**ISSN 2786-7080 (Print)**
**ISSN 2786-7072 (Online)**

УДК 343.983:004
https://doi.org/10.33994/kndise.2026.71.13

**Білик Олександр Сергійович**

*судовий експерт Західноукраїнського відділення науково-дослідного центру судової експертизи в сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України*
*https://orcid.org/0009-0007-4846-1585*
*oleksandr.bilyk@nure.ua*

**Бібліографічний опис статті:** Білик О.С. (2026). Особливості дослідження цифрових носіїв та телеметричних даних в межах судової комп'ютерно-технічної експертизи. *Криміналістика і судова експертиза, 71,* 185-201. doi: https://doi.org/10.33994/kndise.2026.71.13

## ОСОБЛИВОСТІ ДОСЛІДЖЕННЯ ЦИФРОВИХ НОСІЇВ ТА ТЕЛЕМЕТРИЧНИХ ДАНИХ В МЕЖАХ СУДОВОЇ КОМП'ЮТЕРНО-ТЕХНІЧНОЇ ЕКСПЕРТИЗИ

Стаття присвячена комплексному аналізу науково-методичних засад дослідження сучасних цифрових носіїв інформації та специфічного виду цифрових слідів — телеметричних даних, у межах проведення судової комп'ютерно-технічної експертизи. У роботі обґрунтовано, що стрімка еволюція безпілотних авіаційних систем (БАС), пристроїв «інтернету речей» (IoT) та впровадження нових файлових систем потребує трансформації класичних підходів до вилучення та аналізу доказів. **Метою дослідження** є розробка та наукове обґрунтування методичних підходів до дослідження телеметрії як ключового джерела криміналістично значущої інформації. **Методологічну основу** роботи становлять методи системного аналізу, порівняльно-правовий метод, а також спеціальні методи цифрової криміналістики (forensic imaging, live analysis). Окрему увагу приділено технологіям програмно-визначаємих радіосистем (SDR) як інструменту верифікації цифрових доказів. У ході дослідження проаналізовано архітектурні особливості файлової системи APFS (Apple File System), зокрема механізми Copy-on-Write та Snapshots, які відкривають нові можливості для відновлення видалених телеметричних логів. Визначено класифікацію телеметрії на зовнішню, внутрішню та хмарну, що дозволяє експерту структурувати процес пошуку доказів. Висвітлено роль SDR-технологій у процесі ідентифікації пристроїв за радіочастотними сигнатурами та валідації

© Білик О.С. (2026)
Стаття поширюється на умовах ліцензії відкритого доступу CC BY 4.0

GPS-координат, що містяться в польотних листах БПЛА. **Наукова новизна** отриманих результатів полягає у поєднанні методів класичної комп'ютерно-технічної експертизи з радіотехнічним аналізом сигналів керування, що дозволяє не лише реконструювати події, а й виявляти ознаки інтелектуального втручання (GPS-spoofing, wiping). **Практичне значення** роботи полягає у формулюванні рекомендацій для судових експертів щодо роботи з пропрієтарними форматами даних (на прикладі протоколу MAVLink та логів DJI). Запропоновані підходи сприятимуть підвищенню об'єктивності та достовірності експертних висновків у справах, пов'язаних із використанням високотехнологічних пристроїв.

**Ключові слова:** судова комп'ютерно-технічна експертиза, цифрові докази, телеметрія, БПЛА, цифрові носії, IoT.

**Bilyk Oleksandr**

*Forensic Expert, West Ukrainian Department of the Scientific Research Center for Forensic Expertise in the Field of Information Technologies and Intellectual Property of the Ministry of Justice of Ukraine*
https://orcid.org/0009-0007-4846-1585
*oleksandr.bilyk@nure.ua*

## FEATURES OF THE INVESTIGATION OF DIGITAL MEDIA AND TELEMETRIC DATA WITHIN THE FRAMEWORK OF FORENSIC COMPUTER-TECHNICAL EXPERTISE

**To cite this article:** Bilyk, O.S. (2026). Osoblyvosti doslidzhennia tsyfrovykh nosiiv ta telemetrychnykh danykh u mezhakh sudovoi kompiuterno-tekhnichnoi ekspertyzy kompiuternoi kryminalistyky [Features of the Investigation of Digital Media and Telemetric Data within the Framework of Forensic Computer-Technical Expertise]. *Criminalistics and Forensics, 71,* 185-201. doi: https://doi.org/10.33994/kndise.2026.71.13

The article is devoted to a comprehensive analysis of the scientific and methodological foundations for the study of modern digital storage media and a specific type of digital footprints - telemetric data, within the framework of forensic computer-technical examination. The paper substantiates that the rapid evolution of unmanned aerial systems (UAS), Internet of Things (IoT) devices, and the implementation of new file systems requires a transformation of classical approaches to the extraction and analysis of evidence. **The aim of the study** is to develop and scientifically substantiate methodological approaches to the study of telemetry as a key source of forensically significant information. **The methodological basis** of the work consists of systems analysis methods, comparative legal methods, and special digital forensic meth-

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

ods (forensic imaging, live analysis). Particular attention is paid to Software-Defined Radio (SDR) technologies as a tool for the verification of digital evidence. In the course of the research, the architectural features of the APFS (Apple File System) were analyzed, in particular, the Copy-on-Write and Snapshots mechanisms, which open up new opportunities for recovering deleted telemetric logs. A classification of telemetry into external, internal, and cloud categories has been defined, allowing the expert to structure the process of searching for evidence. The role of SDR technologies in the process of identifying devices by radio frequency signatures and validating GPS coordinates contained in UAV flight logs is highlighted. **The scientific novelty** of the results obtained lies in the combination of classical computer-technical examination methods with radio-technical analysis of control signals, which allows not only the reconstruction of events but also the detection of signs of intellectual interference (GPS-spoofing, wiping). **The practical significance** of the work lies in the formulation of recommendations for forensic experts on working with proprietary data formats (on the example of the MAVLink protocol and DJI logs). The proposed approaches will help to increase the objectivity and reliability of expert opinions in cases involving the use of high-tech devices.

