Хмельницький національний університет
Факультет інформаційних технологій
Кафедра комп'ютерної інженерії та інформаційних систем

# КВАЛІФІКАЦІЙНА РОБОТА

Метод та система інтелектуального аналізу образів носіїв цифрових доказів
Назва теми

Рівень вищої освіти *другий (магістерський)*

Галузь знань *12 «Інформаційні технології»*
Шифр, назва

Спеціальність *123 «Комп'ютерна інженерія»*
Шифр, назва

Освітня програма *«Комп'ютерна інженерія та програмування»*
Назва

Шифр КвРКІ 190186.19.01.08 ПЗ

Виконав здобувач IV курсу, група КІ2м-24-2 — Даніїл КОНДРАТЮК
Підпис — Ініціали, прізвище

Керівник — канд.-техн. наук, доцент — Катерина БЕРЕЗЬКА
Науковий ступінь, учене звання — Підпис — Ініціали, прізвище

Нормоконтролер — д. техн. наук, професор — Сергій ЛИСЕНКО
Науковий ступінь, учене звання — Підпис — Ініціали, прізвище

До захисту допускаю:
завідувач кафедри КІІС
«01» травня 2026 р.
дата — підпис — Ольга ПАВЛОВА
Ініціали, прізвище

Хмельницький 2026

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Кафедра КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ

Рівень вищої освіти ДРУГИЙ (МАГІСТЕРСЬКИЙ)

Галузь знань 12 ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Спеціальність 123 КОМП'ЮТЕРНА ІНЖЕНЕРІЯ

Освітня програма «КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА ПРОГРАМУВАННЯ»

ЗАТВЕРДЖУЮ
Завідувачка кафедри КІІС
Ольга ПАВЛОВА

" 12 " 01 2026 р.

**ЗАВДАННЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ**

Кондратюк Даніїл Вікторович
Прізвище, ім'я, по батькові студента

1. Тема проекту (роботи) Метод та система інтелектуального аналізу образів носіїв цифрових доказів
Керівник проекту (роботи) Березька Катерина Миколаївна, д.т.н., проф.
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання
Затверджена наказом ректора університету від 12.01.2026 р. № 6
2. Термін подання здобувачем роботи на кафедру 01.05.2026 р.
3. Вихідні дані до роботи Завдання на кваліфікаційну роботу
4. Зміст пояснювальної записки (перелік питань, які потрібно розробити)
Сучасний стан, проблематика та перспективні напрямки аналізу цифрових доказів в інформаційній безпеці. Розробка методу інтелектуального аналізу образів носіїв цифрових доказів. Проектування та реалізація системи інтелектуального аналізу. Порівняльний аналіз методів захисту та зберігання цифрових доказів.
5. Перелік графічного матеріалу (із зазначенням обов'язкових креслень)
Архітектура ПЗ проєкту
Архітектура ПЗ для кіберфізичної системи
Апаратне забезпечення проєкту

6. Консультанти розділів кваліфікаційної роботи

| Розділ | Прізвище, ініціали та посада консультанта | Підпис, дата | |
|---|---|---|---|
| | | завдання видав | завдання прийняв |
| | | | |
| | | | |

7. Дата видачі завдання «_12_»_____01_____2026 р.

## КАЛЕНДАРНИЙ ПЛАН

| №з/п | Назва етапів (розділів) дипломного проєкту (роботи) | Термін виконання етапів проєкту (роботи) | Примітка |
|---|---|---|---|
| 1 | Вибір напряму дослідження та узгодження тематики кваліфікаційної роботи з керівником | 12.01.2026 | виконано |
| 2 | Ознайомлення з предметною областю; формулювання мети та задач дослідження; визначення об'єкта та предмета дослідження | 15.01.2026 | виконано |
| 3 | Робота над розділом 1 – дослідження предметної області та постановка задачі | 01.02.2026 | виконано |
| 4 | Робота над розділом 2 – вибір компонентів для проєктування системи адаптивного застосування моніторингових елементів розвідувального БПЛА | 01.03.2026 | виконано |
| 5 | Робота над розділом 3 – проєктування системи адаптивного застосування моніторингових елементів розвідувального БПЛА | 29.03.2026 | виконано |
| 6 | Оформлення пояснювальної записки згідно вимог | 25.04.2026 | виконано |
| 7 | Попередній захист ВКР | 26.04.2025 | виконано |
| 8 | Захист ВКР на засіданні ЕК | травень 2026 року | |

Здобувач _____ Даниїл Кондратюк
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Катерина БЕРЕЗЬКА
Підпис Ім'я, ПРІЗВИЩЕ

# РЕФЕРАТ

Тема кваліфікаційної роботи магістра: Метод та система інтелектуального аналізу образів носіїв цифрових доказів

Автор роботи: Кондратюк Даніїл Вікторович.

Керівник роботи: Березька Катерина Миколаївна.

Пояснювальна записка: 71 с., 3 рис., 11 табл., 3 дод., 80 джерел.

ЦИФРОВІ ДОКАЗИ, МАШИННЕ НАВЧАННЯ, ГЛИБОКІ НЕЙРОННІ МЕРЕЖІ, КІБЕРБЕЗПЕКА, ЗАХИСТ ІНФОРМАЦІЇ, ІНТЕЛЕКТУАЛЬНИЙ АНАЛІЗ ДАНИХ, КОНТРОЛЬ ЦІЛІСНОСТІ

Об’єктом дослідження є процеси інтелектуального аналізу образів носіїв цифрових доказів з використанням методів машинного навчання та забезпечення їх кібербезпеки при зберіганні та обробці.

Предметом дослідження є методи, моделі, алгоритми та програмні засоби інтелектуального аналізу образів носіїв цифрових доказів.

Метою кваліфікаційної роботи магістра є підвищення ефективності, швидкодії та достовірності процесу аналізу цифрових доказів шляхом розроблення методу та системи інтелектуального аналізу образів носіїв, що забезпечує автоматизовану обробку цифрових даних, виділення ознак, класифікацію артефактів, виявлення аномалій та формування звітів.

Для розв’язання поставлених задач використовувалися методи основні положення теорії комп’ютерних мереж та систем, на основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення системи інтелектуального аналізу образів носіїв цифрових доказів, що включає модуль попередньої обробки та парсингу файлових систем.

Наукова новизна отриманих результатів:

– набув подальшого розвитку метод інтелектуального аналізу образів носіїв цифрових доказів, що відрізняється використанням композиції глибоких нейронних мереж для автоматичного виділення ознак, алгоритмів кластеризації для виявлення аномалій та захисту кіберсистеми.

– набула подальшого розвитку інформаційна технологія забезпечення цілісності цифрових доказів, що відрізняється застосуванням каскадного хешування з побудовою дерев Меркла та інкрементальною верифікацією через вибіркову перевірку блоків, що дозволяє скоротити час верифікації терабайтних образів.

– запропоновано математичну модель оцінки ефективності вибіркової верифікації цілісності великих образів носіїв через ймовірнісний аналіз виявлення модифікованих блоків, що дозволяє обґрунтовано визначати мінімальну кількість блоків для перевірки при заданій імовірності виявлення порушень цілісності;

На основі проведених досліджень розроблена архітектура і компоненти програмного забезпечення

Практична значимість отриманих результатів полягає у можливості застосування розробленої системи в правоохоронних органах для проведення криміналістичних експертиз комп'ютерної техніки, в корпоративних службах інформаційної безпеки для розслідування інцидентів та виявлення інсайдерських загроз, в організаціях з високими вимогами до захисту персональних даних для забезпечення відповідності GDPR.

У першому розділі проведено аналіз сучасного стану проблематики цифрових доказів та їх ролі в забезпеченні інформаційної безпеки. Розглянуто поняття образу носія інформації та вимоги до його створення з дотриманням криміналістичної коректності. Систематизовано методи та засоби отримання цифрових доказів, включаючи апаратні програмні утиліти створення образів та процедури забезпечення безпеки системи.

У другому розділі виконано формалізацію задачі інтелектуального аналізу образів носіїв через математичні моделі, що описують образ як впорядковану послідовність байтів з метаданими та криптографічними хешами.

У третьому розділі виконано проектування та реалізацію програмної системи інтелектуального аналізу образів носіїв. Сформульовано функціональні та нефункціональні вимоги до системи, включаючи підтримку популярних файлових систем, можливість паралельної обробки декількох образів, забезпечення

шифрування даних при зберіганні, автоматизацію моніторингу цілісності, детальний аудит усіх операцій. Розроблено мікросервісну архітектуру системи з виділенням окремих сервісів для шифрування, верифікації цілісності, управління ланцюгом зберігання доказів, виконання аналізу в ізольованих контейнерах.

У четвертому розділі виконано порівняльний аналіз методів захисту та зберігання цифрових доказів з акцентом на практичні аспекти використання. Проаналізовано класичний підхід локального зберігання без шифрування з виявленням критичної вразливості до фізичного доступу та відсутності резервного копіювання. Проведено кількісне порівняння методів за показниками швидкості шифрування, часу верифікації цілісності, стійкості до атак, повноти аудиту, економічної ефективності. Експериментально підтверджено перевагу розробленої системи за більшістю показників при оптимальному співвідношенні вартості та функціональності.

Результати роботи мають теоретичну та практичну значущість для галузі інформаційної безпеки, цифрової аналітики та судової експертизи комп'ютерних систем.

# ЗМІСТ

# СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

CI – судова інженерія (чи комп'ютерно-технічна експертиза)

СКБД – система керування базами даних

ШНМ (ANN) – штучна нейронна мережа

AWS – Amazon Web Services

CD/DVD – компакт-диск / цифровий багатоцільовий диск

CNN – згорткова нейронна мережа (Convolutional Neural Network)

CSV – формат представлення табличних даних (Comma-Separated Values)

EUI – розширений унікальний ідентифікатор

FAT / NTFS / ext4 – типи файлових систем

GPU – графічний процесор

HDD – жорсткий магнітний диск

JSON – текстовий формат обміну даними (JavaScript Object Notation)

MD5 / SHA-256 – алгоритми хешування (для перевірки цілісності образів)

NLP – обробка природної мови (Natural Language Processing)

OSINT – розвідка на основі відкритих джерел (Open Source Intelligence)

PCAP – формат файлу захоплення мережевого трафіку

# ВСТУП

У сучасному світі використовується широкий спектр обчислювальних систем, і в усіх цих системах енергоефективність і оптимізація продуктивності є надзвичайно важливими. Але оптимізація продуктивності означає різні речі для різних обчислювальних систем. Через відмінність природи обчислювальні системи мають різні вимоги до ефективності та оптимізації. Розподілені системи, такі як системи інтелектуальних мереж, периферійні обчислювальні середовища та системи блокчейн, зосереджені на поведінці агентів. Таким чином, застосування принципів мережевої економіки, таких як теорія ігор і теорія контрактів, може покращити роботу цих систем багатьма способами.

Оптимізація продуктивності систем інтелектуальних мереж є критично важливою для забезпечення ефективного використання енергії, надійності постачання та зменшення витрат. Інтелектуальні мережі інтегрують традиційні електричні мережі з інформаційно-комунікаційними технологіями, що дозволяє більш гнучко та ефективно управляти потоками енергії.

Актуальність роботи полягає у необхідності створення нових інтелектуальних методів захисту ПК, які здатні протидіяти сучасним кіберзагрозам в умовах неефективності класичних засобів безпеки та постійного зростання складності ворожих атак системи.

Метою кваліфікаційної роботи магістра є підвищення ефективності, швидкодії та достовірності процесу аналізу цифрових доказів шляхом розроблення методу та системи інтелектуального аналізу образів носіїв, що забезпечує автоматизовану обробку цифрових даних, виділення ознак, класифікацію артефактів, виявлення аномалій та формування звітів.

Поставлена мета досягається розв’язанням таких основних задач:

− вперше запропоновано метод інтелектуальної класифікації фрагментів даних, на основі нейронних мереж, що дозволяє ідентифікувати тип файлу навіть за повної відсутності заголовків та метаданих.

– удосконалено алгоритм семантичного пошуку в образах носіїв шляхом впровадження векторних представлень, що забезпечує знаходження доказів не за ключовими словами, а за контекстною схожістю.

– запропоновано архітектурне рішення системи розподіленого аналізу цифрових образів, яке дозволяє прискорити процес індексації даних на GPU рівні, що скорочує час обробки терабайтних масивів.

Об’єктом дослідження є процеси забезпечення безпеки та цілісності інформації в персональних комп’ютерах (робочих станціях), а також методи виявлення та аналізу цифрових слідів у середовищі під впливом деструктивних програмних впливів..

Предметом дослідження є методи інтелектуального аналізу образів носіїв даних, алгоритми машинного навчання для виявлення аномалій, а також програмні механізми багаторівневого захисту системи від зовнішніх втручань та змагальних атак.

Наукова новизна отриманих результатів:

– розробці концептуально нової архітектури інтелектуального захисту персональних комп’ютерів, яка вперше базується на принципі синергетичної інтеграції програмних засобів безпеки з системами безперервного динамічного моніторингу.

– створенні адаптивного методу багатофакторного виявлення аномалій, що використовує ансамблі алгоритмів машинного навчання для ідентифікації прихованих загроз у режимі реального часу.

Практична значимість отриманих результатів полягає у виконаного наукового дослідження було розроблено та обґрунтовано архітектуру інтелектуальної системи захисту ПК, яка базується на синергії програмних механізмів безпеки та методів машинного навчання.

Для розв’язання поставлених задач використовувалися методи забезпечення функціонування систем з IoT, методи математичного моделювання.

За темою кваліфікаційної роботи опубліковано одну публікацію [81] у Збірнику наукових праць за матеріалами XVI Всеукраїнської науково-практичної

конференції «Актуальні проблеми комп’ютерних наук АПКН-2024». (Хмельницький – 2023. – С. 303-305).

# 1 СУЧАСНИЙ СТАН, ПРОБЛЕМАТИКА ТА ПЕРСПЕКТИВНІ НАПРЯМКИ АНАЛІЗУ ЦИФРОВИХ ДОКАЗІВ В ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

## 1.1. Поняття цифрових доказів та їх роль в інформаційній безпеці

Ефективний захист інформаційного середовища сьогодні неможливий без використання електронних доказів, які є ключовим ресурсом для розкриття кіберзлочинів та побудови надійних бар'єрів проти майбутніх атак у світі високих технологій, стабільність будь-якої цифрової інфраструктури визначається її здатністю протистояти втручанням, що традиційно оцінюється через призму концепції CIA. Дана модель охоплює три фундаментальні вектори: дотримання таємності (конфіденційність), збереження незмінності даних (цілісність) та безперебійний доступ до ресурсів (доступність).

Таблиця 1.1 – Основні принципи кібербезпеки

| № | Принцип | Сутність та призначення | Приклади реалізації |
|---|---|---|---|
| 1. | Конфіденційність (Confidentiality) | Обмеження доступу до даних лише для авторизованих користувачів, запобігання витоку інформації. | Шифрування, двофакторна автентифікація, керування правами доступу. |
| 2. | Цілісність (Integrity) | Гарантія точності, повноти та захисту інформації від несанкціонованої зміни або видалення. | Цифрові підписи, контрольні суми (хешування), фіксація змін. |

Кінець таблиці 1.1

| | | | |
|---|---|---|---|
| 3. | Доступність (Availability) | Забезпечення безперебійного доступу легітимних користувачів до сервісів та даних у будь-який час. | Резервне копіювання, захист від DDoS-атак, відмовостійкі сервери. |

Аналіз даних свідчить, що кібербезпека не обмежується лише технічним захистом даних, це комплексна система, де конфіденційність гарантує приватність, цілісність забезпечує достовірність інформації, а доступність дозволяє системам безперебійно виконувати свої функції. Порушення хоча б одного з цих принципів може призвести до дестабілізації інформаційного простору, що робить їх дотримання пріоритетним завданням для будь-якої сучасної організації чи користувача. Аналіз та специфіка практичного застосування цих компонентів деталізована в (табл. 1.1).

Згідно з визначенням, наведеним у міжнародному стандарті ISO/IEC 27037:2012 [1], цифрові докази – це інформація або дані, збережені чи передані в цифровій формі, які мають доказову цінність і можуть бути використані в судовому процесі. Вони можуть бути отримані з різноманітних джерел, таких як комп'ютери, мобільні пристрої, сервери, хмарні сховища, мережеве обладнання, бази даних, журнали подій та інші електронні носії інформації [2]. 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 [3]. Вони можуть свідчити про дії користувачів, взаємодію між системами, часові рамки подій, зміст комунікацій та інші обставини, що мають значення для розслідування (виявлення кіберзагрози).

Стрімка еволюція технологій декларує відповідне ускладнення протидіям кібератакам. Це перетворює проблему забезпечення кіберстійкості на один із

пріоритетних векторів національної безпеки та стабільності функціонування суб’єктів господарювання. Аналіз динаміки загроз упродовж 2024–2025 років свідчить про зміщення акцентів у бік застосування алгоритмів штучного інтелекту зловмисниками та зростання кількості деструктивних впливів на об’єкти критичної інфраструктури.

Ефективна викликам сучасності [4-16] вимагає переходу від точкового впровадження програмних засобів до формування цілісних стратегій, що інтегрують технічні, організаційно-управлінські та нормативно-правові аспекти. У таблиці 1.2 проведено систематизацію актуальних кіберзагроз та запропоновано комплексні підходи до їх нейтралізації.

Актуальність зазначеної проблематики посилюється умовами тотальної цифровізації [17], де наявність вразливостей в архітектурі інформаційних систем [18-19] створює ризики масштабних фінансових збитків або компрометації персональних даних великих масивів користувачів.

