УДК 004.9

Кондратюк Д.
Хмельницький національний університет, Україна

СИСТЕМА ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ОБРАЗІВ НОСІЇВ ЦИФРОВИХ ДОКАЗІВ

Анотація. *У роботі обґрунтовано роль цифрових доказів у забезпеченні інформаційної безпеки та розроблено функціональну архітектуру програмного комплексу для їх інтелектуального аналізу. Дослідження фокусується на проєктуванні багаторівневої системи, що забезпечує повний цикл обробки даних – від імпорту та валідації цифрових образів до виділення ознак і формування звітних матеріалів. Архітектура системи побудована за модульним принципом, що дозволяє відокремити відповідальність компонентів і забезпечити гнучку інтеграцію нових аналітичних алгоритмів. Особливу увагу приділено механізмам стійкості до відмов і контролю цілісності даних. Запропоноване рішення автоматизує процес розслідування кіберінцидентів, гарантуючи достовірність результатів, що є критичним для правової оцінки цифрових доказів.*

Ключові слова: *цифрові докази, інформаційна безпека, кіберзлочинність, багаторівнева архітектура програмного комплексу, функціональні вимоги, нефункціональні вимоги.*

Kondratiuk D.
Khmelnytskyi National University, Ukraine

SYSTEM OF INTELLIGENT DIGTAL FORENSICS ANALYSIS

Absdtract. *The paper substantiates the role of digital evidence in ensuring information security and develops a functional architecture of a software complex for their intelligent analysis. The research focuses on the design of a multi-level system that provides a full data processing cycle – from importing and validating digital images to extracting features and generating reporting materials. The system architecture is built on a modular principle, which allows for the separation of responsibilities of components and flexible integration of new analytical algorithms. Particular attention is paid to mechanisms for fault tolerance and data integrity control. The proposed solution automates the process of investigating cyber incidents, guaranteeing the reliability of the results, which is critical for the legal assessment of digital evidence.*

Keywords*: digital evidence, information security, cybercrime, multi-level architecture of the software complex, functional requirements, non-functional requirements.*

Цифрові докази є невід'ємною частиною сучасного інформаційного простору та відіграють ключову роль у забезпеченні інформаційної безпеки. В умовах стрімкого розвитку інформаційних технологій та зростання кількості кіберзлочинів, цифрові докази стають все більш важливими для розслідування інцидентів, притягнення винних до відповідальності та запобігання майбутнім загрозам. Цифрові докази можуть містити широкий спектр даних, включаючи текстові документи, електронні листи, повідомлення, зображення, відео, аудіозаписи, метадані файлів, історію веб-перегляду, геолокаційні дані, логіни та паролі, криптографічні ключі тощо [1]. Вони можуть свідчити про дії користувачів, взаємодію між системами, часові рамки подій, зміст комунікацій та інші обставини, що мають значення для розслідування (виявлення кіберзагрози). Цифрові докази відіграють ключову роль у виявленні, розслідуванні та запобіганні різноманітним інцидентам інформаційної безпеки [2]. Робота з цифровими доказами має певні особливості та складності порівняно з традиційними доказами [3].

Дослідження фокусується на розробленні функціональної архітектури програмного комплексу, що вимагає детальної специфікації кожного етапу обробки даних. Практична реалізація вимагає чіткого визначення типів даних, обґрунтування вибору обчислювальних

бібліотек та розробки протоколів взаємодії між модулями системи. Саме сформовані вимоги визначають архітектуру програмного рішення, набір технологій, спосіб організації даних і логіку взаємодії між програмними компонентами.

До функціональних вимог віднесено можливість імпорту цифрових образів з різних джерел, валідацію вхідних даних, попередню обробку та нормалізацію, виділення ознак, запуск обраного алгоритму аналізу, накопичення проміжних і підсумкових результатів, а також формування звітних матеріалів. Окремо було виділено функції повторного аналізу, порівняння результатів різних моделей та фіксацією операцій користувача.

Нефункціональні вимоги описують властивості системи, які безпосередньо не стосуються окремих операцій, однак істотно впливають на ефективність її застосування. До них належать продуктивність обчислень, стійкість до помилок введення, можливість горизонтального розширення у випадку зростання обсягу даних, інформаційна безпека, контроль доступу, відтворюваність результатів і підтримка модульної заміни окремих алгоритмів.

Архітектурна модель орієнтована на відокремлення відповідальностей між компонентами. Модуль завантаження відповідає лише за отримання та первинну валідацію даних, модуль попередньої обробки – за їх стандартизацію, модуль ознак та опису – за обчислення інформативних характеристик, а аналітичний модуль – за інтерпретацію.

У межах дослідження архітектура системи була спроєктована за багаторівневим принципом (рис. 1). На нижньому рівні розміщено підсистему зберігання, яка відповідає за роботу з метаданими, файлами образів і результатами аналізу. Середній рівень формують сервіси прикладної логіки, у межах яких реалізовано попередню обробку, виділення ознак, аналітичні процедури та службові функції та історії. Сформована архітектура відповідає вимогам до подальшого розвитку. Завдяки модульності в неї можуть бути інтегровані додаткові способи сегментації, нові методи формування ознак, інші класифікатори або блоки пояснення рішень.

З погляду руху потоків даних система працює у такій послідовності: користувач формує запит на аналіз, завантажує образ носія або обирає об’єкт із наявного набору, після чого дані передаються в модуль попередньої обробки. Оброблений образ спрямовується до підсистеми виділення ознак, де формується вектор або дескриптор. Далі аналітичний модуль виконує класифікацію, ранжування чи пошук подібності; отримані результати зберігаються у базі даних і відображаються у візуальному інтерфейсі.