**Key words:** forensic computer and technical expertise, digital evidence, telemetry, UAV, digital media, IoT.

**Постановка проблеми**

В сучасних умовах стрімкого розвитку інформаційних технологій та широкого використання безпілотних літальних апаратів (БПЛА), мобільних пристроїв та “розумних” систем, значно зростає кількість злочинів, у яких цифрові носії та телеметричні дані виступають ключовими джерелами доказової інформації. Особливого значення це набуває в контексті воєнних дій, кіберзлочинності та використання технічних засобів для збору, передачі й обробки даних.

Разом із тим, існуючі методики судової комп’ютерно-технічної експертизи здебільшого орієнтовані на найбільш розповсюджені носії інформації (жорсткі диски, флеш-накопичувачі, SSD) і недостатньо враховують специфіку сучасних джерел даних, таких як телеметричні журнали, лог-файли вбудованих систем, дані сенсорів, а також мережеві протоколи обміну в реальному часі [1, 2].

Проблема ускладнюється відсутністю уніфікованих підходів до вилучення, збереження, декодування та інтерпретації телеметричних даних, які часто мають пропрієтарні формати, шифрування даних або частково втрачену структуру. Крім того, складність встановлення автентичності, цілісності та часової узгодженості таких даних створює додаткові виклики для експертів під час формування обґрунтованих висновків [3, 4].

Недостатня розробленість методичного забезпечення дослі-

дження телеметричних даних у поєднанні з цифровими носіями, а також відсутність чітких алгоритмів їх комплексного аналізу в межах судової комп'ютерно-технічної експертизи зумовлюють необхідність подальших наукових досліджень у цьому напрямку [5].

Актуальність дослідження зумовлена стрімким розвитком цифрових технологій, широким використанням безпілотних літальних апаратів, мобільних пристроїв та вбудованих систем, які генерують значні обсяги телеметричних даних. У сучасних умовах, зокрема в контексті воєнних дій та зростання рівня кіберзлочинності, такі дані дедалі частіше виступають джерелом доказової інформації у кримінальних провадженнях. Водночас відсутність уніфікованих підходів до їх дослідження, складність інтерпретації та необхідність забезпечення належного рівня достовірності зумовлюють потребу у вдосконаленні методичного забезпечення судової комп'ютерно-технічної експертизи.

Наукова новизна дослідження полягає у систематизації підходів до аналізу телеметричних даних як окремого виду цифрових доказів та обґрунтуванні необхідності їх комплексного дослідження разом із традиційними цифровими носіями. Практичне значення отриманих результатів полягає у можливості їх використання експертами під час проведення судових комп'ютерно-технічних експертиз, що сприятиме підвищенню об'єктивності, повноти та достовірності експертних висновків.

Таким чином, актуальною науково-практичною задачею є розробка та вдосконалення підходів до дослідження цифрових носіїв і телеметричних даних БПЛА з урахуванням їх особливостей, що забезпечить підвищення достовірності та доказової цінності результатів судової експертизи.

**Аналіз останніх досліджень і публікацій**

Питання дослідження цифрових носіїв у межах судової комп'ютерно-технічної експертизи можна знайти у наукових працях вітчизняних і зарубіжних дослідників. Зокрема, у роботах [6, 7] підкреслюється, що комп'ютерно-технічна експертиза є одним із ключових інструментів дослідження цифрових доказів у кримінальному провадженні. При цьому відзначається наявність низки проблем, зокрема недосконаліть класифікації видів експертиз, складність постановки завдань експерту та необхідність комплексного використання різних експертних методик.

Значна увага у наукових джерелах [5] приділяється загальним методологічним засадам проведення судової комп'ютерно-технічної експертизи, включаючи процедури вилучення, збереження та аналізу електронної інформації. У відповідних роботах [6, 7] узагальнено підходи до визначення об'єктів, предмета та завдань експертизи, а також окреслено типові помилки, що виникають під час її

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

проведення. Водночас дослідники [8, 9] наголошують, що розвиток інформаційних технологій постійно породжує нові об'єкти дослідження, які раніше не існували, що ускладнює формування універсальних методик.

Окремий напрям досліджень стосується "цифрової криміналістики" як ширшої галузі, що охоплює аналіз даних з різноманітних цифрових пристроїв. Встановлено, що ця сфера сформувалася відносно нещодавно та досі перебуває у стадії активного розвитку, що супроводжується поступовим формуванням стандартів і підходів до дослідження цифрових доказів [5, 6, 7].

У сучасних дослідженнях [7, 8, 9, 10, 11, 12] також приділяється увага специфіці аналізу даних із мобільних та телекомунікаційних пристроїв як важливих джерел доказової інформації. Відзначають складність їх дослідження через різноманітність форматів даних, швидку зміну технологій та необхідність використання спеціалізованих методик.