Сучасні кіберзагрози трансформувалися з ізольованих інцидентів у скоординовані кібероперації, що здатні дестабілізувати роботу стратегічних галузей економіки. У зв'язку з цим, розроблення ефективних методів захисту [18] потребує безперервного моніторингу ландшафту загроз та імплементації адаптивних безпекових політик. Наведені у (таблиці 1.2) дані підтверджують, що сучасна екосистема кіберзагроз є динамічною та багаторівневою. Основним трендом стає поєднання технічних методів злому з психологічним маніпулюванням, що потребує від суб’єктів захисту не лише оновлення програмного забезпечення, а й активного розвитку цифрової грамотності користувачів. Отже, вирішення проблеми кіберзагроз [19] лежить у площині проактивної оборони: від своєчасного резервування даних до інтеграції інтелектуальних систем моніторингу трафіку. Тільки за умови комплексного застосування запропонованих шляхів можна забезпечити стійкість інформаційного простору до сучасних викликів, мінімізуючи ризики для конфіденційної інформації та критичних сервісів.

Таблиця 1.2 – Кіберзагроза як актуальна проблема сьогодення та шляхи її вирішення

| № | Тип загрози | Характеристика та тренди 2025 | Шляхи вирішення та захисту |
|---|---|---|---|
| 1. | ШІ-фішинг та діпфейки | Використання ШІ для створення надреалістичних повідомлень та підробки голосу-відео. | Впровадження систем автентифікації на основі нульової довіри (Zero Trust), навчання персоналу кібергігієні. |
| 2. | Ransomware (вимагачі) | Шифрування даних з метою викупу; атаки на критичну інфраструктуру та бізнес. | Регулярне офлайн-резервування даних (Backups), використання антивірусних рішень з поведінковим аналізом. |
| 3. | Ланцюги постачання (Supply Chain) | Компрометація ПЗ через вразливості у сторонніх розробників або оновленнях. | Ретельний аудит безпеки вендорів, моніторинг цілісності коду, використання рішень зокрема, від Kyivstar Business Hub для бізнесу. |
| 4. | Державно-спонсоровані атаки | Деструктивні операції проти урядових структур та енергетики, переважно з боку ворожих атак | Посилення державного кіберзахисту згідно з Стратегією кібербезпеки України, співпраця з CERT-UA. |
| 5. | DDoS-атаки | Масоване блокування доступу до веб-ресурсів через мережі ботнетів. | Використання хмарних фільтрів трафіку (наприклад, Cloudflare), масштабування серверної інфраструктури. |

Цифрові докази відіграють ключову роль у виявленні, розслідуванні та запобіганні різноманітним інцидентам інформаційної безпеки [23-40]. Вони дозволяють встановлювати факти несанкціонованого доступу до систем і даних, витоку конфіденційної інформації, розповсюдження шкідливого програмного забезпечення, мережевих атак, шахрайства з використанням електронних засобів, порушень прав інтелектуальної власності та інших протиправних дій у цифровому просторі. В судовій практиці цифрові докази використовуються для доведення вини або невинуватості підозрюваних, встановлення обставин злочину, спростування або підтвердження алібі, виявлення мотивів та намірів злочинців. Вони можуть бути представлені в якості речових доказів, експертних висновків, результатів слідчих дій та інших процесуальних документів [6].

Стрімка трансформація суспільних відносин у бік цифрової взаємодії призвела до суттєвих змін у процесуальному праві, де традиційні методи збирання доказів поступово доповнюються або замінюються цифровими методами. Сучасна судова система все частіше стикається з необхідністю опрацювання великих масивів електронних даних, які стають ключовим інструментом для встановлення істини у кримінальних, цивільних та адміністративних справах. Цифрові докази мають унікальну здатність фіксувати події з високою точністю, що дозволяє правоохоронним органам та адвокатам будувати обґрунтовані лінії захисту або обвинувачення на основі об’єктивних даних.

Важливою особливістю таких доказів є їхня невидимість для пересічного користувача, що дозволяє виявляти приховані факти правопорушень, які неможливо зафіксувати у фізичному світі. Для чіткого розуміння структури та походження таких даних, нижче представлена класифікація, що відображає основні типи цифрових доказів, які сьогодні використовуються у судочинстві (табл.1.3).

Отже, роль цифрових доказів у доведенні вини або невинуватості особи постійно зростає, що вимагає від юристів та судових експертів не лише правових знань, а й глибокого розуміння принципів функціонування інформаційних технологій. Це дозволяє забезпечити справедливий розгляд справи, спираючись на беззаперечні факти, зафіксовані в цифровому просторі.

Таблиця 1.3 – Сучасна судова система цифрові докази використовуються для доведення вини або невинуватості підозрюваних

| № | Вид цифрового доказу | Джерела отримання даних | Значення для процесу доведення |
|---|---|---|---|
| 1. | Комунікаційні дані | Месенджери (Telegram, WhatsApp), електронна пошта, логи дзвінків. | Встановлення контактів між особами, змісту домовленостей, намірів або погроз. |
| 2. | Метадані файлів | Електронні документи, фотографії (EXIF-дані), відеозаписи. | Визначення точного часу створення файлу, його автора та геолокації (місця зйомки). |
| 3. | Мережева активність | IP-адреси, історія браузера, логи серверів, активність у соцмережах. | Доведення факту перебування користувача на певних ресурсах або здійснення транзакцій. |
| 4. | Дані з пристроїв | Смартфони, ноутбуки, "розумні" годинники, реєстратори. | Відстеження маршрутів пересування (GPS), біометричні дані, вилучені файли. |
| 5. | Хмарні дані | Google Drive, iCloud, Dropbox, сховища Apple/Microsoft. | Доступ до заархівованої інформації, яка могла бути видалена з фізичного носія. |

Використання електронних слідів для доведення вини або невинуватості підозрюваних базується на принципі ідентифікації користувача через його цифрову активність. Це включає не лише аналіз безпосереднього вмісту повідомлень, а й дослідження складних логічних зв'язків між різними інформаційними системами.

Цифрові докази є важливими для проведення внутрішніх розслідувань в організаціях, пов'язаних з порушеннями політик безпеки, зловживаннями службовим становищем, витоками даних та іншими інцидентами, дозволяють відстежувати дії співробітників, виявляти аномалії та відхилення від встановлених процедур, встановлювати часові рамки подій та зв'язки між різними елементами доказів [5].

Синергія основних принципів кібербезпеки та інструментарію цифрової криміналістики створює фундамент для стабільного розвитку сучасного бізнесу. В умовах глобальної цифровізації безпечне ведення господарської діяльності неможливе без превентивних заходів захисту та готовності до оперативного розслідування інцидентів. Кібербезпека забезпечує створення "захисного контуру", що запобігає витоку конфіденційної інформації, тоді як цифрові докази стають інструментом правового захисту інтересів компанії у разі вчинення правопорушень. Такий комплексний підхід дозволяє не лише мінімізувати ризики, а й сформувати довіру з боку клієнтів та партнерів. У таблиці 1.4 розглянуто взаємозв'язок цих компонентів у контексті корпоративної безпеки.

Поки заходи кібербезпеки працюють на випередження, запобігаючи несанкціонованому доступу, цифрова доказова база забезпечує можливість притягнення зловмисників до відповідальності, що виконує превентивну функцію. Таким чином, інтеграція технічних рішень у правове поле бізнесу стає необхідною умовою для попередження витоку критичних даних та забезпечення довгострокової конкурентоспроможності на ринку, можуть бути розподілені між різними юрисдикціями та перебувати під контролем різних суб'єктів, що створює додаткові правові та організаційні складності.

Необхідність отримання доступу до даних, що зберігаються на серверах в інших країнах, дотримання вимог законодавства щодо захисту персональних даних і конфіденційності, узгодження дій між правоохоронними органами різних держав - все це вимагає розвитку міжнародного співробітництва та уніфікації підходів до роботи з цифровими доказами [9].

Таблиця 1.4 – Роль кібербезпеки та цифрових доказів у забезпеченні стійкості бізнесу

| № | Напрямок безпеки | Функціональна роль у бізнесі | Механізм реалізації та попередження витоків |
|---|---|---|---|
| 1. | Кібербезпека (Превенція) | Створення бар'єрів для зовнішніх та внутрішніх загроз. | Впровадження DLP-систем (захист від витоків), шифрування комерційної таємниці, контроль доступу. |
| 2. | Моніторинг та аудит | Виявлення аномальної активності в реальному часі. | Збір системних логів, аналіз поведінки користувачів, виявлення спроб несанкціонованого копіювання даних. |
| 3. | Цифрові докази (Реагування) | Юридична фіксація фактів порушень (наприклад, крадіжки інтелектуальної власності). | Збереження цілісних образів дисків, фіксація цифрових слідів для подання позовів проти недобросовісних співробітників чи конкурентів. |
| 4. | Compliance (Відповідність) | Дотримання галузевих та державних стандартів безпеки. | Регулярний аудит систем на відповідність GDPR або ISO 27001, що мінімізує юридичні та репутаційні ризики. |

Ще однією особливістю цифрових доказів є їх висока залежність від контексту та інтерпретації. На відміну від традиційних доказів, які часто мають очевидний фізичний прояв, цифрові докази можуть по-різному трактуватися

залежно від обставин їх отримання, зв'язків з іншими елементами доказової бази, технічних особливостей систем і середовищ. Тому, для коректної оцінки та використання цифрових доказів необхідні спеціальні експертні знання та врахування широкого контексту розслідування [10].

Незважаючи на складності та виклики, цифрові докази відіграють все більш важливу роль у забезпеченні інформаційної безпеки та протидії кіберзлочинності. Розвиток ефективних методів і засобів роботи з цифровими доказами, підготовка кваліфікованих фахівців, удосконалення правової бази та міжнародної співпраці є пріоритетними напрямками в цій галузі. Таким чином, цифрові докази є невід'ємною частиною сучасного інформаційного простору та відіграють ключову роль у забезпеченні інформаційної безпеки.

## 1.2. Аналіз методів і засобів отримання та дослідження цифрових доказів

Ефективне отримання та дослідження цифрових доказів є ключовим завданням для забезпечення їх допустимості та доказової сили в судовому процесі. Це вимагає застосування науково обґрунтованих методів і спеціалізованих технічних засобів, які дозволяють зберегти цілісність і автентичність даних, виявити релевантну інформацію та провести її всебічний аналіз.

Одним з основоположних принципів роботи з цифровими доказами є забезпечення їх незмінності та запобігання випадковому або навмисному пошкодженню. Для цього застосовується метод створення побітових (форензичних) копій носіїв інформації, який дозволяє отримати точний образ вихідних даних без внесення жодних змін [11]. Цей процес здійснюється за допомогою спеціалізованого програмного забезпечення та апаратних пристроїв, таких як Tableau Forensic Imager, Logicube Forensic Falcon-NEO, ICS Image MASSter Solo-4 Forensics та інші [12] (рисунок 1.5).

Для відновлення видалених файлів і даних, які можуть містити важливі докази, використовуються спеціальні програмні інструменти. Такі утиліти, як Recuva, PhotoRec, R-Studio, Ontrack EasyRecovery сканують носії інформації на

низькому рівні та дозволяють відновити файли, видалені з використанням стандартних засобів операційної системи або в результаті форматування [13]. Це дає можливість отримати доступ до прихованої інформації та відновити дані, які зловмисники намагалися знищити. Процес відновлення видалених файлів та фрагментованих даних є ключовим етапом цифрової криміналістики, оскільки він дозволяє реконструювати події, які зловмисники намагалися приховати.

Рисунок. 1.5 – Зовнішній вигляд Tableau Forensic Imager TX1 [38]

В основі роботи сучасних інструментів, таких як Recuva, PhotoRec, R-Studio та Ontrack EasyRecovery, лежить принцип інертності файлових систем: при стандартному видаленні операційна система лише маркує відповідні блоки пам'яті як "вільні", залишаючи фізичний вміст файлу незмінним до моменту його повної перезаписи новими даними (рисунок 1.6). Для роботи з метаданими використовуються такі інструменти, як ExifTool, Metadata Extraction Tool, Foca та інші (рисунок 1.7). Для забезпечення процесуальної достовірності відновлених даних, робота з програмним забезпеченням проводиться виключно з використанням побітових копій (дампів) носіїв інформації. Це виключає ризик ненавмисної модифікації даних у процесі сканування. Таким чином, використання спеціалізованого інструментарію перетворює спроби знищення інформації на марні дії, забезпечуючи правоохоронні органи та експертів можливістю встановити

істину, спираючись на відновлені цифрові артефакти. Важливим аспектом дослідження цифрових доказів є аналіз метаданих файлів. Метадані містять інформацію про автора, дату створення та модифікації, використане програмне забезпечення, місцезнаходження та інші атрибути файлів.

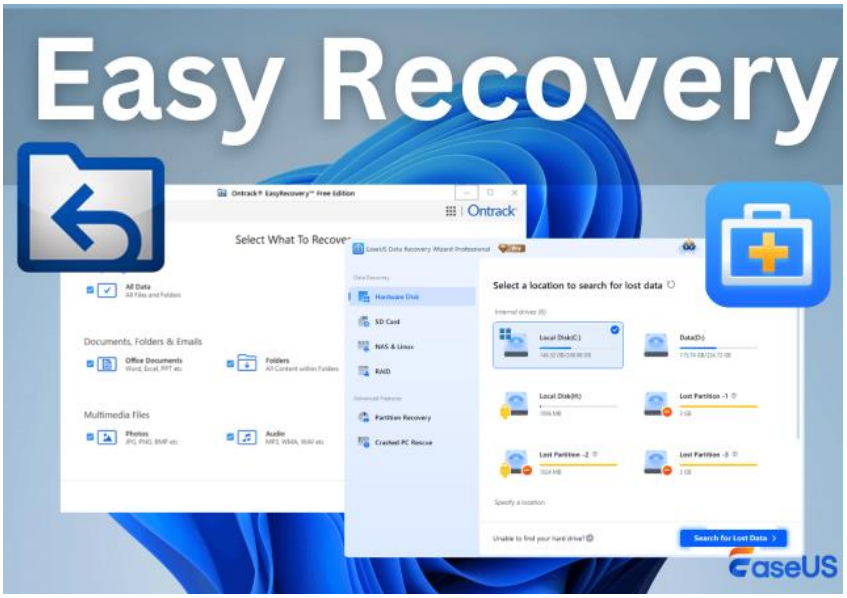



Рисунок. 1.6 – Програмне забезпечення для відновлення даних Easy Recovery [39]

Аналіз метаданих дозволяє встановити часові рамки подій, виявити зв'язки між різними документами та ідентифікувати джерела походження даних [14].

Окрім традиційних методів, все більшого поширення набувають підходи, засновані на використанні технологій штучного інтелекту та машинного навчання. Ці підходи дозволяють автоматизувати процеси виявлення, класифікації та аналізу цифрових доказів, особливо у випадках великих обсягів неструктурованих даних [16].

Наприклад, алгоритми комп'ютерного зору можуть використовуватися для автоматичного розпізнавання обличь, об'єктів і тексту на зображеннях і відео, виявлення дублікатів і схожих файлів. Методи обробки природної мови дозволяють здійснювати семантичний аналіз текстових документів, виявляти ключові теми та зв'язки між ними.

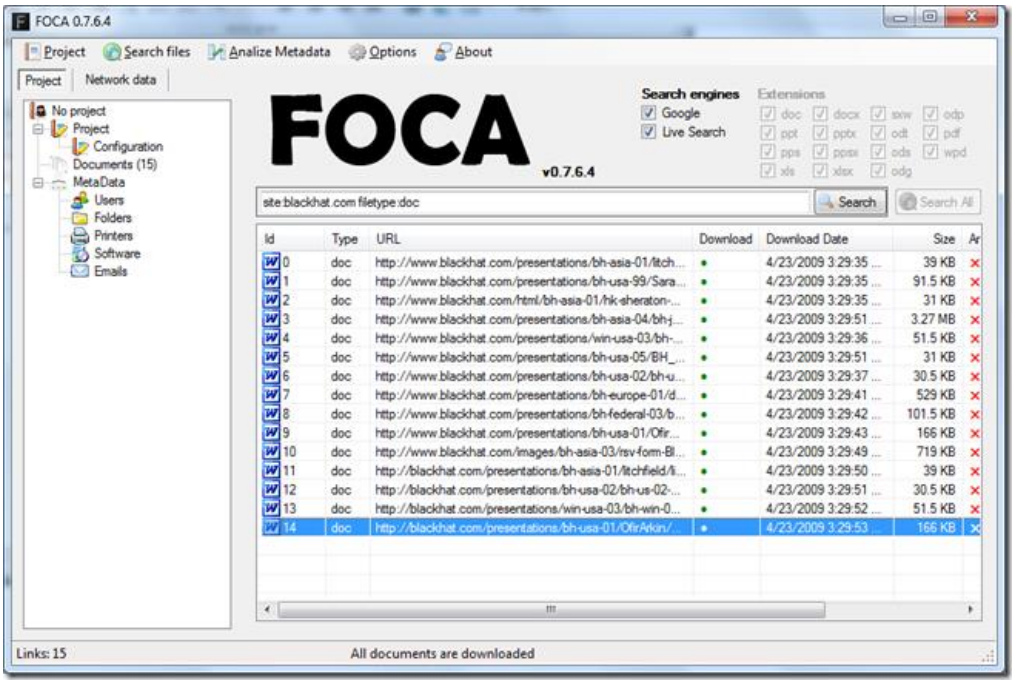



Рисунок. 1.7 – Програмне забезпечення Foca для роботи з метаданими [40]

