic Signatures. 5th ed. London: University of London Press, 2021. 604 p. URL: https://library.oapen.org/bitstream/20.500.12657/55755/1/9781911507246.pdf

44. Franssen, V.; Tosza, S. (eds.). The Cambridge Handbook of Digital Evidence in Criminal Investigations. Cambridge: Cambridge University Press. 2025. 608 p. DOI: 10.1017/9781009049771. URL: https://doi.org/10.1017/9781009049771

45. Gillett, M.; Fan, W. Expert Evidence and Digital Open Source Information: Bringing Online Evidence to the Courtroom. Journal of International Criminal Justice. 2023. 21(4). P. 661–693. DOI: 10.1093/jicj/mqad050.URL: https://doi.org/10.1093/jicj/mqad050

46. Qureshi, S. M.; Saeed, A.; Almotiri, S. H.; Ahmad, F.; Al Ghamdi, M. A. Deepfake forensics: a survey of digital forensic methods for multimodal deepfake identification on social media. *PeerJ Computer Science*. 2024. **10**. e2037. DOI: 10.7717/peerj-cs.2037. URL: https://doi.org/10.7717/peerj-cs.2037

47. Rössler, A.; Cozzolino, D.; Verdoliva, L.; Riess, C.; Thies, J.; Nießner, M. FaceForensics++: Learning to Detect Manipulated Facial Images. In: *ICCV 2019*. URL: https://openaccess.thecvf.com/content_ICCV_2019/papers/Rossler_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images_ICCV_2019_paper.pdf

48. Cozzolino, D.; Verdoliva, L. Noiseprint: A CNN-Based Camera Model Fingerprint. *IEEE Transactions on Information Forensics and Security* 2020. 15. P. 144–159. DOI: 10.1109/TIFS.2019.2916364. URL: https://doi.org/10.1109/TIFS.2019.2916364

49. Бондар В. С.; Парфьонов В. Ю. Про особливості застосування новітніх технологій у документуванні та розслідуванні окремих видів воєнних злочинів. *Прикарпатський юридичний вісник*. 2024. № 6 (59). С. 118–123. DOI: 10.32782/pyuv.v6.2024.22. URL: http://pjv.nuoua.od.ua/v6_2024/24.pdf

50. Буняк В. Нацполіція використовуватиме новітні 3D-сканери для документування російських воєнних злочинів. *Детектор медіа (MediaSapiens)*, 25.11.2023. URL: https://ms.detector.media/withoutsection/post/33567/2023-11-25-natspolitsiya-vykorystovuvatyme-novitni-3d-skanery-dlya-dokumentuvannya-rosiyskykh-voiennykh-zlochyniv/

51. Засоби ураження російської агресії: Довідник / Є. О. Меленті та ін. Київ: НА СБУ, 2023. 142 с. URL: https://ssu.gov.ua/natsionalna-akademiia

52. Погорецький М. А. Функціональне призначення оперативно-розшукової діяльності у кримінальному процесі: монографія. Харків: Арсіс ЛТД, 2007. 576 с. URL: https://library.nlu.edu.ua/POLN_TEXT/UP/POGORECKIY_2007.pdf

53. Погорецький М. Теорія кримінального процесуального доказування: проблемні питання. *Право України*. 2014. № 10. С. 12–25. URL: https://pravoua.com.ua/uk/store/pravoukr/pravoukr_10_14/Pogoretskyi_10_14

54. Погорецький М. А. Нова концепція кримінального процесуального доказування. *Вісник кримінального судочинства*. 2015. № 3. С. 63–79. URL: https://vkslaw.knu.ua/images/verstka/3_2015_Pogoretskyi.pdf

55. Погорецький М. А., Лисаченко Є. І. Допустимість доказів у праві країн ЄС та його вплив на кримінальне судочинство України. *Вісник кримінального судочинства*. 2022. № 3–4. С. 20–34. DOI: 10.17721/2413-5372.2022.3-4/20-34. URL: https://vkslaw.knu.ua/images/verstka/Visnyk_Krim_Sud_3-4_22_231024_avt%20(2)-20-34.pdf

56. Погорецький М. А. Застосування новітніх технологій у розслідуванні та доказуванні воєнних злочинів (проблемні питання). *Вісник кримінального судочинства*. 2023. № 3–4. С. 84–102. DOI: 10.17721/2413-5372.2023.3-4/84-102. URL: https://vkslaw.com.ua/index.php/journal/article/view/485

57. Погорецький М. А. Судовий контроль у забезпеченні справедливого та допустимого доказування в кримінальному процесі України. *Аналітично-порівняльне правознавство*. 2025. № 4 (ч. 3). С. 269–279. DOI: 10.24144/2788-6018.2025.04.3.40. URL: https://app-journal.in.ua/wp-content/uploads/2025/08/42-2.pdf

58. Пчеліна О., Фоміна Т. Особливості проведення огляду місця події під час досудового розслідування злочинів, пов'язаних зі збройною агресією проти України. *Науковий вісник ДДУВС*. 2023. № 2. С. 254–258. URL: https://visnik.dduvs.edu.ua/index.php/visnyk/article/view/660

59. Чернявський С. С., Присяжний В. І., Стрільців О. М. та ін.; за заг. ред. М. С. Цуцкірідзе. Застосування космічних і геоінформаційних технологій під час виявлення та розслідування кримінальних правопорушень: методичні рекомендації. Київ: НАВС, 2023. 92 с. URL: https://elar.navs.edu.ua/items/02907f6a-e6b8-47b8-aa5d-9a747b24a7d3

60. Yevseiev, S.; Milevskyi, S.; Melenti, Y.; Voitko, O.; Aleksieiev, M.; Morklyanyk, B.; Povaliaiev, S.; Shvorak, R.; Sevriukova, Y.; Rykov, D. Development of a method for assessing the society national security level based on the triple helix concept. *Eastern-European Journal of Enterprise Technologies*. 2025. 4(4) (136): 32–45. DOI: https://doi.org/10.15587/1729-4061.2025.337398. URL: https://journals.uran.ua/eejet/article/view/337398

Дата першого надходження рукопису до видання: 16.07.2025
Дата прийнятого до друку рукопису після рецензування: 18.08.2025
Дата публікації: 26.09.2025