Перспективним напрямом є інтеграція новітніх технологій, зокрема штучного інтелекту та машинного навчання [9, 12, 13], у судово-експертну діяльність, що дозволяє підвищити ефективність обробки великих масивів цифрових даних та об'єктивність експертних висновків. Крім того, у сучасних умовах особливого значення набувають дослідження, пов'язані із забезпеченням достовірності цифрових доказів та протидією методам їх фальсифікації (counter forensics).

Водночас аналіз наукових джерел [14, 15, 16] свідчить, що питання дослідження телеметричних даних, зокрема з безпілотних систем, IoT-пристроїв та вбудованих платформ, залишаються недостатньо розробленими. Наявні підходи здебільшого орієнтовані на традиційні цифрові носії та не враховують специфіку телеметрії як динамічних, багатовимірних і часто розподілених у часі та просторі даних. Це зумовлює необхідність подальшого розвитку науково-методичного забезпечення у даній сфері.

**Мета дослідження**

Метою дослідження є розробка та наукове обґрунтування методичних підходів до дослідження телеметрії як ключового джерела криміналістично значущої інформації.

Методи дослідження. Для досягнення поставленої мети у роботі використано комплекс загальнонаукових і спеціальних методів дослідження, що забезпечують системний підхід до аналізу цифрових носіїв та телеметричних даних у межах судової комп'ютерно-технічної експертизи.

Серед загальнонаукових методів застосовано:

- аналіз і синтез - для узагальнення сучасних підходів до дослідження цифрових доказів, а також формування цілісного уявлення

про особливості телеметричних даних як об'єкта експертного дослідження;

- індукцію та дедукцію – для встановлення загальних закономірностей формування, обробки та збереження телеметричної інформації на основі окремих прикладів та навпаки;
- порівняльний аналіз – для зіставлення існуючих методик дослідження традиційних цифрових носіїв і телеметричних даних;
- системний підхід – для розгляду цифрових носіїв і телеметрії як взаємопов'язаних елементів єдиної інформаційної системи.

До спеціальних методів, що використовуються у сфері судової комп'ютерно–технічної експертизи, належать:

- методи цифрової криміналістики (digital forensics) – для вилучення, фіксації, збереження та дослідження інформації з цифрових носіїв із забезпеченням її цілісності (використання контрольних хеш–сум, створення форензічних копій);
- методи аналізу файлових систем і структур даних – для дослідження логічної та фізичної організації даних на носіях інформації;
- методи аналізу журналів подій (логів) – для встановлення хронології подій, пов'язаних із функціонуванням пристроїв і систем;
- методи декодування та інтерпретації телеметричних даних – для обробки інформації, отриманої з вбудованих систем, сенсорів та БПЛА, з урахуванням специфіки форматів (у тому числі пропрієтарних);
- методи часової кореляції даних – для узгодження інформації з різних джерел (лог–файлів, телеметрії, мережевих даних) з метою відновлення послідовності подій;
- методи верифікації та забезпечення достовірності даних – для перевірки їх автентичності, цілісності та відсутності несанкціонованих змін.

Окрім цього, у роботі використано інструментальні методи, що передбачають застосування спеціалізованого програмного забезпечення для цифрової криміналістики, аналізу мережевого трафіку, обробки телеметричних даних, а також середовищ моделювання для відтворення умов функціонування досліджуваних систем [3, 4].

Застосування зазначених методів у комплексі дозволяє забезпечити повноту, об'єктивність і відтворюваність результатів дослідження, а також підвищити достовірність висновків судової комп'ютерно–технічної експертизи при роботі з цифровими носіями та телеметричними даними.

**ISSN 2786-7080 (Print)**
**ISSN 2786-7072 (Online)**

**Виклад основного матеріалу**

Сучасна судова комп'ютерно–технічна експертиза (СКТЕ) виходить за межі аналізу жорстких дисків (HDD/SSD) [1, 2]. Експерт працює з мікросхемами пам'яті, що інтегровані в плати (eMMC, UFS), та специфічними картами флеш пам'яті, де дані можуть бути пошкоджені внаслідок фізичного впливу (падіння БПЛА). Ключовою особливістю є робота з накопичувачами, що мають вбудоване шифрування (T2 chip, FileVault). Також важливою є диференціація між методами:

- "Dead Forensic": побітове копіювання носія (класичний підхід).
- "Live Forensic": аналіз даних в оперативній пам'яті та хмарних сервісах, що особливо актуально для IoT, де фізичний носій може містити лише зашифрований завантажувач.

На відміну від класичних комп'ютерних систем, БПЛА мають специфічні особливості, що впливають на процес вилучення даних: обмежений фізичний доступ до носіїв (вбудовані компоненти, складний демонтаж), ризик втрати волатильних даних (оперативна пам'ять, кеш телеметрії), пошкодження внаслідок аварій або бойових дій та залежність від стану живлення пристрою.

У зв'язку з цим вилучення може здійснюватися за кількома сценаріями:

- прямий доступ до знімних носіїв (SD–карти);
- логічне копіювання через інтерфейси (USB, UART, JTAG);
- вилучення даних із супутніх пристроїв (пульт керування, мобільні застосунки).

Телеметрія – це динамічні дані, що відображають життєвий цикл пристрою. У контексті судової експертизи вони поділяються на:

1. Зовнішня телеметрія: лог–файли мобільних застосунків керування на смартфонах операторів.
2. Внутрішня телеметрія: дані на польотному контролері (BlackBox).
3. Хмарна телеметрія: синхронізовані записи про маршрути на серверах виробника (напр. DJI Cloud).