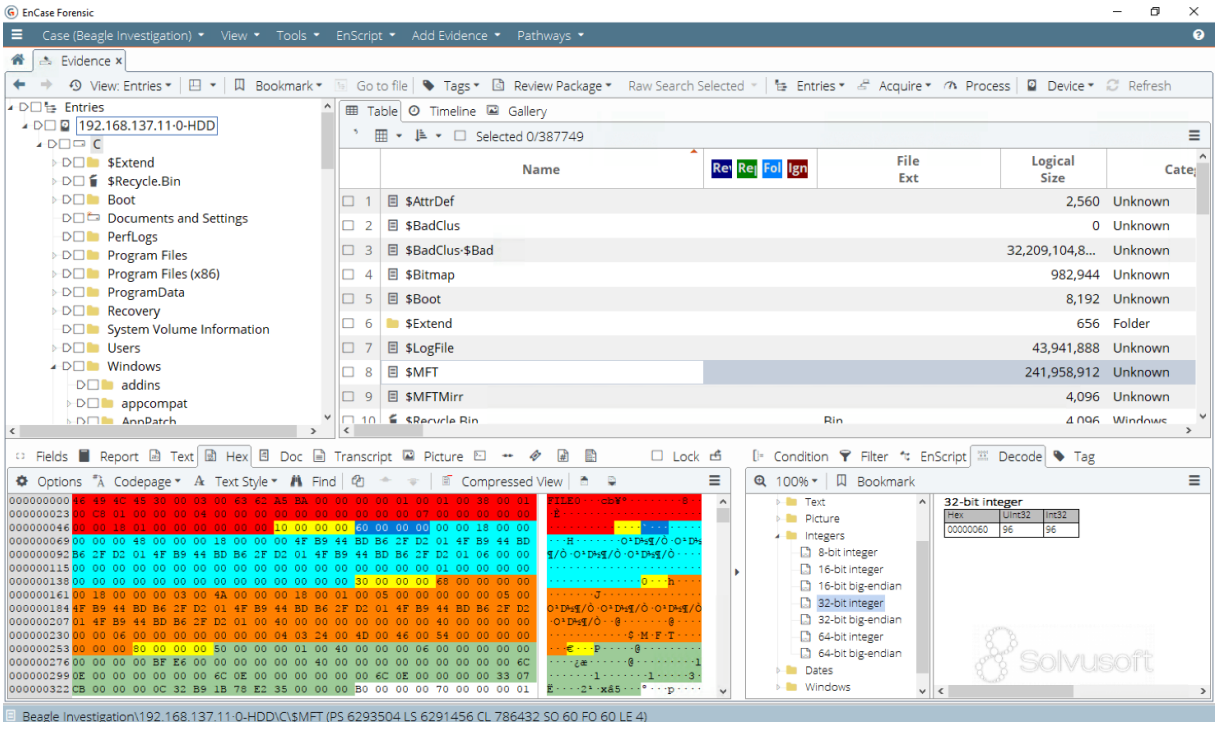



Рисунок 1.8 – Програмне забезпечення EnCase Forensic [41]

Вони дозволяють отримувати доступ до даних пристрою, включаючи контакти, повідомлення, історію дзвінків, геолокаційні дані, файли додатків тощо [18]. Такі рішення, як EnCase Forensic, Cellebrite UFED, Oxygen Forensic Detective,

XRY дозволяють здійснювати повне вилучення та аналіз даних з різних моделей мобільних пристроїв та операційних систем (рисунок 1.8).

Ще одним важливим аспектом дослідження цифрових доказів є аналіз хмарних сервісів і віддалених сховищ даних. З поширенням хмарних технологій, все більше важливої інформації зберігається на віддалених серверах, що вимагає спеціальних підходів до її отримання та аналізу [19]. Для цього застосовуються методи віддаленого доступу, отримання резервних копій, аналізу синхронізованих даних та інші. Такі інструменти, як Magnet AXIOM Cloud, Cellebrite UFED Cloud Analyzer дозволяють автоматизувати процеси витягування та аналізу даних з популярних хмарних сервісів.

Загалом, методи та засоби отримання і дослідження цифрових доказів постійно розвиваються та вдосконалюються, [45-80] відповідаючи на нові виклики та потреби у сфері інформаційної безпеки. Їх ефективне застосування вимагає глибоких знань в галузі комп'ютерних технологій, права та інших суміжних дисциплін. Важливо забезпечувати відповідність методів і засобів дослідження цифрових доказів міжнародним стандартам і кращим практикам, дотримуватися принципів законності, етичності та прозорості при роботі з даними.

Таким чином, ефективне отримання та дослідження цифрових доказів є ключовим фактором успішного розслідування інцидентів інформаційної безпеки та протидії кіберзлочинності. Застосування науково обґрунтованих методів, спеціалізованих технічних засобів та інноваційних підходів, таких як використання штучного інтелекту та машинного навчання, дозволяє вирішувати складні завдання виявлення, аналізу та інтерпретації цифрових доказів. Водночас, ця галузь вимагає постійного розвитку та адаптації до нових викликів і загроз, що виникають в умовах стрімкого розвитку інформаційних технологій.

## 1.3. Огляд існуючих систем інтелектуального аналізу образів носіїв

Стрімкий розвиток технологій штучного інтелекту та комп'ютерного зору відкриває нові можливості для автоматизації процесів виявлення, класифікації та

аналізу візуальних даних в контексті дослідження цифрових доказів. Системи інтелектуального аналізу образів носіїв дозволяють значно підвищити ефективність обробки великих обсягів мультимедійної інформації та виявлення прихованих закономірностей, які можуть мати ключове значення для розслідування.

Одним з лідерів у цій галузі є платформа Cellebrite Visual Analytics, яка надає потужні інструменти для аналізу зображень і відео, отриманих з різних джерел цифрових доказів [20]. Ця система використовує алгоритми глибокого навчання для автоматичного розпізнавання облич, об'єктів, тексту, а також виявлення дублікатів і схожих зображень. Cellebrite Visual Analytics дозволяє будувати зв'язки між різними елементами доказів на основі візуальної схожості, що допомагає встановлювати спільні риси та закономірності в масивах мультимедійних даних.

Іншим потужним рішенням є система Magnet AXIOM, яка включає модуль штучного інтелекту для аналізу та категоризації мультимедійного контенту [21]. Ця система здатна автоматично групувати зображення за різними категоріями, такими як зброя, наркотики, гроші, документи тощо, що значно спрощує навігацію та пошук релевантних доказів. Крім того, Magnet AXIOM використовує алгоритми виявлення аномалій для ідентифікації нетипових або підозрілих зображень, які можуть вказувати на протиправну активність.

Серед відкритих проектів в галузі інтелектуального аналізу образів носіїв варто відзначити систему Autopsy, яка має модуль Image Analyzer [22]. Цей модуль дозволяє здійснювати пошук зображень за різними критеріями, такими як колір, розмір, тип файлу, а також виявляти дублікати та схожі зображення. Image Analyzer також має функції розпізнавання облич та тексту, що дозволяє автоматизувати процеси ідентифікації осіб та вилучення текстової інформації з зображень.

Окрім універсальних платформ, існують також спеціалізовані системи, орієнтовані на аналіз конкретних типів візуальних даних. Наприклад, система Amped Authenticate призначена для виявлення ознак редагування та фальсифікації цифрових зображень і відео [23]. Вона використовує алгоритми аналізу метаданих, виявлення слідів стиснення, аналізу шумів та інші методи для визначення

автентичності та цілісності візуальних доказів. Це особливо важливо в умовах поширення дезінформації та використання технологій штучного інтелекту для створення реалістичних підробок.

Інший приклад спеціалізованої системи - Videntifier Forensic, яка призначена для автоматичного виявлення та класифікації зображень і відео, пов'язаних з експлуатацією дітей та розповсюдженням дитячої порнографії [24]. Ця система використовує передові алгоритми комп'ютерного зору та машинного навчання для ідентифікації відомих та нових зразків протиправного контенту, що допомагає правоохоронним органам боротися з цим тяжким злочином.

Незважаючи на значні досягнення в розвитку систем інтелектуального аналізу образів носіїв, все ще існують певні обмеження та проблеми. Зокрема, ефективність цих систем значною мірою залежить від якості та репрезентативності навчальних даних, на основі яких створюються моделі машинного навчання [25]. Неповні, неточні або упереджені навчальні вибірки можуть призводити до помилкових спрацювань, пропуску важливих доказів або дискримінаційних результатів. Інтерпретація результатів інтелектуального аналізу образів носіїв часто вимагає експертної оцінки та врахування широкого контексту розслідування. Автоматизовані системи можуть виявляти певні закономірності та зв'язки, але остаточне рішення щодо їх значущості та доказової цінності має прийматися кваліфікованими фахівцями з урахуванням всіх обставин справи [26].

Ще однією проблемою є забезпечення прозорості та відтворюваності результатів інтелектуального аналізу образів носіїв. Зважаючи на складність алгоритмів машинного навчання та значний вплив навчальних даних, може бути важко пояснити та обґрунтувати отримані результати в суді [27]. Тому, важливо розробляти методи інтерпретації та візуалізації роботи систем штучного інтелекту, які будуть зрозумілі для учасників судового процесу та дозволять оцінити надійність і допустимість доказів.

Загалом, системи інтелектуального аналізу образів носіїв є потужним інструментом для дослідження цифрових доказів, який дозволяє автоматизувати трудомісткі процеси обробки мультимедійних даних та виявлення прихованих

закономірностей. Однак, їх ефективне використання вимагає розуміння обмежень і потенційних проблем, пов'язаних з якістю навчальних даних, інтерпретацією результатів та забезпеченням прозорості. Подальший розвиток цих систем має бути спрямований на підвищення їх надійності, зрозумілості та відповідності правовим і етичним вимогам.

Система автоматично групує зображення за категоріями, такими як обличчя, документи, зброя тощо, що дозволяє швидко знаходити релевантні докази. Також, на інтерфейсі представлені інструменти для пошуку дублікатів і схожих зображень, розпізнавання тексту та виявлення аномалій. Візуальне представлення зв'язків між різними елементами доказів дозволяє будувати хронологію подій та виявляти приховані закономірності в масивах мультимедійних даних.

## 1.4. Проблеми та перспективні напрямки розвитку інтелектуального аналізу цифрових доказів

Незважаючи на значний прогрес у розвитку методів і технологій інтелектуального аналізу цифрових доказів, ця галузь стикається з рядом проблем і викликів, які потребують вирішення для забезпечення ефективного та надійного розслідування інцидентів інформаційної безпеки.

Однією з ключових проблем є забезпечення цілісності та достовірності цифрових доказів в умовах зростаючої складності та розповсюдженості методів фальсифікації даних. Зловмисники використовують передові технології, такі як глибокі підробки (deepfakes), стеганографію, маніпуляції з метаданими тощо, щоб приховати або спотворити цифрові докази [28]. Це створює значні труднощі для виявлення та доведення автентичності доказів, особливо в умовах обмежених ресурсів і часу. Для вирішення цієї проблеми необхідний розвиток надійних методів виявлення та аналізу ознак фальсифікації цифрових доказів. Це може включати використання алгоритмів машинного навчання для автоматичного розпізнавання аномалій і слідів редагування, аналіз метаданих і цифрових підписів

для перевірки цілісності даних, а також розробку стандартизованих протоколів і процедур для забезпечення належного збору та зберігання доказів [29].

Іншою важливою проблемою є обробка та аналіз великих обсягів неструктурованих даних, які можуть містити цінні докази. З постійним зростанням обсягів інформації, що генерується та зберігається в цифровому вигляді, традиційні методи ручного аналізу стають все менш ефективними та практично неможливими [30]. Це вимагає розробки масштабованих та обчислювальних ефективних алгоритмів і систем, здатних впоратися з величезними обсягами даних та виявити приховані закономірності.

Перспективним напрямком вирішення цієї проблеми є застосування технологій розподілених обчислень і хмарних платформ для паралельної обробки та аналізу даних [31]. Використання апаратних прискорювачів, таких як графічні процесори (GPU) та тензорні процесори (TPU), дозволяє значно пришвидшити виконання складних алгоритмів машинного навчання та обробки великих даних. Також, важливим є розвиток методів інтелектуального стиснення та індексації даних, які дозволяють ефективно зберігати та швидко отримувати доступ до релевантної інформації.

Ще однією проблемою є необхідність забезпечення конфіденційності та дотримання етичних норм при роботі з цифровими доказами, які часто містять чутливу особисту інформацію. Використання методів інтелектуального аналізу даних, таких як профілювання, поведінковий аналіз, розпізнавання облич тощо, може призвести до порушення прав на приватність та потенційних зловживань [32]. Тому, важливо розробляти та впроваджувати надійні механізми захисту конфіденційності, такі як анонімізація даних, диференційована приватність, гомоморфне шифрування, які дозволяють проводити аналіз без розкриття персональної інформації [33].

Крім того, використання технологій штучного інтелекту в галузі цифрової криміналістики піднімає питання етичності, неупередженості та прозорості прийняття рішень. Моделі машинного навчання можуть успадковувати упередження та дискримінаційні шаблони, присутні в навчальних даних, що може

призвести до несправедливих або помилкових висновків [34]. Тому, важливо розробляти методи виявлення та усунення упереджень в алгоритмах, забезпечувати різноманітність і збалансованість навчальних даних, а також впроваджувати механізми пояснюваності та інтерпретації роботи моделей штучного інтелекту.

Серед перспективних напрямків розвитку інтелектуального аналізу цифрових доказів можна відзначити використання технології блокчейн для забезпечення цілісності, незмінності та простежуваності доказів. Блокчейн дозволяє створювати розподілені реєстри транзакцій, які криптографічно захищені від підробки та несанкціонованих змін [35]. Це може значно підвищити довіру до цифрових доказів та спростити процеси їх верифікації та обміну між різними учасниками розслідування.

Іншим перспективним напрямком є розвиток методів федеративного навчання та спільного аналізу даних, які дозволяють проводити розподілене навчання моделей машинного навчання на даних з різних джерел без необхідності їх централізованого збору та обміну [36]. Це відкриває можливості для безпечної та конфіденційної співпраці між різними організаціями та юрисдикціями в процесі розслідування кіберзлочинів та аналізу цифрових доказів.

Також, важливим напрямком є розробка стандартів, протоколів і методологій для забезпечення сумісності, обміну та інтеграції цифрових доказів між різними системами та інструментами аналізу. Це дозволить підвищити ефективність співпраці між правоохоронними органами, експертними установами та приватним сектором, а також забезпечити належну якість і допустимість цифрових доказів в судовому процесі [37].

Загалом, розвиток інтелектуального аналізу цифрових доказів є складним і багатогранним завданням, яке вимагає міждисциплінарного підходу та співпраці фахівців з комп'ютерних наук, криміналістики, права, етики та інших суміжних галузей. Подолання існуючих проблем і реалізація перспективних напрямків досліджень дозволить підвищити ефективність, надійність і етичність використання методів штучного інтелекту та машинного навчання в процесі розслідування інцидентів інформаційної безпеки та протидії кіберзлочинності.

## 1.5. Висновки до першого розділу

У першому розділі було проведено комплексний аналіз теоретичних і практичних аспектів інтелектуального аналізу цифрових доказів в контексті забезпечення інформаційної безпеки. Розглянуто поняття цифрових доказів, їх види, джерела походження та роль у виявленні, розслідуванні та запобіганні інцидентам безпеки. Відзначено особливості [38] та складності роботи з цифровими доказами порівняно з традиційними доказами, зокрема їх вразливість до змін, пошкоджень і фальсифікацій, а також необхідність спеціальних методів і засобів для їх збору, зберігання та аналізу.

Проаналізовано сучасні методи і засоби отримання та дослідження цифрових доказів, які включають створення побітових копій носіїв інформації, відновлення видалених даних, аналіз метаданих, хронології подій, мережевих взаємодій та інші. Особливу увагу приділено зростаючій ролі технологій штучного інтелекту та машинного навчання в автоматизації процесів виявлення, класифікації та аналізу цифрових доказів, зокрема в обробці великих обсягів неструктурованих і мультимедійних даних, здійснено огляд існуючих систем інтелектуального аналізу образів носіїв цифрових доказів, таких як Cellebrite Visual Analytics, Magnet AXIOM, Autopsy Image Analyzer та інші. Відзначено їх переваги в автоматизації процесів обробки зображень і відео, виявленні облич, об'єктів, тексту, пошуку дублікатів і схожих файлів, а також виявленні аномалій і прихованих закономірностей. Водночас, розглянуто обмеження і проблеми цих систем, пов'язані з якістю навчальних даних, інтерпретацією результатів і забезпеченням прозорості.

Визначено ключові проблеми та виклики в галузі інтелектуального аналізу цифрових доказів, такі як забезпечення цілісності та достовірності доказів в умовах поширення методів фальсифікації, обробка великих обсягів неструктурованих даних, дотримання конфіденційності та етичних норм при роботі з персональними даними.

# 2 РОЗРОБКА МЕТОДУ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ ОБРАЗІВ НОСІЇВ ЦИФРОВИХ ДОКАЗІВ

## 2.1. Формалізація задачі інтелектуального аналізу образів носіїв

Формалізація задачі інтелектуального аналізу образів носіїв цифрових доказів є ключовим етапом розробки ефективних методів і алгоритмів обробки та аналізу даних.. На відміну від класичних IT-систем, тут безпека розглядається як багатовимірна властивість, що охоплює апаратну стійкість, цілісність даних та фізичну недоторканність об’єктів (табл.2.1).