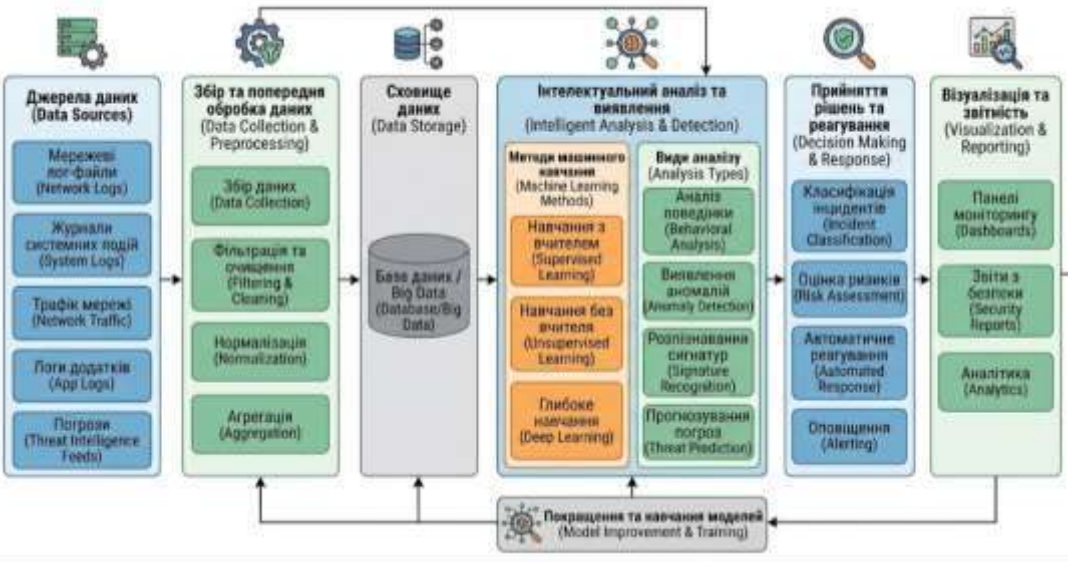

Рис. 1 – Узагальнена архітектура системи інтелектуального аналізу образів носіїв цифрових доказів

Для підвищення стійкості до відмов було передбачено додаткові механізми контролю: перевірка цілісності файлів, оброблення некоректних форматів, логування помилок, фіксація параметрів запуску моделі та відновлення сеансу користувача після збою.

Розроблена функціональна архітектура програмного комплексу забезпечує системний підхід до обробки цифрових доказів, поєднуючи суворі вимоги до інформаційної безпеки з гнучкістю інтелектуального аналізу. Завдяки впровадженню багаторівневого принципу побудови та чіткому розмежуванню відповідальностей між модулями – від завантаження й попередньої обробки до виділення ознак та інтерпретації результатів – система демонструє високу адаптивність до нових методів класифікації та типів даних. Таке архітектурне рішення дозволяє не лише автоматизувати рутинні процеси розслідування кіберінцидентів, а й гарантує достовірність і відтворюваність отриманих результатів, що є критично важливим для юридичної легітимності цифрових доказів.

Джерела та література

1. Liu D. Digital Forensics and Analyzing Data. Cisco Router and Switch Forensics. 2019. P. 15–38. URL: https://doi.org/10.1016/b978-1-59749-418-2.00001-6.

2. Hargreaves C., Nelson A., Casey E. An abstract model for digital forensic analysis tools A foundation for systematic error mitigation analysis. Forensic Science International: Digital Investigation. 2024. Vol. 48. P. 301679. URL: https://doi.org/10.1016/j.fsidi.2023.301679.

3. A Guide to Digital Forensics and Cybersecurity Tools (2026). URL: https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools.

УДК 004.9:504.064:711.4

Кульчицький С., Козак С.
Тернопільський національний технічний університет імені Івана Пулюя, Україна
Гончаренко А., доктор філософії
Київський національний університет будівництва і архітектури, Україна

ІНФОРМАЦІЙНО-АНАЛІТИЧНІ СИСТЕМИ ДЛЯ ПЛАНУВАННЯ ВІДБУДОВИ ТЕРИТОРІЙ З УРАХУВАННЯМ ЕКОЛОГІЧНИХ РИЗИКІВ

Анотація. *У тезах обґрунтовано доцільність застосування інформаційно-аналітичних систем для планування відбудови територій, що зазнали руйнувань унаслідок воєнних дій і техногенних впливів. Сучасне відновлення має базуватися на інтеграції просторових, екологічних, інфраструктурних і соціально-економічних даних, багатокритеріальному аналізі та засобах підтримки прийняття рішень. Запропоновано функціональну структуру системи, що охоплює модулі збору даних, геоінформаційного аналізу, оцінювання екологічних ризиків, сценарного моделювання та пріоритезації відновлювальних заходів. Визначено переваги використання таких систем для мінімізації вторинних загроз, підвищення управлінських рішень.*

Ключові слова: *інформаційна система, відбудова, екологічні ризики, геоінформаційний аналіз, підтримка прийняття рішень, моніторинг.*

Kulchytskyi S., Kozak S.
Ternopil Ivan Puluj National Technical University, Ukraine
Honcharenko A., Ph.D.
Kyiv National University of Construction and Architecture, Ukraine

INFORMATION-ANALYTICAL SYSTEMS FOR TERRITORY RECONSTRUCTION PLANNING WITH CONSIDERATION OF ENVIRONMENTAL RISKS

Abstract. *This paper justifies the use of information and analytical systems for planning the reconstruction of areas damaged by military action and man-made factors. Modern reconstruction must be based on the integration of spatial, environmental, infrastructural and socio-economic*