Телеметричні дані мають низку специфічних властивостей, що ускладнюють їх вилучення та збереження: волатильність частини даних (тимчасові журнали, буфери), розподіленість джерел (БПЛА, наземна станція, сервери), висока частота оновлення, використання пропрієтарних форматів і протоколів.

У зв'язку з цим доцільним є: одночасне вилучення даних із декількох джерел, фіксація часових міток під час вилучення, збереження сирих (raw) даних поряд з обробленими. На рис.1 наведено узагальнений алгоритм дослідження телеметричних даних БПЛА.

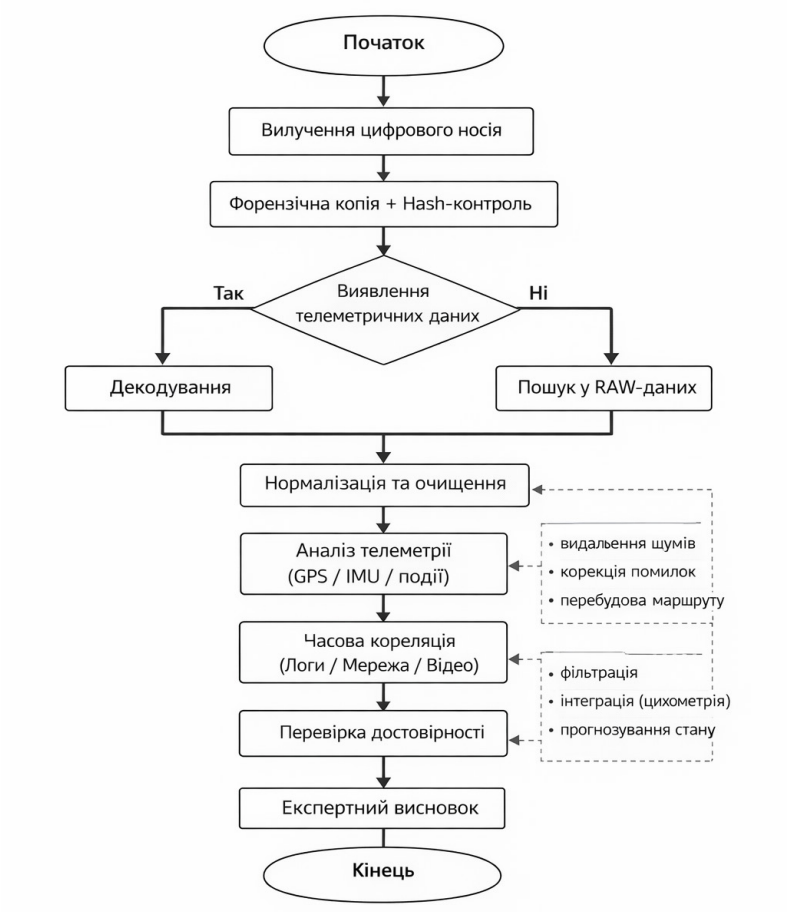


Рис. 1. Узагальнений алгоритм дослідження телеметричних даних БПЛА

В процесі дослідження телеметрія вирішує задачу “прив’язки” віртуальної події до фізичного простору, дозволяючи встановити точний час, місце (координати GPS/ГЛОНАСС) та параметри середовища. БПЛА є унікальним об’єктом, оскільки він постійно взаємодіє з радіоефіром. Це відкриває новий напрямок у СКТЕ – використання програмно-визначаємих радіосистем (SDR) для аналізу цифрових слідів.

Застосування SDR (наприклад, HackRF One, RTL-SDR) в межах експертизи дозволяє:

- перехоплення та аналіз сигналів керування: встановлення частотного діапазону та протоколу обміну (FHSS, ELRS), що допома-

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

гає ідентифікувати тип пульта керування;

◆ аналіз радіочастотних сигнатур: ідентифікація пристрою за унікальними характеристиками його передавача (Radio Frequency Fingerprinting), що може слугувати доказом ідентичності конкретного апарату;

◆ валідація телеметрії: зіставлення записаних координат у логах з реальними радіозавадами чи сигналами навігаційних супутників у певному районі.

Аналіз внутрішніх файлів (наприклад, .DAT у DJI) потребує використання спеціалізованого ПЗ (CVSView, DatCon) для дешифрування пропрієтарних форматів та візуалізації польотних треків, що є критичним для реконструкції обставин авіаційних подій або правопорушень.

Основною проблемою є навмисне спотворення даних:

◆ GPS Spoofing: підробка координат у логах за допомогою зовнішніх SDR-передавачів.

◆ Wiping: автоматичне видалення журналів після завершення сесії.

◆ Encryption: використання алгоритмів AES-256 для закриття доступу до пам'яті польотного контролера. Експерт повинен вміти розрізняти апаратні збої та навмисні втручання в структуру цифрового доказу.

**Визначення структури та декодування даних**

Процес декодування включає:

1. Ідентифікацію формату
◆ аналіз сигнатур файлів;
◆ використання інструментів (наприклад, binwalk);
◆ визначення версії прошивки/ПЗ.
2. Розбір структури
◆ заголовки (headers);
◆ блоки даних (frames);
◆ типи повідомлень (message types).
3. Декодування
◆ перетворення бінарних значень у фізичні величини;
◆ застосування масштабуючих коефіцієнтів;
◆ відновлення часових міток.