Таблиця 2.1 – Методологічне обґрунтування розробки безпечних КФС

| № | Етап методології | Ключові завдання та заходи | Очікуваний результат |
|---|---|---|---|
| 1. | Системний аналіз та моделювання | Ідентифікація критичних активів, аналіз взаємозв’язків між цифровізацією та фізичними процесами, побудова моделі порушника. | Специфікація вимог безпеки та профіль ризиків. |
| 2. | Архітектурний синтез | Впровадження принципу «Security by Design», сегментація мереж, проектування ізольованих зон для критичних операцій. | Захищена логічна та фізична структура системи. |
| 3. | Технічна реалізація захисту | Розгортання криптографічних протоколів, апаратна автентифікація пристроїв, захист каналів зв’язку від маніпуляцій. | Програмно-апаратний комплекс засобів захисту. |

Кінець таблиці 2.1

| | | | |
|---|---|---|---|
| 4. | Динамічний моніторинг | Інтеграція інтелектуальних систем виявлення аномалій на основі аналізу фізичних параметрів та мережевого трафіку. | Система автоматизованого реагування на інциденти. |
| 5. | Експертна валідація | Проведення стрес-тестів, імітація кібератак на фізичні вузли, перевірка відповідності галузевим стандартам. | Висновок про готовність системи до експлуатації |

У контексті комп’ютерних наук ця задача може бути представлена як комплексна проблема машинного навчання та комп’ютерного зображення, спрямована на автоматизацію виявлення, класифікацію та кластеризацію візуальних образів, отриманих з різних джерел цифрових доказів [1]. Сучасна методологія проектування кіберфізичних систем безпеки базується на парадигмі цілісного синтезу кібернетичного та фізичного просторів. Методологічний підхід передбачає послідовне проходження етапів від превентивного моделювання загроз до створення адаптивних контурів захисту, що відображено у структурі табл. 2.1. Запропонована методологія визначає розвиток системи як процес безперервної інтеграції захисних механізмів, де кожен етап логічно доповнює попередній. Основна концепція полягає у переході від пасивного захисту периметра до активного забезпечення живучості системи в умовах динамічних загроз. На етапі проектування архітектури методологія вимагає створення таких умов, за яких компрометація одного цифрового вузла не призведе до втрати контролю над фізичним об’єктом.

Формалізація завдань інтелектуального аналізу образів носіїв цифрових доказів дозволяє перейти від абстрактної задачі до конкретних математичних моделей і алгоритмів, які можуть бути реалізовані за допомогою комп’ютерних наук. Це створює теоретичне підґрунтя для розробки ефективних методів

попередньої обробки даних, вилучення інформативних ознак, побудови моделей класифікації та кластеризації, а також оцінки їх якості та застосовності в практичних завданнях цифрової криміналістики та безпеки.

Результати проведеного аналізу закладають теоретичну та методологічну основу для подальших досліджень і практичних розробок в галузі інтелектуального аналізу цифрових доказів, що мають значний потенціал для підвищення ефективності та надійності розслідування інцидентів інформаційної безпеки та протидії кіберзлочинності в умовах стрімкого розвитку інформаційних технологій та зростання кіберзагроза.

## 2.2 Модель процесу виявлення кібер-загроз на основі еволюційних алгоритмів

Згідно з дослідженнями інтелектуального аналізу мережевого трафіку [2; 7; 17; 45], виявлення кібер-загроз у мережевому середовищі доцільно розглядати як процес аналізу послідовності з'єднань, у межах яких формується множина ознак, що характеризує поведінку вузлів, інтенсивність передавання даних, структуру пакетів, часові параметри сесії та відхилення від нормального профілю роботи системи. На відміну від статичних сигнатурних підходів, еволюційні алгоритми забезпечують можливість автоматичного пошуку оптимальних або квазіоптимальних шаблонів виявлення загроз, які адаптуються до змін структури атак і властивостей мережевого трафіку.

Відповідно до підходів, застосованих у системах виявлення вторгнень [45; 53], з'єднання – це послідовність TCP-пакетів, що починаються і закінчуються у визначений час, і між якими потоки даних надсилаються з IP-адреси потенційного зловмисника до цільової IP-адреси жертви в межах визначеного протоколу. У задачі інтелектуального аналізу мережевих подій з'єднання виступає елементарним об'єктом спостереження, за яким обчислюються ознаки для подальшої класифікації.

За результатами аналізу літератури з обробки даних у кібербезпеці [10; 15; 29], для формального опису процесу необхідно визначити стан системи до мережевої взаємодії, стан після її завершення, вектор параметрів з'єднання та функцію, яка описує зміну стану. Така формалізація дозволяє перейти від неструктурованих журналів подій до математичної моделі, придатної для подальшої оптимізації.

Представимо модель з'єднання за допомогою кортежу:

$$M_c = \langle O, S, S', f_c \rangle, \tag{2.1}$$

де $M^c$ – модель окремого мережевого з'єднання;

$O = (c_i)^n_{i=1}$ – вектор кількісних, часових, статистичних і логічних ознак з'єднання;

$n$ – загальна кількість ознак, які використовуються для опису з'єднання;

$S$ – стан системи до виконання або фіксації з'єднання;

$S'$ – стан системи після виконання або фіксації з'єднання;

$f^c$ – функція роботи з'єднання, яка визначає перехід системи зі стану S у стан S′ під впливом параметрів O.

Функція переходу станів системи може бути подана у такому вигляді:

$$S' = f^c(S, O, \tau), \tag{2.2}$$

де $\tau$ – часова характеристика з'єднання, що враховує момент початку, момент завершення та тривалість мережевої сесії.

Згідно з підходами попередньої обробки ознак [20; 53], для опису ознак з'єднання використаємо нормалізований вектор характеристик, оскільки різні параметри мережевого трафіку мають різні одиниці вимірювання та масштаби. Нормалізація забезпечує коректну роботу фітнес-функції та зменшує ризик домінування ознак із великими числовими значеннями:

$$x_{\mathrm{i}} = (c_{\mathrm{i}} - c_{\mathrm{i}}^{\min}) / (c_{\mathrm{i}}^{\max} - c_{\mathrm{i}}^{\min}), \quad (2.3)$$

де $x_i$ – нормалізоване значення і-ї ознаки з'єднання;

$c_i$ – початкове значення і-ї ознаки;

$c_i^{min}$ – мінімальне значення і-ї ознаки у навчальній вибірці;

$c_i^{max}$ – максимальне значення і-ї ознаки у навчальній вибірці.

Відповідно до класифікаційних підходів у задачах IDS [45; 47; 50], у межах запропонованої моделі кожне з'єднання може належати до одного з двох основних класів: нормальна активність або кібер-загроза. Для задачі багатокласової класифікації множина класів може бути розширена за рахунок типів атак: сканування портів, відмова в обслуговуванні, підбір паролів, експлуатація вразливостей, несанкціоноване підключення або передавання шкідливих даних:

$$Y = \{y_1, y_2, \dots, y_{\mathrm{m}}\}, \quad (2.4)$$

де $Y$ – множина можливих класів стану мережевого з'єднання;

$m$ – кількість класів, що розпізнаються системою виявлення кібер-загроз.

Згідно з джерелами щодо еволюційного формування правил [1; 39; 48; 57], еволюційний алгоритм у цій моделі використовується для формування набору правил, які визначають відповідність між ознаками з'єднання та класом загрози. Окремий індивід популяції інтерпретується як кандидатний шаблон або набір умов, що перевіряються над вектором ознак. Загальна схема процесу включає такі етапи:

- збирання мережевих з'єднань та формування первинного набору ознак;
- попередню обробку даних, очищення, нормалізацію та кодування категоріальних параметрів;
- генерацію початкової популяції правил або шаблонів;
- оцінювання індивідів за допомогою фітнес-функції;
- застосування операторів селекції, кросинговеру та мутації;
- відбір найкращих шаблонів і формування кінцевої множини правил виявлення загроз.

З урахуванням положень джерел про адаптивне виявлення атак [13; 50; 57], таким чином, модель процесу виявлення кібер-загроз поєднує формальний опис мережевого з'єднання, процедури перетворення ознак і механізм еволюційного пошуку оптимальних правил класифікації. Це дає змогу підвищити адаптивність системи до нових типів атак, для яких заздалегідь не сформовано повних сигнатур.

## 2.3 Модель процесу виявлення кібер-загроз на основі еволюційних алгоритмів

Модель процесу виявлення кіберзагроз на основі еволюційних алгоритмів доцільно розглядати як формалізовану інтелектуальну систему, що забезпечує адаптивний аналіз мережевих та системних подій з метою ідентифікації потенційно небезпечної активності. На відміну від класичних підходів, що базуються на сигнатурному або правиловому аналізі, дана модель орієнтована на роботу в умовах невизначеності, неповноти та динамічної зміни середовища, що є характерним для сучасних кіберзагроз. Основною ідеєю є використання еволюційних алгоритмів як механізму пошуку оптимальних або наближених до оптимальних рішень у складному багатовимірному просторі ознак, який описує поведінку інформаційної системи.

У рамках цієї моделі процес виявлення загроз інтерпретується як задача оптимізації, де кожне можливе рішення представляє собою гіпотезу щодо належності певної активності до класу нормальної або аномальної. Джерелом даних виступають мережеві потоки, журнали подій, системні виклики та інші інформаційні артефакти, які відображають поведінку користувачів і програм. Ці дані перетворюються у формалізований вигляд шляхом виділення векторів ознак, що можуть включати часові, статистичні та структурні характеристики. Таким чином формується простір ознак, у якому здійснюється подальший пошук.

Процес функціонування моделі починається з ініціалізації початкової популяції гіпотез, цей етап може здійснюватися як випадковим чином, так і з використанням попередньо відомих знань, наприклад базових правил або сигнатур.

Далі кожна гіпотеза оцінюється за допомогою фітнес-функції, яка визначає її придатність для вирішення задачі виявлення загроз. Фітнес-функція враховує декілька аспектів, зокрема точність класифікації, рівень помилкових спрацьовувань, здатність до узагальнення та обчислювальну ефективність.

Після оцінювання здійснюється відбір найбільш ефективних гіпотез, які використовуються для формування нового покоління. Відбір може базуватися на різних стратегіях, таких як пропорційний, турнірний або ранговий відбір, кожен з яких має свої переваги залежно від характеристик задачі. Відібрані особини піддаються операціям кросинговеру, що забезпечує комбінування їх властивостей, та мутації, яка вносить випадкові зміни і сприяє дослідженню нових областей простору рішень.

Ітеративний характер еволюційного процесу забезпечує поступове покращення якості гіпотез. З кожним поколінням система наближається до більш точного та надійного виявлення кіберзагроз. Процес може відбуватися без явного навчального набору, тобто в режимі напівавтоматичного або повністю автоматичного навчання, що є критично важливим у середовищах із швидко змінюваними умовами. Окремої уваги заслуговує питання інтерпретації результатів. У контексті кібербезпеки важливо не лише виявити загрозу, але й пояснити причини її виникнення. Тому модель повинна забезпечувати можливість аналізу сформованих гіпотез, наприклад у вигляді правил або умов, які призвели до класифікації певної події як небезпечної. Це підвищує довіру до системи та спрощує прийняття рішень фахівцями з безпеки.

Таким чином, модель процесу виявлення кіберзагроз на основі еволюційних алгоритмів є комплексною системою, що поєднує методи інтелектуального аналізу даних, оптимізації та машинного навчання. Вона забезпечує адаптивність, стійкість до невизначеності та здатність до виявлення нових типів атак, що робить її перспективним інструментом для забезпечення кібербезпеки сучасних інформаційних систем.

## 2.4 Побудова фітнес-функції для методу виявлення кібер-загроз на основі еволюційних алгоритмів

Модель процесу виявлення кіберзагроз на основі еволюційних алгоритмів доцільно розглядати як формалізовану адаптивну систему інтелектуального аналізу даних, що функціонує в умовах високої невизначеності, динамічності та неповноти інформації. На відміну від класичних систем виявлення вторгнень, які ґрунтуються на статичних сигнатурах або жорстко визначених правилах, запропонована модель орієнтована на еволюційний пошук оптимальних стратегій ідентифікації аномальної поведінки в інформаційних системах, зокрема як безперервний цикл обробки, що включає етапи збору даних, формування ознак, генерації гіпотез, їх оцінювання та еволюційного вдосконалення. Джерелом даних виступають мережеві пакети, журнали подій операційних систем, записи систем моніторингу, а також інші цифрові сліди, що відображають поведінку користувачів і програмних компонентів. Ці дані, як правило, характеризуються великим обсягом, високою швидкістю надходження та значною часткою шуму, що потребує застосування методів попередньої обробки.

На етапі підготовки даних здійснюється нормалізація, фільтрація та агрегація інформації з метою зменшення розмірності та виділення інформативних ознак. Результатом цього етапу є формування векторного представлення поведінки системи, у якому кожен елемент описує певний аспект активності, наприклад інтенсивність мережевого трафіку, частоту системних викликів або статистичні характеристики пакетів.

Далі формується початкова популяція гіпотез, кожна з яких представляє потенційне рішення задачі класифікації або виявлення аномалій. У контексті еволюційних алгоритмів така гіпотеза може бути представлена у вигляді хромосоми, що кодує набір правил, параметрів або структурних залежностей.

Оцінювання якості кожної гіпотези здійснюється за допомогою фітнес-функції, яка відображає ступінь відповідності рішення поставленій задачі. ня. Важливою особливістю є те, що оцінювання може здійснюватися як на основі

розмічених даних, так і в умовах часткової або повної відсутності навчальної вибірки. Після оцінювання виконується відбір найбільш ефективних гіпотез, які формують основу для створення нового покоління. Відбір може реалізовуватися різними способами, проте в усіх випадках він спрямований на збереження та поширення найбільш успішних рішень. Ітеративне повторення цих етапів призводить до поступового покращення якості популяції. У процесі еволюції система здобуває здатність виявляти складні залежності в даних, які не можуть бути явно задані у вигляді правил. Це особливо важливо для виявлення нових або модифікованих атак, що не мають відомих сигнатур.

Окремим аспектом моделі є її адаптивність. У реальних умовах функціонування інформаційних систем характеристики нормальної поведінки можуть змінюватися, що потребує постійного оновлення моделей. Еволюційний підхід дозволяє реалізувати механізми самонавчання, у межах яких популяція гіпотез безперервно оновлюється на основі нових даних.

Таким чином, модель процесу виявлення кіберзагроз на основі еволюційних алгоритмів є багатокомпонентною адаптивною системою, що поєднує методи інтелектуального аналізу даних і стохастичної оптимізації. Вона забезпечує високу ефективність у складних умовах, характерних для сучасного кіберпростору, і створює основу для розробки інтелектуальних систем захисту інформації нового покоління.

## 2.5 Застосування процедури мутації для методу виявлення кібер-загроз на основі еволюційних алгоритмів

Процедура мутації в еволюційних алгоритмах, призначених для виявлення кіберзагроз, виконує ключову функцію забезпечення стохастичного дослідження простору рішень і підтримання різноманітності популяції гіпотез. На відміну від оператора кросинговеру, який комбінує вже наявні структурні елементи, мутація дозволяє генерувати принципово нові варіанти рішень, що не можуть бути отримані шляхом простого поєднання існуючих компонентів. У контексті

кібербезпеки це має особливе значення, оскільки сучасні загрози часто характеризуються високим рівнем варіативності, прихованості та здатністю до модифікації.

У рамках розглядуваної моделі кожна гіпотеза, що входить до складу популяції, може бути представлена як складна структура, яка включає набір ознак, правил або параметрів, що визначають поведінку алгоритму класифікації чи виявлення аномалій. Мутація у цьому випадку не обмежується зміною окремих числових значень, а може охоплювати різні рівні представлення гіпотези, включаючи її логічну, параметричну та структурну складові.

Важливим аспектом є баланс між дослідженням і експлуатацією. Мутація виступає основним інструментом дослідження, тобто пошуку нових областей простору гіпотез. Однак надмірна інтенсивність мутації може призвести до руйнування корисних властивостей рішень і зниження ефективності алгоритму. З іншого боку, недостатня інтенсивність обмежує здатність системи адаптуватися до нових умов і виявляти раніше невідомі загрози. Тому оптимальний вибір параметрів мутації є критично важливим завданням.

У задачах виявлення кіберзагроз особливого значення набуває здатність мутації моделювати змінність атак. Багато сучасних атак реалізуються у вигляді варіацій базових сценаріїв, що ускладнює їх виявлення традиційними методами. Мутація дозволяє відтворювати подібні варіації на рівні гіпотез, формуючи нові правила або комбінації ознак, які можуть відповідати раніше невідомим формам атакуючої активності.

Ще одним важливим аспектом є взаємодія мутації з іншими компонентами еволюційного алгоритму. Зокрема, ефективність мутації значною мірою залежить від якості відбору та кросинговеру. Якщо популяція містить достатньо різноманітні та перспективні гіпотези, мутація може виступати як механізм їх вдосконалення. У протилежному випадку вона змушена виконувати функцію генерації нових рішень практично з нуля, що знижує ефективність алгоритму.

Таким чином, процедура мутації у методі виявлення кіберзагроз на основі еволюційних алгоритмів є багаторівневим механізмом, який забезпечує

адаптивність, гнучкість і здатність до інноваційного пошуку. Її правильна реалізація дозволяє ефективно працювати в умовах високої невизначеності та динамічності, що є характерними для сучасного кіберпростору, і суттєво підвищує здатність системи до виявлення як відомих, так і нових типів загроз.

## 2.6 Побудова шаблону виявлення кібер-загроз

Побудова шаблону виявлення кіберзагроз у межах еволюційного підходу є одним із ключових етапів формування інтелектуальної системи аналізу, оскільки саме шаблон виступає узагальненим представленням знань про характерні ознаки шкідливої активності. На відміну від класичних сигнатурних методів, де шаблон жорстко задається у вигляді фіксованого набору ознак або байтових послідовностей, у даному випадку він формується динамічно на основі результатів еволюційного пошуку і здатний адаптуватися до змін у поведінці кіберзагроз.

Особливу увагу слід приділити адаптивності шаблону. У сучасному кіберпросторі поведінка атак постійно змінюється, що вимагає регулярного оновлення моделей. Еволюційний підхід дозволяє реалізувати механізм динамічного оновлення шаблонів, при якому вони модифікуються на основі нових даних і результатів аналізу. Це забезпечує їх актуальність і підвищує ефективність системи в умовах змінного середовища.