Приклад структури бінарного лог-файлу (.BIN). Типовий запис може містити:

◆ GPS ( Lat, Lon, Alt; Speed, FixType);
◆ IMU (AccX, AccY, AccZ; GyroX, GyroY, GyroZ);
◆ стан системи: Mode (Loiter, Auto, RTL), Battery, SignalStrength.

Кожен запис прив'язаний до часової мітки, що дозволяє відновити повну динаміку польоту. Перед аналізом виконується підготовка даних:

◆ нормалізація часу (приведення до UTC, компенсація затримок);

- очищення даних (видалення шумів, фільтрація аномальних значень);
- заповнення пропусків (лінійна інтерполяція, сплайн-інтерполяція);
- синхронізація сенсорів (узгодження частоти дискретизації).

GPS-дані є ключовим компонентом телеметрії, що забезпечує просторову прив'язку подій.

Основні параметри:

- географічні координати (широта, довгота);
- висота;
- швидкість;
- точність позиціонування (HDOP, кількість супутників).

Аналіз включає:

- побудова траєкторії польоту;
- обчислення швидкості:

$$V = \frac{\Delta S}{\Delta t}$$

- визначення зон перебування;
- виявлення аномалій (стрибки координат, втрата сигналу).

Інерціальні вимірювальні модулі (IMU) забезпечують інформацію про рух і орієнтацію БПЛА. Основні параметри:

- прискорення (AccX, AccY, AccZ);
- кутові швидкості (GyroX, GyroY, GyroZ);
- орієнтація (roll, pitch, yaw).

Методи аналізу:

- визначення прискорення:

$$a = \frac{\Delta v}{\Delta t}$$

- визначення орієнтації (roll, pitch, yaw);
- виявлення різких маневрів або ударів;
- інтеграція даних (dead reckoning).

Аналіз подій:

- визначення режимів польоту;
- виявлення аварійних ситуацій;
- аналіз системних повідомлень.

В ході дослідження встановлено ефективність використання таких інструментів:

- Mission Planner / QGroundControl - аналіз .BIN, .ULog;
- DJI Assistant / DatCon / CsvView - декодування .DAT;
- Wireshark - аналіз MAVLink-трафіку;
- Python (pandas, NumPy, Matplotlib) - обробка та візуалізація;
- binwalk, hexdump - низькорівневий аналіз.

Основні складнощі, які виникають під час дослідження:

- відсутність документації для пропрієтарних форматів;
- залежність від версії прошивки;

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

- пошкодження або неповнота файлів;
- шифрування або обфускація даних.

Таким чином, декодування телеметричних даних БПЛА є складним багаторівневим процесом, що включає ідентифікацію форматів, перетворення даних та їх подальший аналіз. Використання спеціалізованих інструментів і методів цифрової обробки дозволяє відновити параметри польоту та встановити обставини функціонування БПЛА, що має важливе значення для судової експертизи.

З метою апробації запропонованого підходу було проведено дослідження телеметричних даних безпілотного літального апарата, отриманих із цифрових носіїв після інциденту втрати зв'язку з оператором.

В ході роботи досліджувались:

- SD-карта з БПЛА (файли формату .BIN);
- мобільний пристрій оператора (кешовані дані, файл .DAT);
- відеозапис польоту;
- журнал подій наземної станції.

Основні досліджувані файли - flight_log_01.BIN (ArduPilot) та DJIFlightRecord_2024-05-12.DAT.

**Етап вилучення та підготовки об'єктів дослідження:**

- створено копії носіїв;
- обчислено хеш-значення (SHA-256);
- підтверджено цілісність даних;
- виконано первинний аналіз структури файлів.

**Декодування телеметричних даних**

Для декодування даних .BIN (ArduPilot) було використано програмне забезпечення Mission Planner та (бібліотеки для парсингу логів написані на мові програмування Python).

В результаті декодування отримано: GPS-дані (Lat, Lon, Alt), IMU (Acc, Gyro) дані режиму польоту та події системи.

Для декодування даних .DAT (DJI) було використано ПЗ DatCon та CsvView. В результаті декодування отримано детальні часові ряди телеметрії, стан сигналу, дані про батарею та журнали помилок.

**Аналіз GPS-даних**

В результаті дослідження GPS даних встановлено:

- маршрут польоту довжиною ~3.2 км;
- максимальна висота: 145 м;
- швидкість: до 18 м/с.

Також виявлено аномалію: різкий стрибок координат на ~250 м протягом 1 секунди та подальше відновлення траєкторії. Можливими причинами можуть бути GPS spoofing або втрата супутникового сигналу.

**Аналіз IMU**

В ході дослідження даних інерціального обладнання зафіксовано:

- різке прискорення по осі Z (~3.5g);

- нестабільність по осі yaw перед інцидентом;
- короткочасна втрата стабілізації.

Це може свідчити про можливий вплив зовнішнього фактора (вітер/перешкода) або наслідок втрати коректних GPS-даних.

В результаті аналізу подій в логах виявлено послідовність:

T+00:12:15 — Mode: AUTO

T+00:14:02 — Warning: GPS signal degraded

T+00:14:05 — Event: Signal Lost

T+00:14:07 — Mode: RTL (Return-to-Launch)

T+00:14:12 — Critical: Navigation error

Встановлено, що всі джерела узгоджено підтверджують момент втрати сигналу, а часове відхилення не перевищує 1–2 секунди.

**Виявлення аномалій**

Ідентифіковано:

- GPS-аномалія (стрибок координат);
- деградація сигналу перед інцидентом;
- помилки навігації після переходу у RTL;
- відсутність ознак ручного втручання оператора.

**Оцінка достовірності отриманих даних.**

В результаті дослідження перевірено цілісність логів (hash OK), узгодженість між .BIN і .DAT, відповідність фізичним законам руху. Ознак модифікації даних, підміни логів не виявлено. Також в результаті дослідження встановлено:

1. Політ БПЛА відбувався у штатному режимі до моменту втрати GPS-сигналу.
2. Зафіксовано деградацію навігаційного сигналу, що призвела до помилки визначення координат.
3. Перехід у режим RTL відбувся автоматично відповідно до алгоритмів керування.
4. Подальші помилки навігації спричинили втрату стабільного керування.
5. Ознак зовнішнього несанкціонованого втручання або модифікації даних не встановлено.

Цілісність цифрових даних забезпечується шляхом використання криптографічних хеш-функцій:

- MD5;
- SHA-1;
- SHA-256 (рекомендовано).

Процедура включає: обчислення хеш-значення оригінального носія, створення форензічної копії, обчислення хеш-значення копії та порівняння отриманих значень. Співпадіння хеш-сум підтверджує відсутність змін у даних.

ISSN 2786-7080 (Print)
ISSN 2786-7072 (Online)

**Висновки**

В результаті проведеного дослідження особливостей дослідження цифрових носіїв та телеметричних даних у межах судової комп'ютерно-технічної експертизи отримано такі основні результати.

1. Встановлено, що сучасні безпілотні літальні апарати формують розподілену систему зберігання цифрової інформації, яка включає вбудовані, знімні, наземні та хмарні носії. Це зумовлює необхідність комплексного підходу до їх дослідження.
2. Обґрунтовано, що телеметричні дані доцільно розглядати як окремий тип цифрових доказів, який відрізняється від традиційних файлів своєю структурою, багатовимірністю та залежністю від фізичних процесів функціонування технічних систем.
3. Визначено ключові особливості вилучення та забезпечення цілісності даних у системах БПЛА, зокрема необхідність створення копій, використання криптографічних хеш-функцій та дотримання принципів незмінності та відтворюваності результатів.
4. Проаналізовано методи декодування телеметричних даних різних форматів (.BIN, .DAT, ULog), а також встановлено необхідність застосування спеціалізованих інструментів і методів обробки для перетворення даних у придатний для аналізу вигляд.
5. Розроблено підхід до комплексного аналізу телеметрії, що включає дослідження GPS, IMU та подій системи, а також їх інтеграцію для відновлення динаміки функціонування БПЛА.
6. Доведено ефективність використання методів часової кореляції та крос-перевірки даних із різних джерел, що дозволяє підвищити достовірність висновків та виявити приховані аномалії.
7. Виявлено основні проблеми достовірності та автентичності телеметричних даних, зокрема можливість їх спотворення, втрати або навмисної модифікації, що потребує застосування додаткових методів верифікації.
8. Запропоновано узагальнений алгоритм дослідження телеметричних даних БПЛА, який забезпечує систематизацію процесу експертизи та може бути використаний у практичній діяльності судових експертів.

Практичне значення отриманих результатів полягає у можливості їх використання під час проведення судових комп'ютерно-технічних експертиз, зокрема при розслідуванні інцидентів, пов'язаних із використанням безпілотних систем.

**Список використаних джерел:**

1. Про судову експертизу: Закон України від 25.02.1994 № 4038-XII. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (дата звернення: 20.03.2026).
2. Інструкція про призначення та проведення судових експертиз та експертних досліджень : наказ Міністерства юстиції України

від 08.10.1998 № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98 (дата звернення: 20.03.2026).

3. Білик О. С., Мартинчук О. О. Дослідження БПЛА в судовій комп'ютерно-технічній експертизі. Проблеми теорії та практики судової експертизи з питань інтелектуальної власності («Крайнєвські читання»): матеріали VIII Міжнар. наук.-практ. конф., Київ, 2024.

4. Сулейманов Е. А., Сулейманов С. А., Мартинчук О. О., Білик О. С. Дослідження методів локалізації джерела випромінювання з використанням стаціонарних багатопозиційних систем та технологій програмно-визначаємих приймачів. ІКТК-2023: матеріали IX Міжнар. наук.-техн. конф. (Харків, 7 груд. 2023 р.). Харків : ХНУРЕ, 2023. С. 57–60.

5. Карпінська Н., Крикунов О. Окремі питання проведення судової комп'ютерно-технічної експертизи у кримінальному судочинстві. *Історико-правовий часопис*. 2017. № 1. С. 140–144. URL: https://chasopys.hl.vnu.volyn.ua/index.php/chasopys/article/view/351 (дата звернення: 20.03.2026).

6. Черемнова А., Бєлік Л. Цифрова інформація як об'єкт експертного дослідження в умовах діджиталізації: проблеми та перспективи розвитку. *Криміналістика і судова експертиза*. 2023. Вип. 68. С. 57–64. DOI: https://doi.org/10.33994/kndise.2023.68.06

7. Білик О. С., Мартинчук О. О. Огляд методів виявлення БПЛА з використанням ортогонально-поляризованих шумоподібних радіосигналів та технології SDR. ІКТК-2023 : матеріали IX Міжнар. наук.-техн. конф. Харків: ХНУРЕ, 2023. С. 52–56.