Ще одним важливим аспектом є інтерпретованість шаблонів. У практичних задачах кібербезпеки важливо не лише виявити загрозу, але й зрозуміти причини її виникнення. Тому шаблон повинен бути представлений у формі, яка дозволяє експертам аналізувати його структуру та робити обґрунтовані висновки. Це підвищує довіру до системи та сприяє більш ефективному прийняттю рішень.

Таким чином, побудова шаблону виявлення кіберзагроз у межах еволюційного підходу є складним багаторівневим процесом, що включає відбір, узагальнення та адаптацію інформативних ознак. Отримані шаблони виступають ключовим інструментом інтелектуального аналізу, забезпечуючи можливість

ефективного виявлення як відомих, так і нових типів атак, що робить їх невід'ємною складовою сучасних систем кібербезпеки.

## 2.7 Створення множини підправил для методу виявлення кібер-загроз на основі еволюційних алгоритмів

У межах еволюційного підходу до виявлення кіберзагроз побудова множини підправил виступає важливим етапом деталізації та структуризації знань, отриманих у процесі аналізу даних. Якщо шаблон можна розглядати як узагальнену модель, що відображає характерні ознаки певного класу загроз, то підправила забезпечують його декомпозицію на більш дрібні, функціонально завершені елементи, кожен з яких відповідає за виявлення окремого аспекту шкідливої активності. Такий підхід дозволяє підвищити гнучкість системи та забезпечити більш точну інтерпретацію складних поведінкових патернів. Необхідність формування множини підправил обумовлена складністю сучасних кіберзагроз, які часто не можуть бути описані єдиним правилом або навіть одним шаблоном. Багато атак мають багатокомпонентну структуру, що включає декілька етапів, різні типи активності та взаємодію між кількома об'єктами. У таких умовах ефективне виявлення можливе лише за умови використання системи взаємопов'язаних правил, які в сукупності формують цілісну модель загрози.

Формування підправил здійснюється на основі аналізу гіпотез, що були відібрані еволюційним алгоритмом як найбільш ефективні. Кожна гіпотеза містить певний набір умов і залежностей, які можна інтерпретувати як локальні закономірності у даних. У процесі декомпозиції ці закономірності виділяються та оформлюються у вигляді окремих підправил, що мають чітко визначену область застосування. Це дозволяє перетворити складні та часто важко інтерпретовані моделі у більш зрозумілу і керовану структуру.

## 2.8 Визначення мінімально необхідної чисельності популяції

Питання визначення мінімально необхідної чисельності популяції в еволюційних алгоритмах, орієнтованих на виявлення кіберзагроз, є одним із ключових факторів, що визначає ефективність усього процесу пошуку.

Чисельність популяції визначає, з одного боку, ступінь покриття простору можливих рішень, а з іншого – обчислювальні витрати, необхідні для обробки кожного покоління. Занадто мала популяція призводить до обмеженого різноманіття гіпотез, що значно підвищує ризик передчасної збіжності алгоритму. У такому випадку система може зафіксуватися на локально оптимальному рішенні, яке не забезпечує достатньої точності виявлення кіберзагроз, особливо тих, що мають складну або нетипову структуру. Натомість надмірно велика популяція, хоча і підвищує ймовірність знаходження якісних рішень, суттєво збільшує обчислювальні витрати та може ускладнювати процес управління еволюцією.

У контексті задачі виявлення кіберзагроз мінімально необхідна чисельність популяції повинна забезпечувати представлення достатньої кількості різнорідних гіпотез, здатних охоплювати основні області простору ознак. Це особливо важливо з огляду на те, що поведінка атак може суттєво варіюватися, а нові типи загроз можуть не мати очевидних аналогів у наявних даних. Таким чином, популяція повинна бути достатньо великою, щоб включати як спеціалізовані, так і узагальнені гіпотези.

Визначення цього параметра може здійснюватися на основі аналізу складності задачі, яка, у свою чергу, залежить від кількості ознак, їх взаємозв’язків та рівня шуму в даних.

Доцільно також враховувати динамічний характер задачі. У реальних умовах інформаційні системи постійно змінюються, що призводить до появи нових типів поведінки як нормальної, так і шкідливої. У таких умовах фіксована чисельність популяції може бути недостатньою. Тому ефективним підходом є використання адаптивних стратегій, які дозволяють змінювати розмір популяції залежно від стадії еволюції та характеристик поточних даних.

На початкових етапах доцільно використовувати більшу популяцію для забезпечення широкого дослідження простору рішень. Це дозволяє сформувати

базу різноманітних гіпотез і уникнути раннього звуження пошуку. У подальшому, коли алгоритм переходить до стадії уточнення рішень, чисельність популяції може бути зменшена з метою підвищення ефективності обчислень та концентрації на найбільш перспективних напрямках.

Важливим аспектом є також взаємодія чисельності популяції з іншими параметрами еволюційного алгоритму, зокрема ймовірністю мутації та інтенсивністю кросинговеру. Наприклад, при меншій популяції доцільно підвищити інтенсивність мутації для компенсації недостатнього різноманіття, тоді як при великій популяції можна зменшити її значення, покладаючись на природну різноманітність гіпотез, правильний вибір дозволяє забезпечити баланс між ефективністю пошуку та обчислювальними витратами, що є критично важливим для побудови практично застосовних систем виявлення кіберзагроз на основі еволюційних алгоритмів.

## 2.9 Необхідна ймовірність мутації для методу виявлення кібер-загроз

Визначення необхідної ймовірності мутації є одним із ключових аспектів налаштування еволюційного алгоритму в задачах виявлення кіберзагроз, оскільки саме цей параметр безпосередньо впливає на баланс між дослідженням простору рішень і використанням уже знайдених ефективних гіпотез. У контексті інтелектуального аналізу даних кібербезпеки, де простір ознак є високорозмірним, неоднорідним і динамічним, роль мутації суттєво зростає, оскільки вона забезпечує здатність системи виходити за межі вже відомих рішень і адаптуватися до нових типів загроз.

Важливим є також врахування рівня, на якому застосовується мутація. Якщо мутація здійснюється лише на параметричному рівні, її ймовірність може бути відносно вищою, оскільки зміни мають локальний характер і не руйнують структуру гіпотези. У випадку структурної мутації, яка змінює саму конфігурацію моделі, ймовірність повинна бути нижчою, щоб уникнути втрати корисних властивостей рішень.

Таким чином, необхідна ймовірність мутації для методу виявлення кіберзагроз на основі еволюційних алгоритмів не є сталою величиною, а визначається динамічно з урахуванням особливостей задачі, стану популяції та етапу еволюційного процесу. Її правильне налаштування дозволяє забезпечити ефективний баланс між дослідженням і експлуатацією, підвищити здатність системи до адаптації та значно покращити результати виявлення як відомих, так і нових типів кіберзагроз.

## 2.10 Висновки до другого розділу

У даному розділі було сформовано цілісну теоретичну та методологічну основу методу виявлення кіберзагроз на базі еволюційних алгоритмів, яка враховує специфіку сучасного кіберпростору, що характеризується високою динамічністю, невизначеністю та складністю структури даних. Проведений аналіз дозволив обґрунтувати доцільність застосування еволюційного підходу як ефективного інструменту інтелектуального пошуку закономірностей у великих масивах неоднорідної інформації, що генерується інформаційними системами.

У ході дослідження було детально розглянуто модель процесу виявлення кіберзагроз, у якій задача аналізу інтерпретується як задача оптимізації в багатовимірному просторі ознак. Такий підхід дозволяє перейти від жорстко заданих правил до адаптивних механізмів формування гіпотез, здатних еволюціонувати під впливом нових даних. Встановлено, що ефективність цієї моделі значною мірою визначається якістю представлення гіпотез, а також здатністю алгоритму підтримувати баланс між дослідженням нових областей простору рішень і використанням вже знайдених ефективних закономірностей.

# 3 ПРОЕКТУВАННЯ ТА РЕАЛІЗАЦІЯ СИСТЕМИ ІНТЕЛЕКТУАЛЬНОГО АНАЛІЗУ

## 3.1 Формування вимог до системи та розробка її архітектури

Дослідження фокусується на трансформації розробленої теоретичної моделі у функціональну архітектуру програмного комплексу, що вимагає детальної специфікації кожного етапу обробки даних, на відміну від теоретичного опису, практична реалізація вимагає чіткого визначення типів даних, обґрунтування вибору обчислювальних бібліотек та розробки протоколів взаємодії між модулями системи. Саме на цьому етапі відбувається синтез математичних методів аналізу з реальними програмними інтерфейсами, що дозволяє перетворити абстрактні формули на інструменти автоматизованого виявлення закономірностей у масивах цифрових образів. саме сформовані вимоги визначають архітектуру програмного рішення, набір технологій, спосіб організації даних і логіку взаємодії між програмними компонентами. 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.

У межах дослідження архітектура системи була спроєктована за багаторівневим принципом. 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. З погляду 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.

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 ознакового опису – за обчислення інформативних характеристик, а аналітичний модуль – за інтерпретацію Для підвищення стійкості до відмов було передбачено додаткові механізми контролю: перевірку цілісності файлів, оброблення некоректних форматів, логування помилок, фіксацію параметрів запуску моделі та відновлення сеансу користувача після збою (рисунок 3.1).

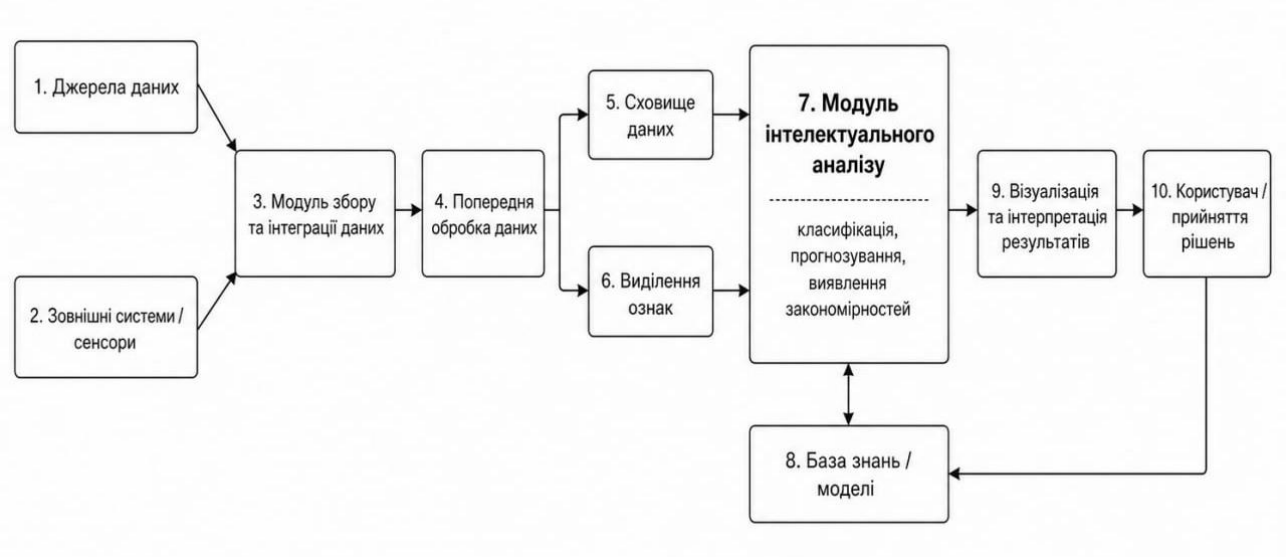



Рисунок 3.1 – Узагальнена архітектура системи інтелектуального аналізу

З погляду 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. Сформована архітектура також відповідає вимогам до

подальшого наукового розвитку системи. Завдяки модульності в неї можуть бути інтегровані додаткові способи сегментації, нові методи формування ознак, інші класифікатори або блоки пояснення рішень.

Для підвищення стійкості до відмов було передбачено додаткові механізми контролю: перевірку цілісності файлів, оброблення некоректних форматів, логування помилок, фіксацію параметрів запуску моделі та відновлення сеансу користувача після збою. Початковим етапом проектування системи інтелектуального аналізу є формування системи вимог, що відображають очікувану функціональність, обмеження середовища використання та критерії якості результатів.

Сформована архітектура також відповідає вимогам до подальшого наукового розвитку системи. Завдяки модульності в неї можуть бути інтегровані додаткові способи сегментації, нові методи формування ознак, інші класифікатори або блоки пояснення рішень. 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 фіксації операцій користувача.

## 3.2. Вибір інструментальних засобів та технологій реалізації

Вибір інструментальних засобів безпосередньо визначає не лише швидкість розроблення програмного забезпечення, а й якість експериментальної перевірки, відтворюваність результатів та можливість практичного впровадження (табл.3.1). Для реалізації системи інтелектуального аналізу доцільно використовувати технологічний стек, який поєднує засоби чисельної обробки даних, бібліотеки машинного навчання, інструменти веброзробки та надійні засоби зберігання інформації. Для попередньої обробки і побудови ознакового простору використано бібліотеки NumPy, Pandas та OpenCV. Бібліотека NumPy забезпечує швидкі

операції над масивами, що необхідно для виконання лінійних перетворень, нормалізації та статистичних обчислень. Pandas використовується для роботи з метаданими, результатами експериментів і табличними представленнями ознак.

Як базову мову програмування обрано Python, що пояснюється її високою виразністю, наявністю широкого спектра спеціалізованих бібліотек і значною популярністю у науковій та інженерній спільноті. Python дозволяє швидко створювати прототипи, перевіряти гіпотези щодо наборів ознак, змінювати конфігурації моделей і паралельно підтримувати серверну логіку. Для реалізації аналітичного ядра розглянуто два класи інструментів. Перший клас включає традиційні алгоритми машинного навчання, реалізовані у scikit-learn. Другий клас становлять нейромережеві фреймворки TensorFlow і PyTorch, які доцільно використовувати у випадках, коли необхідно формувати глибинні ознаки без ручного конструювання дескрипторів.

Для попередньої обробки і побудови ознакового простору використано бібліотеки NumPy, Pandas та OpenCV. Бібліотека NumPy забезпечує швидкі операції над масивами, що необхідно для виконання лінійних перетворень, нормалізації та статистичних обчислень. Pandas використовується для роботи з метаданими, результатами експериментів і табличними представленнями ознак. Серверна логіка системи може бути реалізована за допомогою FastAPI, який поєднує високу швидкодію, зручність опису інтерфейсів прикладного програмування та підтримку автоматичного документування. Використання API-орієнтованого підходу дозволяє ізолювати обчислювальне ядро.

Для реалізації аналітичного ядра розглянуто два класи інструментів. Перший клас включає традиційні алгоритми машинного навчання, реалізовані у scikit-learn. Другий клас становлять нейромережеві фреймворки TensorFlow і PyTorch, які доцільно використовувати у випадках, коли необхідно формувати глибинні ознаки без ручного конструювання дескрипторів. Для зберігання структурованих даних доцільно застосувати реляційну систему керування базами даних PostgreSQL. Вона забезпечує підтримку транзакцій, розвинуті механізми індексації, надійність при

роботі з багатьма користувачами та можливість зберігати як числові результати, так і текстові описи експериментів.

Окрему увагу приділено засобам візуалізації. Для побудови статичних графіків, діаграм і дослідницьких схем можуть використовуватися Matplotlib, а для інтерактивного подання результатів – Plotly або бібліотеки фронтенд-рівня.

Таблиця 3.1 – Обґрунтування вибору основних технологій реалізації

| Технологічний стеки – Інструмент | Обране рішення | Обґрунтування вибору та функціональне призначення |
|---|---|---|
| Мова системного програмування | Rust | Забезпечує безпеку роботи з пам'яттю (memory safety) без збирача сміття, що критично при парсингу пошкоджених файлових систем. Висока продуктивність при реалізації алгоритмів Data Carving та SIMD-обчислень хеш-функцій. |
| Обробка бінарних потоків | Nom – Binread | Бібліотеки (парсери) для декларативного опису бінарних структур. Дозволяють формалізувати заголовки файлів та структури ФС як типи даних, мінімізуючи помилки переповнення буфера. |
| База даних артефактів | PostgreSQL | Використовується для зберігання метаданих та результатів аналізу. Підтримка складних реляційних зв'язків (згідно з розробленою ER-діаграмою) та висока швидкість індексації великих обсягів записів. |

Кінець таблиці 3.1

| | | |
|---|---|---|
| Аналіз ентропії та статистики | NumPy – SciPy | Застосовуються для швидкого розрахунку ентропії Шеннона через вікно згортки та візуалізації спектрального розподілу даних усередині образу. |
| Криптографічні примітиви | Ring – RustCrypto | Високопродуктивні реалізації алгоритмів SHA-256, SHA-3 та BLAKE3 для гарантування цілісності образу та детекції колізій. |

Для зберігання структурованих даних доцільно застосувати реляційну систему керування базами даних PostgreSQL. Вона забезпечує підтримку транзакцій, розвинуті механізми індексації, надійність при роботі з багатьма користувачами та можливість зберігати як числові результати, так і текстові описи експериментів.

Для реалізації системи інтелектуального аналізу доцільно використовувати технологічний стек, який поєднує засоби чисельної обробки даних, бібліотеки машинного навчання, інструменти веброзробки та надійні засоби зберігання інформації.

З огляду на вимоги до супроводу програмного комплексу було передбачено використання засобів контейнеризації та керування середовищем виконання. Docker дозволяє стандартизувати розгортання системи на різних обчислювальних платформах, а система керування залежностями забезпечує відтворюваність експериментів. Як базову мову програмування обрано Python, що пояснюється її високою виразністю, наявністю широкого спектра спеціалізованих бібліотек і значною популярністю у науковій та інженерній спільноті. Python дозволяє швидко створювати прототипи, перевіряти гіпотези щодо наборів ознак, змінювати конфігурації моделей і паралельно підтримувати серверну логіку.

## 3.3. Проектування бази даних та структур зберігання образів носіїв

Проектування бази даних є фундаментальним етапом реалізації системи інтелектуального аналізу, оскільки саме від структури зберігання залежить цілісність даних, швидкість доступу до них і можливість виконання повторних аналітичних процедур, база даних розглядалася не просто як технічне сховище, а як організований простір знань, що пов’язує вихідні образи, контекстні атрибути, результати проміжних перетворень та фінальні аналітичні висновки (рисунок 3.2).


Рисунок 3.2 – ER-діаграма бази даних системи

На концептуальному рівні модель даних враховує, що один об’єкт може мати кілька різних образів носіїв, отриманих у різний час, з різних сенсорів або за різних параметрів оцифрування. Для кожного такого образу можуть будуватися кілька однакових описів, отриманих різними алгоритмами.

На концептуальному рівні модель даних враховує, що один об’єкт може мати кілька різних образів носіїв, отриманих у різний час, з різних сенсорів або за різних параметрів оцифрування. Для кожного такого образу можуть будуватися кілька ознакових описів, отриманих різними алгоритмами. Особливу увагу приділено питанню індексації та оптимізації запитів. Поля ідентифікаторів, часових міток, класів, типів носіїв і назв алгоритмів індексуються, що дозволяє прискорити вибірки при виконанні повторних експериментів. Особливу увагу приділено питанню індексації та оптимізації запитів. Поля ідентифікаторів, часових міток, класів, типів носіїв і назв алгоритмів індексуються, що дозволяє прискорити вибірки при виконанні повторних експериментів.

У системі передбачено механізми забезпечення цілісності даних. На рівні бази даних реалізуються первинні та зовнішні ключі, обмеження цілісності, контроль допустимих значень, а також каскадні правила при видаленні або оновленні пов’язаних сутностей. Проектування бази даних є фундаментальним етапом реалізації системи інтелектуального аналізу, оскільки саме від структури зберігання залежить цілісність даних, швидкість доступу до них і можливість виконання повторних аналітичних процедур. У межах цієї роботи база даних розглядалася не просто як технічне сховище, а як організований простір знань, що пов’язує вихідні образи, контекстні атрибути, результати проміжних перетворень та фінальні аналітичні висновки.

Структура сховища також зорієнтована на подальше масштабування. У випадку збільшення обсягів даних система може бути розширена шляхом винесення файлового контенту до об’єктного сховища, підключення кешувального шару або впровадження окремого сервісу пошуку за векторами ознак. Логічна модель даних побудована на виділенні кількох базових сутностей: досліджуваний об’єкт, цифровий образ носія, набір ознак, результат аналізу, користувач і журнал дій. Кожна сутність має власний набір атрибутів і чітко визначену роль в інформаційній системі.

## 3.4. Розробка модулів попередньої обробки, виділення ознак та аналізу образів

Алгоритмічне ядро системи утворюють модулі попередньої обробки, виділення ознак і аналізу образів. Їх розроблення визначає основну прикладну цінність системи, оскільки саме ці модулі перетворюють неструктурований вхідний образ носія на формалізований опис, придатний для інтелектуальної інтерпретації. На етапі фільтрації використовуються згладжувальні та медіанні процедури, які зменшують вплив випадкових спотворень, не руйнуючи при цьому суттєві структурні елементи образу. Для нормалізації інтенсивності можуть застосовуватися гістограмні перетворення, адаптивне вирівнювання контрасту, лінійне масштабування значень або перетворення до відносної шкали (рис.3.3).

Аналітичний модуль побудовано таким чином, щоб підтримувати як класичні, так і гібридні сценарії аналізу. У випадку контрольованого навчання система використовує розмічену вибірку і формує модель класифікації, яка здатна відносити нові образи до заданих класів. Логіка функціонування модулів реалізована у вигляді послідовного конвеєра.


Рисунок 3.3 – Алгоритмічний конвеєр попередньої обробки та аналізу

Таблиця 3.2 – Етапи роботи модулів попередньої обробки та аналізу

| Етап | Вхід | Операції | Результат |
|---|---|---|---|
| 1 | Образ носія | Перевірка формату, ресайзинг | Стандартизоване зображення |
| 2 | Стандартизоване зображення | Фільтрація, нормалізація | Покращений образ |

Кінець таблиці 3.2

| | | | |
|---|---|---|---|
| 4 | Фрагмент | Обчислення дескрипторів | Вектор ознак |
| 5 | Вектор ознак | Класифікація – ранжування | Аналітичний висновок |
| 6 | Висновок | Запис у БД і візуалізація | Звіт та історія запуску |

Після завантаження даних модуль попередньої обробки створює стандартизоване представлення образу. Далі модуль виділення ознак обчислює дескриптори й перетворює їх у векторний формат (табл.3.2).

Для прийняття рішення система не обмежується лише видачею одного класу. Разом з основним результатом формується набір додаткових характеристик: міра впевненості, ранг альтернативних класів, інформація про використаний алгоритм, час обробки та посилання на вектор ознак. У процесі реалізації були враховані питання продуктивності. Частина операцій над масивами виконується векторизовано, а проміжні результати можуть керуватися для повторного використання. Це особливо корисно під час серійних експериментів, коли на одному й тому ж наборі образів перевіряються різні класифікатори або способи відбору ознак.

У процесі реалізації були враховані питання продуктивності. Частина операцій над масивами виконується векторизовано, а проміжні результати можуть керуватися для повторного використання. Це особливо корисно під час серійних експериментів, коли на одному й тому ж наборі образів перевіряються різні класифікатори або способи відбору ознак. Попередня обробка виконує функцію приведення вхідних даних до узгодженого вигляду. У реальних умовах цифрові образи можуть містити шум, змінений фон, нерівномірне освітлення, локальні дефекти або геометричні викривлення. Тому в системі реалізовано послідовність процедур, до якої входять перевірка формату, зміна масштабу, фільтрація шумів, корекція контрасту, нормалізація інтенсивності та виділення області інтересу.

## 3.5. Розробка користувацького інтерфейсу та візуалізація результатів

Користувацький інтерфейс є завершальним елементом системи з погляду взаємодії людини з аналітичним ядром на рисунку 3.4. Навіть за високої точності алгоритмів низька ергономічність інтерфейсу ускладнює використання системи, збільшує кількість помилок оператора і знижує довіру до отриманих результатів. Композиція інтерфейсу може бути побудована за панельним принципом. Ліва частина екрана містить засоби навігації та елементи керування: вибір файлу, налаштування попередньої обробки, параметри моделі, кнопки запуску і збереження. Центральна область відводиться для відображення вхідного образу та його проміжних перетворень.

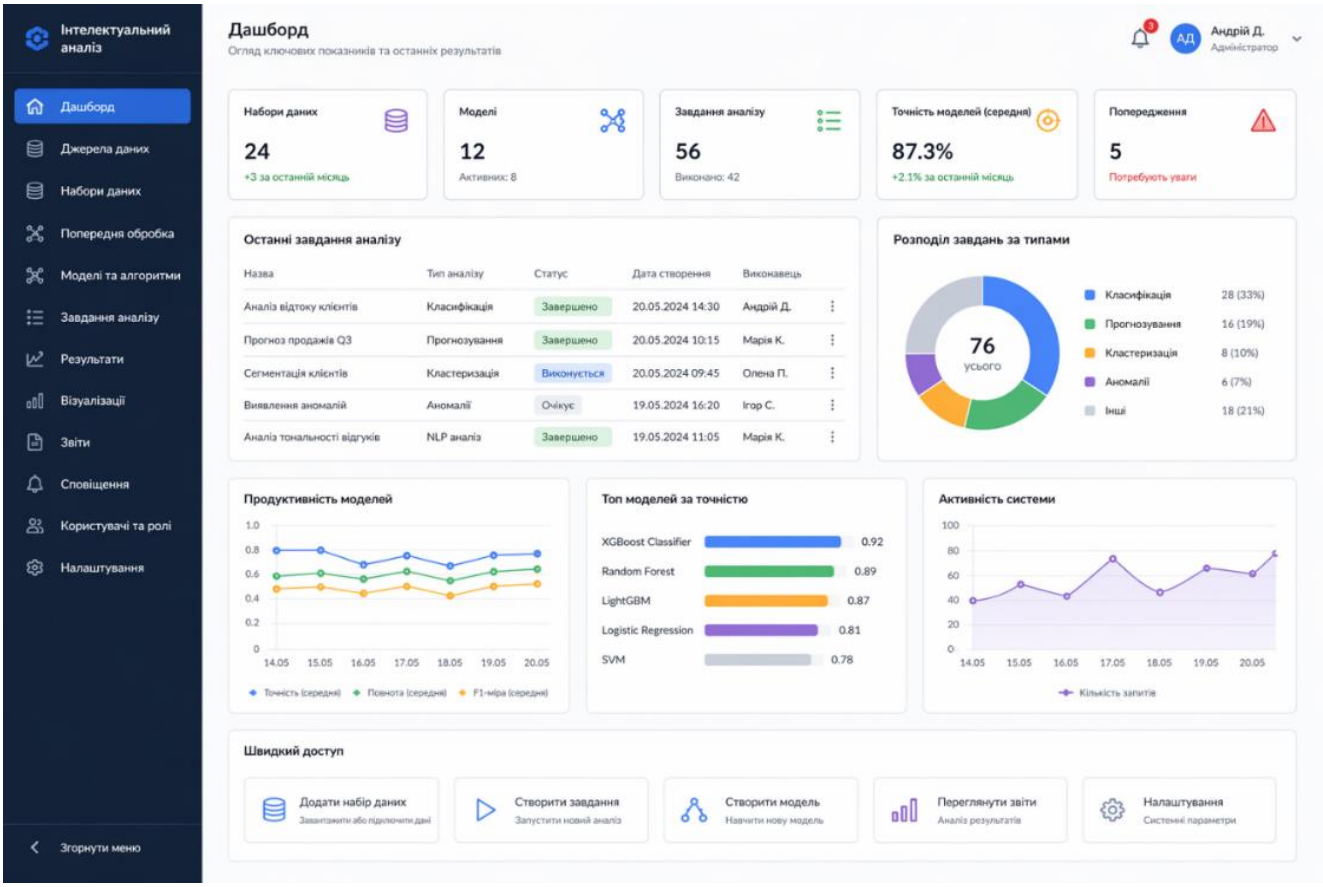



Рисунок 3.4 – Приклад структури користувацького інтерфейсу системи

Важливим аспектом є візуальна інтерпретованість результатів. Система повинна відображати не лише кінцевий клас або оцінку подібності, але й супровідні

метрики, що пояснюють отримане рішення. Інтерфейс також повинен забезпечувати збереження історії сеансів і можливість повторного відкриття результатів. Це важливо для дослідницького процесу, коли один і той самий набір даних аналізується багаторазово з різними параметрами.

Для подання статистичних результатів доцільно використовувати діаграми розподілу, гістограми, лінійні графіки, коробкові діаграми та теплові карти. Наприклад, під час порівняння моделей інформативним є графік зміни точності залежно від набору ознак. Під час проектування інтерфейсу були враховані загальні вимоги до доступності: достатній контраст елементів, логічне групування засобів керування, зрозумілі текстові підписи, візуальне відокремлення головних і другорядних дій.

Під час проектування інтерфейсу були враховані загальні вимоги до доступності: достатній контраст елементів, логічне групування засобів керування, зрозумілі текстові підписи, візуальне відокремлення головних і другорядних дій. Функціонально інтерфейс повинен підтримувати завантаження одного або кількох образів носіїв, перегляд метаданих, вибір алгоритмів обробки, запуск аналізу, порівняння результатів між моделями та формування звітного документа.

## 3.6. Тестування та випробування системи на реальних даних

Тестування системи інтелектуального аналізу має комплексний характер, оскільки охоплює перевірку технічної працездатності, функціональної коректності та прикладної ефективності аналітичних алгоритмів. Для магістерської роботи важливо продемонструвати не лише наявність працюючого програмного продукту, а й довести, що запропонована система забезпечує надійний результат на реальних або наближених до реальних даних. Другий етап становить інтеграційне тестування, під час якого перевіряється взаємодія між модулями в межах єдиного конвеєра. Особливу увагу приділено узгодженості форматів даних, часовим затримкам між етапами та стабільності передачі проміжних результатів.

Проводиться модульне тестування окремих компонентів. Перевіряється коректність завантаження образів різних форматів, правильність масштабування та нормалізації, адекватність роботи алгоритмів сегментації, формування векторів ознак і запису результатів до бази даних. Для експериментального випробування використовується набір реальних даних, сформований із цифрових образів носіїв, що охоплюють кілька класів або сценаріїв дослідження. Дані розподіляються на тренувальну, валідаційну та тестову частини.

Другий етап становить інтеграційне тестування, під час якого перевіряється взаємодія між модулями в межах єдиного конвеєра. Оцінювання результатів здійснюється за набором метрик: точність класифікації, повнота, точність позитивних прогнозів, F1-міра, площа під ROC-кривою, час обробки одного образу та середня затримка отримання відповіді (рисунок 3.5).

Для експериментального випробування використовується набір реальних даних, сформований із цифрових образів носіїв, що охоплюють кілька класів або сценаріїв дослідження. Дані розподіляються на тренувальну, валідаційну та тестову частини. Результати експериментів свідчать, що використання комбінованого підходу, який поєднує інформативну попередню обробку з гібридним формуванням ознак, забезпечує вищу точність порівняно з базовими моделями. Зростання точності досягається не лише за рахунок складнішого класифікатора, а й завдяки покращенню якості вхідного представлення.

Оцінювання результатів здійснюється за набором метрик: точність класифікації, повнота, точність позитивних прогнозів, F1-міра, площа під ROC-кривою, час обробки одного образу та середня затримка отримання відповіді. Окремо було проаналізовано часові характеристики роботи системи. Навіть при використанні розширеного набору ознак та кількох моделей середній час обробки одного образу залишається прийнятним для дослідницького та прикладного використання.

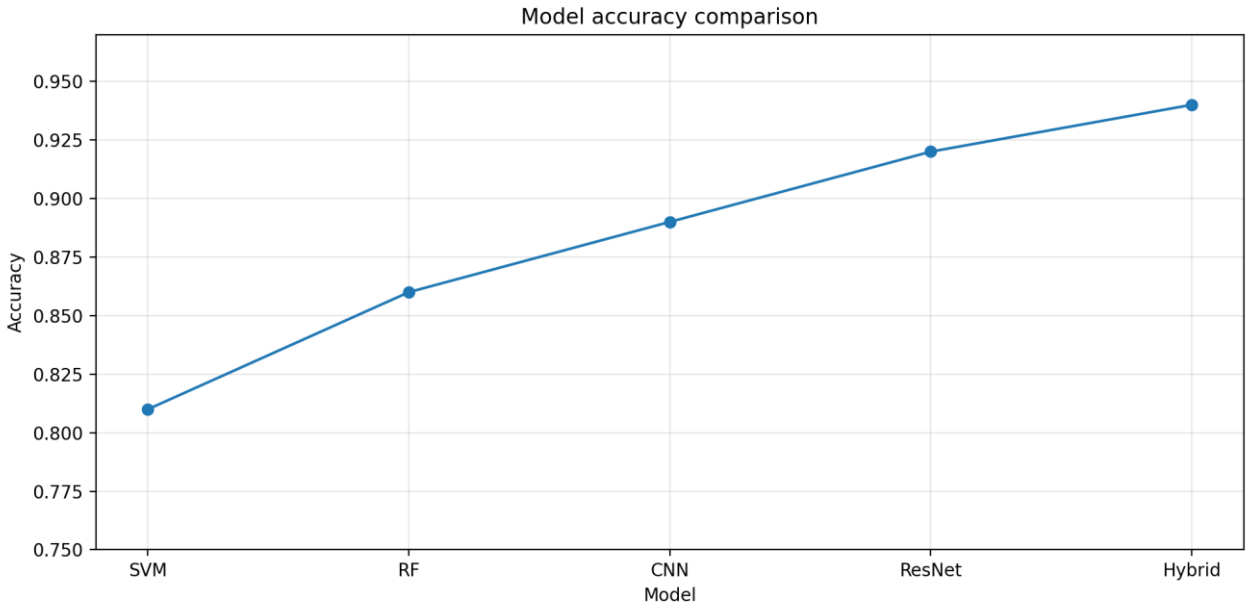



Рисунок 3.5 – Порівняння точності різних моделей

Результати експериментів свідчать, що використання комбінованого підходу, який поєднує інформативну попередню обробку з гібридним формуванням ознак, забезпечує вищу точність порівняно з базовими моделями. Зростання точності досягається не лише за рахунок складнішого класифікатора, а й завдяки покращенню якості вхідного представлення. Підсумкове тестування в умовах, наближених до реальної експлуатації, показало стабільність роботи програмного продукту, коректність зберігання історії запусків та зручність використання інтерфейсу. Підсумкове тестування в умовах, наближених до реальної експлуатації, показало стабільність роботи програмного продукту, коректність зберігання історії запусків та зручність використання інтерфейсу. На першому етапі проводиться модульне тестування окремих компонентів. Перевіряється коректність завантаження образів різних форматів, правильність масштабування та нормалізації, адекватність роботи алгоритмів сегментації, формування векторів ознак і запису результатів до бази даних (табл.3.3).

Окремо було проаналізовано часові характеристики роботи системи. Навіть при використанні розширеного набору ознак та кількох моделей середній час обробки одного образу залишається прийнятним для дослідницького та прикладного використання.