8. Білик О. С., Мартинчук О. О. Створення моделі штучного інтелекту для виявлення БПЛА. Радіоелектроніка та молодь у XXI столітті: матеріали 28-го Міжнар. форуму. Харків : ХНУРЕ, 2024. Т. 4. С. 5–7.

9. Білик О. С., Мартинчук О. О. Дослідження спектральних характеристик сигналів безпілотних літальних апаратів на ортогональних складових. Актуальні питання судової експертизи і криміналістики : матеріали міжнар. наук.-практ. конф. Харків : ННЦ «ІСЕ ім. М. С. Бокаріуса», 2025. С. 60.

10. Kuchuk, H., Mozhaiev, O., Tiulieniev, S., Mozhaiev, M., Kuchuk, N., Khorobrykh, P., Gnusov, Y., Horelov, Y., Svitlychnyi, V., & Bilyk, O. (2025). Devising a method for managing computing resources in a fog layer of the mobile high-density internet of things. Eastern-European Journal of Enterprise Technologies, 6(4 (138), 15–25. DOI: https://doi.org/10.15587/1729-4061.2025.344553

11. Білик О., Мартинчук О. Розробка програмного забезпечення для обробки сигналів БПЛА та їх подальше використання у машинному навчанні. Collection of Scientific Papers «ΛΟΓΟΣ», (April 26, 2024; Bologna, Italy), с. 231–235. DOI: https://doi.org/10.36074/logos-26.04.2024.047

12. Бабенко В., Лученко С., Білик О., Дроздик Є. Візуальна система налаштування алгоритмів машинного навчання та даних. *Вимірювальна та обчислювальна техніка в технологічних процесах*. 2025.

№ 3. С. 194–203. DOI: https://doi.org/10.31891/2219-9365-2025-83-26

13. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Amsterdam : Academic Press, 2011. 840 p. DOI: https://doi.org/10.1016/C2009-0-20033-X

14. D. A. Hamdi, F. Iqbal, S. Alam, A. Kazim and Á. MacDermott, "Drone Forensics: A Case Study on DJI Phantom 4," 2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA), Abu Dhabi, United Arab Emirates, 2019, pp. 1-6, DOI: 10.1109/AICCSA47632.2019.9035302

15. Yousef Maryam, Iqbal Farkhund, Hussain Mohammed. Drone Forensics: A Detailed Analysis of Emerging DJI Models. 2020. 066-071. DOI: 10.1109/ICICS49469.2020.239530

16. Horsman G. Unmanned aerial vehicles: A survey of forensic challenges and opportunities. *Digital Investigation*. 2016. Vol. 18. P. 56–73. DOI: https://doi.org/10.1016/j.diin.2015.11.002

17. Rekhis S., Boudriga N. Formal forensic analysis of digital evidence in smart cities. IEEE *Communications Magazine*. 2020. Vol. 58, No. 3. P. 60–66. DOI: https://doi.org/10.1109/MCOM.001.1900534

18. ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence. Geneva: ISO, 2012.

19. ISO/IEC 27041:2015. Guidance on assuring suitability and adequacy of incident investigative methods. Geneva: ISO, 2015.

20. ISO/IEC 27042:2015. Guidelines for the analysis and interpretation of digital evidence. Geneva: ISO, 2015.

21. NIST SP 800-86. Guide to Integrating Forensic Techniques into Incident Response. Gaithersburg: NIST, 2006.

22. NIST SP 800-101 Rev.1. Guidelines on Mobile Device Forensics. Gaithersburg: NIST, 2014.

23. MAVLink Development Team. MAVLink Micro Air Vehicle Communication Protocol. URL: https://mavlink.io (дата звернення: 20.03.2026).

24. ArduPilot Dev Team. ArduPilot Documentation (DataFlash Logs). URL: https://ardupilot.org (дата звернення: 20.03.2026).

25. PX4 Development Team. PX4 User Guide (ULog File Format). URL: https://docs.px4.io (дата звернення: 20.03.2026).

26. DJI. DJI Flight Log Data Analysis Documentation. URL: https://www.dji.com (дата звернення: 20.03.2026).

**References:**

1. Pro sudovu ekspertyzu: Zakon Ukrainy vid 25.02.1994 № 4038-XII [On forensic examination: Law of Ukraine]. (1994). Retrieved April 20, 2026, from https://zakon.rada.gov.ua/laws/show/4038-12 (in Ukrainian)

2. Instruktsiia pro pryznachennia ta provedennia sudovykh ekspertyz ta ekspertnykh doslidzhen: Nakaz Ministerstva yustytsii Ukrainy vid 08.10.1998 № 53/5 [Instruction on the appointment and

conduct of forensic examinations]. (1998). Retrieved April 20, 2026 (in Ukrainian)

3. Bilyk, O. S., & Martynchuk, O. O. (2024). Doslidzhennia BPLA v sudovii kompiuterno-tekhnichnii ekspertyzi [UAV research in forensic computer examination]. In Proceedings of the VIII International Scientific Conference. Kyiv. (in Ukrainian)

4. Suleimanov, E. A., Suleimanov, S. A., Martynchuk, O. O., & Bilyk, O. S. (2023). Doslidzhennia metodiv lokalizatsii dzherela vyprominiuvannia... [Methods of RF source localization using SDR]. In ICTC-2023 Proceedings (pp. 57–60). (in Ukrainian)