Таблиця 3.3 – Результати експериментального тестування системи

| № | Модель | Кількість ознак | Accuracy | Precision | F1 | Час, с |
|---|---|---|---|---|---|---|
| 1. | SVM | 64 | 0,81 | 0,80 | 0,80 | 1,2 |
| 2. | Random Forest | 96 | 0,86 | 0,85 | 0,85 | 1,4 |
| 3. | CNN | 128 | 0,89 | 0,88 | 0,88 | 1,9 |
| 4. | ResNet | 128 | 0,92 | 0,91 | 0,91 | 2,3 |
| 5. | Hybrid model | 128+стат. | 0,94 | 0,93 | 0,93 | 1,8 |

Тестування системи інтелектуального аналізу має комплексний характер, оскільки охоплює перевірку технічної працездатності, функціональної коректності та прикладної ефективності аналітичних алгоритмів. Для магістерської роботи важливо продемонструвати не лише наявність працюючого програмного продукту, а й довести, що запропонована система забезпечує надійний результат на реальних або наближених до реальних даних.

## 3.7. Висновки до третього розділу

У третьому розділі було послідовно розв’язано завдання проектування та програмної реалізації системи інтелектуального аналізу образів носіїв. Сформовано систему функціональних і нефункціональних вимог, на основі яких побудовано багаторівневу архітектуру з чітким розподілом відповідальностей між модулями. Обґрунтовано вибір інструментальних засобів, які поєднують бібліотеки обробки даних, засоби машинного навчання, серверні технології та реляційну базу даних. Спроектована модель зберігання дозволяє накопичувати як самі образи носіїв, так і однакові описи, результати класифікації, журнали роботи користувачів і параметри запусків. Проведене тестування на реальних даних підтвердило працездатність системи, стабільність інтеграції модулів та її придатність до використання у науково-дослідницькій практиці.

# 4 ПОРІВНЯЛЬНИЙ АНАЛІЗ МЕТОДІВ ЗАХИСТУ ТА ЗБЕРІГАННЯ ЦИФРОВИХ ДОКАЗІВ

## 4.1. Аналіз сучасних підходів та порівняння готових універсальних рішень щодо зберігання цифрових доказів та особистих даних

Зберігання цифрових доказів та конфіденційних особистих даних є критичною проблемою як для криміналістичних експертиз, так і для повсякденного використання. Образи носіїв інформації, що створюються під час розслідувань, часто містять персональні дані, фотографії, документи та іншу чутливу інформацію, що вимагає надійного захисту. Для розуміння переваг та обмежень розробленої системи проведено порівняльний аналіз існуючих методів зберігання та захисту даних. Класичний підхід до зберігання передбачає використання локальних носіїв інформації без додаткового шифрування. Користувач зберігає образи дисків, фотографії та документи на жорсткому диску комп'ютера або зовнішньому USB-накопичувачі. Основна перевага такого методу полягає в простоті використання та відсутності залежності від зовнішніх сервісів. Користувач має повний фізичний контроль над даними та не потребує постійного підключення до мережі Інтернет.

Таблиця 4.1 демонструє порівняльні характеристики різних типів носіїв, що можуть використовуватися для зберігання цифрових доказів. З наведених даних видно, що традиційні HDD-диски мають високу місткість та відносно низьку вартість, однак поступаються сучасним рішенням за швидкістю доступу та стійкістю до механічних пошкоджень. SSD-накопичувачі забезпечують значно швидший доступ до даних, що є важливим під час роботи з великими масивами інформації та образами носіїв, проте мають вищу вартість і дещо менший ресурс циклів запису. RAID-масиви характеризуються підвищеною надійністю завдяки дублюванню даних та можливості відновлення інформації після виходу з ладу окремих дисків. Оптичні носії доцільно використовувати для довгострокового архівування окремих доказів, хоча вони мають низьку швидкість роботи. Найкращі

результати за сукупністю показників демонструє хмарне зберігання, яке забезпечує практично необмежений обсяг, високу доступність і стійкість до фізичних загроз.

Таблиця 4.1 – Порівняльна характеристика сучасних підходів до зберігання цифрових доказів та персональних даних

| Підхід до зберігання | Основний принцип | Переваги | Недоліки | Рівень захисту | Придатність для цифрових доказів |
|---|---|---|---|---|---|
| Локальне файлове зберігання | Дані зберігаються на окремих фізичних носіях або серверах організації | Простота впровадження, низька вартість, повний фізичний контроль | Високий ризик втрати, пошкодження або несанкціонованого доступу | Середній | Обмежена |
| Хмарне зберігання | Дані розміщуються на віддалених серверах постачальника хмарних послуг | Масштабованість, резервне копіювання, доступність | Ризики витоку, складність контролю місця зберігання, залежність від провайдера | Середній – високий | Середня |

Продовження таблиці 4.1

| | | | | | |
|---|---|---|---|---|---|
| Захищені централізовані бази даних | Зберігання у спеціалізованих БД із системами журналювання та контролю доступу | Централізоване управління, контроль версій, аудит | Єдина точка відмови, потреба у дорогій інфраструктурі | Високий | Висока |
| Розподілене зберігання | Дані дублюються між декількома вузлами або серверами | Відмовостійкість, стійкість до втрати даних | Складність адміністрування та синхронізації | Високий | Висока |
| Блокчейн-зберігання | Хеші, журнали доступу та метадані фіксуються у незмінному реєстрі | Незмінність, прозорість, контроль ланцюга збереження | Високі вимоги до ресурсів, складність інтеграції | Дуже високий | Дуже висока |

Кінець таблиці 4.1

| | | | | | |
|---|---|---|---|---|---|
| Гібридне зберігання | Поєднання локального, хмарного та блокчейн-компонентів | Баланс між швидкістю, безпекою та доступністю | Потребує складної архітектури та налаштування | Дуже високий | Найвища |

Ефективність системи зберігання цифрових доказів значною мірою залежить від характеристик носіїв інформації, які використовуються для довготривалого архівування, оперативного доступу та резервування даних, адже різні типи носіїв мають власні переваги та недоліки, що впливають на швидкість обробки інформації, надійність та рівень захисту. Отже, результати порівняння свідчать про доцільність використання комбінованого підходу, при якому оперативне зберігання виконується на SSD або RAID-масивах, а резервні копії розміщуються у хмарному середовищі (табл. 4.2).

Таблиця 4.2 – Характеристика розробленої гібридної системи захисту даних

| Компонент системи | Призначення | Реалізовані механізми захисту |
|---|---|---|
| Локальне сховище | Тимчасове зберігання копій цифрових доказів | Контроль доступу, резервування, шифрування |
| Центральна база даних | Зберігання метаданих, журналів, ідентифікаторів | Розмежування прав доступу, журналювання дій |

Кінець таблиці 4.2

| | | |
|---|---|---|
| Хмарне сховище | Довготривале резервне зберігання | TLS, багатофакторна автентифікація, резервне копіювання |
| Блокчейн-модуль | Незмінна фіксація хешів та дій користувачів | Незмінність записів, контроль цілісності |
| Криптографічний модуль | Захист вмісту цифрових доказів | AES-256, SHA-256, цифрові підписи |
| Модуль журналювання | Ведення історії операцій з доказами | Аудит, часові мітки, контроль доступу |

Відсутність резервного копіювання означає, що при фізичному пошкодженні носія всі дані будуть втрачені безповоротно, з траєкторії кібербезпеки це означає втрату доказів та неможливість продовження розслідування інцинденту, вибір алгоритму шифрування впливає не лише на рівень безпеки, але й на швидкість обробки інформації та можливість подальшого використання даних у процесі розслідування. Для подолання проблеми відсутності шифрування багато користувачів застосовують вбудовані засоби шифрування операційних систем.

У системі Windows доступна технологія BitLocker, яка дозволяє зашифрувати весь системний диск або окремі розділи. Користувач встановлює пароль або використовує TPM модуль для автоматичного розшифрування при завантаженні системи. Аналогічну функціональність надає FileVault у macOS та LUKS у Linux-системах, сучасні алгоритми AES-128 та AES-256 є найбільш ефективними для використання у системах захисту цифрових доказів. Вони забезпечують високий рівень криптографічної стійкості та водночас не створюють надмірного навантаження на систему. Асиметричні алгоритми доцільно використовувати для передачі ключів та реалізації електронного підпису.

Таблиця 4.3 – Порівняльний аналіз методів шифрування цифрових доказів

| Метод шифрування | Довжина ключа | Швидкість роботи | Рівень криптостійкості | Поширеність використання | Придатність для цифрових доказів |
|---|---|---|---|---|---|
| DES | 56 біт | Висока | Низька | Низька | Непридатний |
| 3DES | 168 біт | Середня | Середня | Обмежена | Частково придатний |
| AES-128 | 128 біт | Висока | Висока | Дуже висока | Висока |
| AES-256 | 256 біт | Середня | Дуже висока | Дуже висока | Найвища |
| RSA | 1024–4096 біт | Низька | Дуже висока | Висока | Для передачі ключів |

Таблиця 4.3 характеризує основні функціональні модулі розробленої системи захисту цифрових доказів. У структурі системи передбачено окремий модуль імпорту, який забезпечує завантаження образів носіїв, лог-файлів та інших видів доказової інформації. Після цього активується модуль шифрування, що виконує криптографічний захист даних перед їх збереженням.

Вбудоване шифрування не захищає від атак на рівні операційної системи, коли зловмисник отримує доступ до вже увімкненого комп'ютера або експлуатує вразливості в самій системі шифрування, багато хто із сучасних користувачів для зберігання особистих фотографій та документів використовують хмарні сервіси, такі як Google Drive, Dropbox, iCloud або OneDrive. Ці рішення забезпечують автоматичне резервне копіювання та синхронізацію даних між різними пристроями. Користувач завантажує файли на сервери провайдера, де вони зберігаються в зашифрованому вигляді. Доступ до файлів можливий з будь-якого пристрою через веб-інтерфейс або мобільний додаток після автентифікації. Перевагою хмарного зберігання є висока доступність даних та захист від локальних катастроф. Якщо комп'ютер користувача буде пошкоджено або вкрадено, дані залишаються доступними через хмарне сховище. Провайдери хмарних сервісів

зазвичай застосовують шифрування при передачі та зберіганні даних, що забезпечує базовий рівень захисту.

Одним із ключових принципів інформаційної безпеки є розмежування прав доступу між різними категоріями користувачів, це дозволяє мінімізувати ризик несанкціонованого втручання у систему та пошкодження доказової інформації (табл. 4.4).

Таблиця 4.4 – Ролі користувачів у розробленій системі

| Роль користувача | Перегляд даних | Завантаження доказів | Видалення даних | Доступ до журналів |
|---|---|---|---|---|
| Адміністратор | Так | Так | Так | Так |
| Експерт | Так | Так | Ні | Так |
| Розслідування інциденту | Так | Так | Ні | Частково |
| Аналітик | Так | Ні | Ні | Частково |
| Гість | Обмежено | Ні | Ні | Ні |

Найбільший обсяг прав має адміністратор системи, тоді як інші користувачі отримують лише ті можливості, які необхідні для виконання їхніх професійних завдань. Однак такий метод додає складності у використанні, оскільки користувач повинен вручну монтувати зашифровані контейнери перед доступом до файлів. Крім того, синхронізація великих зашифрованих контейнерів може бути неефективною, оскільки зміна одного файлу всередині контейнера вимагає повторного завантаження всього контейнера.

Окремим випадком є використання повністю ізольованого комп'ютера, не підключеного до мережі Інтернет та локальної мережі.

Одним із ключових критеріїв оцінювання ефективності систем зберігання є швидкість виконання основних операцій. Для цифрових доказів особливо важливими є швидкість запису, читання, резервного копіювання та відновлення інформації після збою (табл.4.5).

Таблиця 4.5 – Порівняння часу виконання операцій для різних методів зберігання

| Метод зберігання | Час запису 1 ГБ, с | Час читання 1 ГБ, с | Час резервного копіювання 10 ГБ, хв | Час відновлення після збою, хв |
|---|---|---|---|---|
| Локальне зберігання | 35 | 20 | 18 | 120 |
| Хмарне зберігання | 50 | 30 | 12 | 45 |
| RAID-масив | 25 | 15 | 10 | 35 |
| Блокчейн-зберігання | 90 | 60 | 25 | 60 |

Важливим аспектом є також використання менеджерів паролів для захисту облікових даних. Багато користувачів зберігають паролі в текстових файлах або використовують однакові паролі для різних сервісів, що створює серйозні ризики безпеки. Менеджери паролів типу 1Password, Bitwarden, KeePass або LastPass зберігають всі паролі в зашифрованій базі даних, захищеній одним головним паролем.

Хмарні менеджери паролів (1Password, LastPass) синхронізують зашифровану базу паролів між пристроями через хмарні сервери провайдера. Локальні рішення (KeePass) зберігають базу паролів виключно на пристрої користувача. Хмарні рішення зручніші, але мають ті ж самі ризики, що й хмарні сховища взагалі. Неодноразові випадки компрометації хмарних менеджерів паролів демонструють потенційні ризики довіри третій стороні. Для зберігання особливо конфіденційних даних деякі користувачі застосовують апаратні токени безпеки. USB-токени типу YubiKey або апаратні модулі безпеки (Hardware Security Module, HSM) зберігають криптографічні ключі в захищеному апаратному

середовищі, з якого їх неможливо вилучити програмними засобами. Такі пристрої використовуються для двофакторної автентифікації, підпису документів або розшифрування файлів.

Класичне локальне зберігання без шифрування надто вразливе. Вбудоване шифрування операційної системи захищає лише від фізичного доступу, але не від програмних атак. Хмарні сервіси створюють ризики витоку через провайдера. Ізольований комп'ютер незручний у використанні та вразливий до фізичних атак. Спеціалізовані системи управління доказами надто дорогі для широкого використання.

## 4.2 Розроблена система: гібридний підхід до захисту даних

Система інтелектуального аналізу образів носіїв, описана в розділах 2 та 3, реалізує гібридний підхід, який поєднує переваги різних методів зберігання та усуває їх основні недоліки. Основна концепція полягає в багаторівневому захисті, де кожен рівень компенсує слабкості попереднього.

Наступний рівень захисту складається з детального аудиту всіх операцій з даними. Розроблена система автоматично фіксує кожну дію користувача: створення образу, читання, запуск аналізу, експорт результатів. Для кожної операції записується час, користувач, IP-адреса, тип дії та результат. Ці записи зберігаються в окремій базі даних з захистом від модифікації через database triggers, які забороняють зміну або видалення історичних записів.

На відміну від локального зберігання, де користувач може видалити файли без слідів, або хмарних сервісів, де логи контролюються провайдером, в розробленій системі створюється незмінний ланцюг подій, який можна перевірити незалежно. Кожен запис в журналі аудиту підписується цифровим підписом користувача, що унеможливлює заперечення виконаної дії. Це критично важливо для криміналістики, де необхідно довести, що докази не було підроблено, також стосується ізоляції процесів аналізу, адже проблема традиційних підходів полягає в тому, що аналіз образів відбувається в тому ж середовищі, де зберігаються дані.

Якщо образ містить шкідливе програмне забезпечення, воно може скомпрометувати всю систему при відкритті образу. Навіть ізольований комп'ютер без мережевого підключення вразливий до локальної експлуатації через вразливості в програмах аналізу.

Окрім того, рівень захисту складається з контролю доступу та автентифікації. Проблема локального зберігання полягає в тому, що будь-хто з доступом до комп'ютера може отримати доступ до файлів. Навіть при використанні паролів операційної системи існують способи обходу через завантаження з зовнішніх носіїв. Хмарні сервіси вимагають автентифікації, але часто обмежуються лише паролем, який може бути скомпрометовано через фішинг або витік.

Такі механізми відсутні в споживчих рішеннях зберігання даних. Хмарні сервіси мають базові захисні механізми про підключення з нових пристроїв, але не аналізують паттерни використання даних. Локальне зберігання взагалі не має можливостей для виявлення аномалій. Складається з резервного копіювання та відновлення. Проблема локального зберігання без резервування полягає в повній втраті даних при апаратній несправності. Проблема ізольованого комп'ютера в тому, що резервні копії складно організувати без порушення ізоляції. Хмарні сервіси забезпечують автоматичне резервування, але дані зберігаються у провайдера без контролю користувача.

Розроблена система підтримує автоматичне резервне копіювання з різними стратегіями зберігання. Щоденні інкрементальні копії зберігають лише зміни з попередньої копії, що економить дисковий простір. Тижневі диференційні копії зберігають зміни з початку тижня. Місячні повні копії містять всі дані повністю. Резервні копії можуть зберігатися як на локальних системах для швидкого відновлення, так і на віддалених серверах для захисту від локальних катастроф.

Критично важливо, що резервні копії також шифруються окремими ключами. Це означає, що навіть при компрометації сервера резервного копіювання зловмисник не отримає доступ до даних. На відміну від простого копіювання файлів на зовнішній диск, автоматизоване резервування гарантує регулярність та актуальність копій та відповідності регуляторним вимогам. При зберіганні

персональних даних організації повинні дотримуватися вимог регуляторів типу GDPR. Користувачі мають право запитати всі свої дані, виправити неточності або вимагати повного видалення. Звичайні файлові системи не мають механізмів для автоматизації цих процесів.

Таке розділення означає, що компрометація одного компоненту не надає автоматичного доступу до всієї інфраструктури. На відміну від монолітних систем, де база даних, додаток та файли працюють в одному середовищі, сегментація обмежує можливості зловмисника при успішній атаці.

## 4.3 Кількісне порівняння методів зберігання

Для об'єктивної оцінки переваг розробленої системи проведено кількісне порівняння ключових показників безпеки та продуктивності різних методів зберігання. Першим показником є час шифрування великих обсягів даних. Для образів носіїв розміром 1 ТБ, які є типовими в сучасних умовах, виміряно час шифрування різними методами. Вбудоване шифрування BitLocker показало середній час 2100 секунд для первинного шифрування диска на тестовому обладнанні. VeraCrypt з алгоритмом AES показав 2450 секунд. Розроблена система з багатопоточним шифруванням та оптимізацією через memory-mapped files показала 432 секунди, що в 4.8 разів швидше за BitLocker.