5. Karpinska, N., & Krykunov, O. (2017). Certain Issues of Carrying Out Judicial Computer-Technical Expertise in Criminal Proceeding. History and Law Journal, 9(1), 140–144. Retrieved from https://chasopys.hl.vnu.volyn.ua/index.php/chasopys/article/view/351. (in Ukrainian)

6. Cheremnova, A., & Bielik, L. (2023). Digital information as an object of expert examination in the context of digitalization: problems and prospects of development. Criminalistics and Forensic Expertise, (68), 57–64. https://doi.org/10.33994/kndise.2023.68.06

7. Bilyk, O. S., & Martynchuk, O. O. (2023). Ohliad metodiv vyiavlennia BPLA... [Review of UAV detection methods using SDR]. In ICTC-2023 Proceedings (pp. 52–56). (in Ukrainian)

8. Bilyk, O. S., & Martynchuk, O. O. (2024). Stvorennia modeli shtuchnoho intelektu dlia vyiavlennia BPLA [AI model for UAV detection]. In Radioelectronics and Youth Forum (Vol. 4, pp. 5–7). (in Ukrainian)

9. Bilyk, O. S., & Martynchuk, O. O. (2025). Doslidzhennia spektralnykh kharakterystyk syhnaliv BPLA [Spectral characteristics of UAV signals]. In Forensic Science Conference Proceedings. (in Ukrainian)

10. Kuchuk, H., Mozhaiev, O., Tiulieniev, S., Mozhaiev, M., Kuchuk, N., Khorobrykh, P., Gnusov, Y., Horelov, Y., Svitlychnyi, V., & Bilyk, O. (2025). Devising a method for managing computing resources in a fog layer of the mobile high-density internet of things. Eastern-European Journal of Enterprise Technologies, 6(4 (138), 15–25. https://doi.org/10.15587/1729-4061.2025.344553

11. Bilyk, O. S., & Martynchuk, O.O. (2024). Development of software for UAV signal processing and their further use in machine learning. Collection of Scientific Papers «ΛΟΓΟΣ», (April 26, 2024; Bologna, Italy), 231–235. https://doi.org/10.36074/logos-26.04.2024.047

12. Babenko B., Luchenko C., Bilyk O., & Drozdyk E. (2025). Visual System For Setting Up Machine Learning Algorithms And Data. Measuring And Computing Devices In Technological Processes, (3), 194–203. https://doi.org/10.31891/2219-9365-2025-83-26

13. Casey, E. (2011). Digital evidence and computer crime (3rd ed.). Academic Press. https://doi.org/10.1016/C2009-0-20033-X

14. Hamdi, Dua'a & Iqbal, Farkhund & Alam, Saiqa & Kazim, Abdulla & MacDermott, Áine. (2019). Drone Forensics: A Case Study on DJI Phantom 4. 1-6. 10.1109/AICCSA47632.2019.9035302.

**ISSN 2786-7080 (Print)**
**ISSN 2786-7072 (Online)**

15. Yousef, Maryam & Iqbal, Farkhund & Hussain, Mohammed. (2020). Drone Forensics: A Detailed Analysis of Emerging DJI Models. 066-071. 10.1109/ICICS49469.2020.239530.

16. Horsman, Graeme. (2016). Unmanned aerial vehicles: A preliminary analysis of forensic challenges. Digital Investigation. 16. 1-11. DOI: 10.1016/j.diin.2015.11.002

17. Rekhis, S., & Boudriga, N. (2020). Formal forensic analysis of digital evidence in smart cities. IEEE Communications Magazine, 58(3), 60–66. https://doi.org/10.1109/MCOM.001.1900534

18. ISO. (2012). ISO/IEC 27037: Guidelines for identification, collection, acquisition and preservation of digital evidence.

19. ISO. (2015). ISO/IEC 27041: Guidance on assuring suitability and adequacy of incident investigative methods.

20. ISO. (2015). ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence.

21. NIST. (2006). Guide to integrating forensic techniques into incident response (SP 800-86).

22. NIST. (2014). Guidelines on mobile device forensics (SP 800-101 Rev.1).

23. MAVLink Development Team. (2026). MAVLink micro air vehicle communication protocol. Retrieved March 20, 2026, from https://mavlink.io

24. ArduPilot Dev Team. (2026). ArduPilot documentation: DataFlash logs. Retrieved April 20, 2026, from https://ardupilot.org

25. PX4 Development Team. (2026). PX4 user guide: ULog file format. Retrieved March 20, 2026, from https://docs.px4.io

26. DJI. (2026). DJI flight log data analysis documentation. Retrieved March 20, 2026, from https://www.dji.com

*Надійшла до редакції / Received: 27.04.2026*
*Отримана після доопрацювання / Received after revision: 29.04.2026*
*Прийнято до друку / Accepted for publication: 29.04.2026*
*Опубліковано / Published: 29.05.2026*

Фінансування: відсутнє / Funding: none.
Конфлікт інтересів: автор(и) заявляє(ють) про відсутність конфлікту інтересів / Conflict of interest: the author(s) declare no conflict of interest.
Дотримання етичних норм: дослідження виконано з дотриманням принципів академічної доброчесності / Ethical compliance: the study was conducted in accordance with the principles of academic integrity.
Дані дослідження: усі дані, необхідні для обґрунтування висновків, наведено у статті / Research data: all data necessary to substantiate the conclusions are presented in the article.