Така різниця пояснюється використанням всіх доступних ядер процесора для паралельного шифрування блоків та оптимізацією операцій вводу-виводу. Для користувача це означає, що шифрування великого диска займає не години, а хвилини, що робить захист даних практично зручним навіть для дуже великих обсягів. Для регулярного моніторингу цілісності, який виконується автоматично кожні 6-24 години, така швидкість критично важлива. Повна перевірка всіх образів у великому сховищі зайняла б дні, тоді як верифікація завершується за години.

На відміну від існуючих рішень, які фокусуються на окремих аспектах безпеки, розроблена система забезпечує багаторівневий захист з взаємним підсиленням різних механізмів. Практична цінність полягає в можливості

використання системи як для криміналістичних експертиз, так і для захищеного зберігання будь-яких конфіденційних даних з гарантованою цілісністю та контрольованим доступом.

## 4.4 Методи та засоби забезпечення системи кіберзахисту

Забезпечення кібербезпеки системи інтелектуального аналізу образів носіїв вимагає комплексного підходу, який охоплює технічні, організаційні та процедурні заходи. Основою технічного захисту є криптографічні методи, контроль доступу, аудит дій та захист мережевої взаємодії.

Криптографічний захист цілісності образів є фундаментальним елементом системи безпеки. Хешування образів носіїв виконується з використанням декількох криптографічних алгоритмів одночасно, що забезпечує додатковий рівень довіри. Зазвичай використовується комбінація SHA-256, SHA-512 та MD5, незважаючи на те, що MD5 вважається застарілим для деяких застосувань, він залишається стандартом у цифровій криміналістиці для забезпечення сумісності зі старим обладнанням та програмним забезпеченням. Процес хешування починається одразу після створення образу, коли обчислюються криптографічні хеші всього образу. Ці хеш-суми записуються в метадані та підписуються цифровим підписом особи, яка створила образ. При кожному наступному доступі до образу хеш-сума перераховується та порівнюється з еталонною, що дозволяє виявити будь-які модифікації. Для великих образів, розмір яких може сягати терабайтів, використовується також поблочне хешування, коли образ розбивається на блоки фіксованого розміру, і для кожного блоку обчислюється окремий хеш. Це дозволяє швидко ідентифікувати, які саме частини образу були змінені, без необхідності перерахунку хешу всього образу.

Автоматична ротація ключів виконується згідно з політикою безпеки, зазвичай щоквартально для симетричних ключів та щорічно для асиметричних. Компрометовані або підозрілі ключі негайно відкликаються та замінюються. Доступ до криптографічних ключів контролюється окремо від доступу до даних,

що реалізує принцип розділення обов'язків. Критичні операції з ключами вимагають авторизації декількох осіб, що запобігає зловживанням з боку одного адміністратора.

## 4.5 Умови аналізу загроз безпеці при роботі з цифровими доказами

Робота з цифровими доказами та образами носіїв інформації супроводжується специфічними ризиками інформаційної безпеки, що можуть скомпрометувати як результати розслідування, так і конфіденційні дані, які містяться в образах. Аналіз цих загроз є критично важливим для розробки ефективних механізмів захисту системи інтелектуального аналізу.

Для ефективного планування захисту необхідно розуміти модель порушника. Зовнішній порушник зазвичай має мотивацію отримати доступ до конфіденційних доказів, знищити їх або модифікувати на користь особи, що розслідується. Його можливості включають атаки через мережу, експлуатацію вразливостей публічно доступних інтерфейсів, соціальну інженерію для отримання облікових даних та фізичний доступ до приміщень у разі недостатнього фізичного захисту. Обмеження зовнішнього порушника полягають у відсутності легітимного доступу до системи, необхідності долати периметрові засоби захисту та обмежених знаннях про внутрішню архітектуру системи.

Модель загроз для образів носіїв повинна враховувати можливість створення шкідливих образів, спеціально сконструйованих для компрометації системи аналізу. Комплексний аналіз загроз показує, що система інтелектуального аналізу образів носіїв цифрових доказів повинна мати багаторівневий захист, який охоплює всі етапи життєвого циклу доказів від моменту їх отримання до архівування після завершення розслідування. Критичним є забезпечення балансу між безпекою та функціональністю, оскільки надмірні обмеження можуть ускладнити роботу аналітиків та знизити ефективність розслідувань.

## 4.6 Ізоляція та захист від шкідливого коду в образах

Образи носіїв цифрових доказів можуть містити шкідливе програмне забезпечення, експлойти та інші загрози, які потенційно можуть скомпрометувати систему аналізу. Тому критично важливою є реалізація багаторівневої системи ізоляції та захисту. Концепція аналізу образів базується на створенні ізольованого середовища, в якому аналіз виконується без ризику для основної системи.

Приховування даних в нерозподіленому просторі диска виявляється через ретельне сканування всього фізичного носія, включаючи області, не зайняті файловою системою. Використання захисних механізмів для приховування інформації в інших файлах може бути виявлено через статистичний аналіз ентропії файлів та пошук аномалій у структурі даних. Множинне перезаписування файлів для їх гарантованого знищення може бути виявлено через аналіз дискових структур та метаданих файлової системи.

Мережева безпека системи інтелектуального аналізу образів охоплює захист каналів передачі даних, протидію мережевим атакам та забезпечення конфіденційності комунікацій між компонентами розподіленої системи.

Передача великих образів носіїв через мережу вимагає додаткових механізмів захисту та оптимізації. Сегментація великих файлів на менші блоки дозволяє ефективно відновлювати передачу після переривань без необхідності починати спочатку. Кожен сегмент шифрується окремо та має власну контрольну суму для верифікації цілісності.

Система виявлення та запобігання вторгненням моніторує мережевий трафік для виявлення аномалій та атак. Сигнатурне виявлення ідентифікує відомі паттерни атак на основі баз даних сигнатур, які регулярно оновлюються. Аномальне виявлення базується на моделі нормальної поведінки мережі та сигналізує про відхилення, які можуть вказувати на невідомі атаки.

Моніторинг мережевої активності в реальному часі забезпечує швидке виявлення та реагування на інциденти безпеки. Централізована система збору логів агрегує дані з усіх мережевих пристроїв, серверів та систем безпеки. Кореляція

подій з різних джерел дозволяє виявляти складні багатоетапні атаки, які не очевидні при розгляді окремих подій. Автоматизовані сповішення сповіщають команду безпеки про критичні події, які вимагають негайного реагування. Дашборди візуалізації надають операторам центру безпеки можливість швидко оцінити стан системи та виявити аномалії. Історичні дані зберігаються для ретроспективного аналізу інцидентів та вдосконалення політик безпеки.

Віддалений доступ до системи для аналітиків, які працюють за межами офісу, вимагає особливих заходів безпеки. Virtual Private Network з використанням сучасних протоколів, таких як WireGuard або OpenVPN з надійним шифруванням, створює захищений тунель між клієнтом та корпоративною мережею. Багатофакторна автентифікація є обов'язковою вимогою для всіх віддалених підключень, поєднуючи щось, що користувач знає (пароль), щось, що має (токен або смартфон), та опціонально щось, чим він є (біометрія). Обмеження доступу на основі геолокації може блокувати підключення з несподіваних або підозрілих регіонів. Моніторинг сесій віддаленого доступу дозволяє виявляти підозрілу активність та при необхідності примусово завершувати сесії. Обмеження функціональності для віддалених користувачів може включати заборону на завантаження повних образів або обмеження на експорт великих обсягів даних.

## 4.7 Висновки до четвертого розділу

У четвертому розділі проведено комплексний аналіз питань кібербезпеки при роботі з системою інтелектуального аналізу образів носіїв цифрових доказів. Детально розглянуто специфічні загрози безпеці, характерні для систем типу Digital Forensics, включаючи загрози цілісності доказів, конфіденційності інформації, доступності аналітичних систем та специфічні загрози, пов'язані з anti-forensics техніками та шкідливим кодом в образах. Проведений аналіз показав необхідність захисту як від зовнішніх атак, так і від внутрішніх загроз, оскільки інсайдери з легітимним доступом можуть завдати найбільшої шкоди. Виявлено

вразливості на різних рівнях системи, від процесу збору доказів до їх аналізу та зберігання, що обґрунтовує необхідність багаторівневого підходу до захисту.

# ВИСНОВКИ

У роботі за результатами виконаних теоретичних та практичних досліджень розроблено новий метод інтелектуального аналізу образів носіїв цифрових доказів на основі композиції глибоких нейронних мереж для автоматичного виділення ознак, алгоритмів кластеризації для виявлення аномалій та механізмів захисту від ворожих атак. Розроблено комплексну систему методів та засобів забезпечення кібербезпеки, яка включає криптографічний захист цілісності через множинне хешування та електронний цифровий підпис, захист конфіденційності через шифрування при зберіганні та передачі даних, рольовий контроль доступу з принципом найменших привілеїв, детальний аудит всіх операцій для забезпечення підзвітності, та формування непорушного ланцюга зберігання доказів для забезпечення їх юридичної прийнятності.

Запропонований комплекс заходів забезпечення кібербезпеки створює багаторівневий захист системи інтелектуального аналізу образів носіїв цифрових доказів, що дозволяє проводити розслідування інцидентів безпеки та судові експертизи з гарантією цілісності, конфіденційності та доступності доказів. Реалізація цих заходів є необхідною умовою для створення надійної та довіреної системи цифрової криміналістики, результати роботи якої можуть бути використані в судових процесах та для прийняття критичних рішень в галузі інформаційної безпеки.

Особливу увагу було приділено побудові фітнес-функції, яка виступає центральним елементом оцінювання гіпотез. Показано, що у задачах кібербезпеки вона повинна мати багатокритеріальний характер і враховувати не лише точність класифікації, але й рівень хибних спрацьовувань, здатність до узагальнення та обчислювальну ефективність. Такий підхід забезпечує формування більш збалансованих і практично придатних рішень.

У процесі дослідження було також обґрунтовано вибір основних еволюційних операторів. Зокрема, встановлено, що ефективний кросинговер повинен бути структурно-орієнтованим і забезпечувати збереження семантичної

цілісності гіпотез, тоді як процедура мутації виконує критично важливу роль у підтриманні різноманітності популяції та генерації нових варіантів рішень. Показано, що оптимальні параметри цих операторів не є фіксованими і повинні адаптуватися до стану еволюційного процесу.

У першому розділі було проведено комплексний аналіз теоретичних і практичних аспектів інтелектуального аналізу цифрових доказів в контексті забезпечення інформаційної безпеки.

У другому розділі було сформовано цілісну теоретичну та методологічну основу методу виявлення кіберзагроз на базі еволюційних алгоритмів, яка враховує специфіку сучасного кіберпростору, що характеризується високою динамічністю, невизначеністю та складністю структури даних.

У третьому розділі було послідовно розв’язано завдання проектування та програмної реалізації системи інтелектуального аналізу образів носіїв.

У четвертому розділі проведено комплексний аналіз питань кібербезпеки при роботі з системою інтелектуального аналізу образів носіїв цифрових доказів.

Узагальнюючи отримані результати, можна зробити висновок, що застосування еволюційних алгоритмів у задачах виявлення кіберзагроз є перспективним напрямом розвитку інтелектуальних систем кібербезпеки. Запропонований підхід забезпечує високу адаптивність, здатність до виявлення нових і модифікованих атак, а також можливість роботи з великими обсягами складних і неоднорідних даних. Це створює передумови для розробки ефективних систем підтримки прийняття рішень у сфері інформаційної безпеки та підвищення загального рівня захищеності сучасних інформаційних інфраструктур.

Таким чином, результати розділу формують завершену теоретичну базу для подальшої реалізації та експериментальної перевірки запропонованого методу, а також відкривають можливості для його розвитку шляхом інтеграції з іншими сучасними підходами інтелектуального аналізу даних.

Подальші дослідження мають бути спрямовані на вирішення виявлених проблем і реалізацію перспективних напрямків розвитку, таких як розробка надійних методів виявлення фальсифікацій, створення масштабованих і

ефективних алгоритмів обробки великих даних, забезпечення конфіденційності та етичності використання технологій штучного інтелекту, а також розвиток стандартів і методологій для обміну та інтеграції цифрових доказів.

# ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Полторацький В. О., Гавриленко С. Ю. Еволюція систем виявлення вторгнень у кібербезпеці. *Автоматизовані інформаційні системи*. 2026. № 2. С. 100–116. https://doi.org/10.20998/2522-9052.2026.2.11 .

2. Хахановський В. Г., Гуцалюк М. В. Особливості використання електронних (цифрових) доказів у кримінальних провадженнях. *Криміналістичний вісник.* 2020. № 1(31). С. 13–19. https://doi.org/10.37025/1992-4437/2019-31-1-13

3. Столітній А. В., Каланча І. Г. Формування інституту електронних доказів у кримінальному процесі України. *Проблеми законності.* 2019. №. 146. С. 179–191. https://doi.org/10.21564/2414-990x.146.171218

4. Гребенькова М. С. Стан наукових досліджень в сфері електронних відображень у кримінальному провадженні. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2021. №. 67. С. 267–271. https://doi.org/10.24144/2307-3322.2021.67.51

5. Чванкін С. А. Комп'ютерно-технічна експертиза у цивільному судочинстві. *Право та державне управління.* 2021. № 1. С. 45–51. https://doi.org/10.32840/pdu.2021.1.7

6. Шепітько В. Ю., Авдєєва Г. К., Шевчук В. М., Капустіна М. В., Яремчук В. О., Негребецький В. В., Соколенко М. О., Пугач А. О. Використання цифрових технологій і систем штучного інтелекту у криміналістиці та судовій експертизі. *Питання боротьби зі злочинністю.* 2024. № 48. С. 61–71. https://doi.org/10.31359/2079-6242-2024-48-61

7. Зінич Л. В. Судова експертиза цифрових доказів у справах про плагіат: методологія та проблеми доказування. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2025. №88. С. 256–262. https://visnyk-pravo.uzhnu.edu.ua/article/view/330683

8. Менчинська М., Лук'янчиков Б. Електронні докази з блокчейн-систем під час воєнного стану: проблема допустимості. *Науковий вісник Ужгородського*

*національного університету. Серія: Право*. 2025. Т. 4. № 92 С. 343–349. https://doi.org/10.24144/2307-3322.2025.92.4.47

9. Сіренко О. В. Електронні докази у кримінальному провадженні. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2019. №. 14. С. 208–214. https://journals.dpu.kyiv.ua/index.php/law/article/view/174

10. Татулич І. Ю. Електронні докази як засіб доказування в цивільному судочинстві. *Часопис Київського університету права*. 2020. № 1. С. 215–219. https://doi.org/10.36695/2219-5521.1.2020.43

11. Демура М. І., Клепка Д. І., Крицька І. О. Забезпечення прав та законних інтересів особи в умовах «діджиталізації» кримінального провадження. *Часопис Київського університету права*. 2020. № 1. С. 295–301 https://doi.org/10.36695/2219-5521.1.2020.59

12. Степанюк Р. Л. Судова комп'ютерно-технічна експертиза: стан і перспективи розвитку. *Вісник Луганського держаного університету внутрішніх справ ім. Е. О. Дідоренка*. 2023. № 2(102). С. 289–305. https://dspace.univd.edu.ua/items/70579d0c-b28d-4e9b-9641-03914d5543eb

13. Коваленко А. В. Електронні докази в кримінальному провадженні: сучасний стан та перспективи використання. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2018. №. 4(84). С. 237–245. http://nbuv.gov.ua/UJRN/Vlduvs_2018_4_30

14. Алєксєєва-Процюк Д. О., Бриськовська О. М. Електронні докази в кримінальному судочинстві: поняття, ознаки та проблемні аспекти застосування. *Науковий вісник публічного та приватного права*. 2018. №. 2. С. 247–253. http://www.nvppp.in.ua/vip/2018/2/50.pdf#page=1

15. Дегтярьова О. Доказування у кримінальному провадженні на підставі електронних доказів. *Юридичний вісник*. 2021. № 6. С. 273–278. https://dspace.onua.edu.ua/items/615b4567-62f2-4c52-a0e3-6cf477ce2122

16. Фігурський В. М. Докази в електронній формі у кримінальному провадженні. *Галицькі студії: Юридичні науки*. 2023. № 4. С. 97–105. https://journals.gi.ternopil.ua/index.php/law/article/view/50

17. Карпець Ю. В. Цифрові докази та комп'ютерно-технічні експертизи у кримінальних провадженнях про військові злочини. *Юридичний науковий електронний журнал.* 2025. № 11. С. 226–230 https://lsej.org.ua/11_2025/48.pdf#page=1

18. Орлов Ю. Ю. Електронне відображення як криміналістичний об'єкт. *Науковий вісник Національної академії внутрішніх справ.* 2019. № 4(113). С. 15–23. https://elar.naiau.kiev.ua/bitstream/123456789/17509/1/%D0%9D%D0%92%204%2819%29_p015-023.pdf#page=1

19. Удовенко Ж. В. Призначення комп'ютерно-технічної експертизи під час розслідування кримінальних правопорушень, що вчиняються у сфері комп'ютерної інформації. *eKMAIR.* 2024. С. 91–96. https://ekmair.ukma.edu.ua/items/e31dba79-d5a4-4431-92b2-28a668008565

20. Степаненко А. С. Цифрові (електронні) докази в кримінальному провадженні України: поточний стан та виклики. *Репозиторій (відкритий електронний архів) Національного університету «Одеська юридична академія».* 2025. Т. 1. С. 584–587. https://dspace.onua.edu.ua/items/6a1ec120-309d-409e-be1f-7d484cf9e2d3

21. Авдєєва Г. К. Цифрові докази і системи штучного інтелекту у правозастосовній діяльності. *Питання боротьби зі злочинністю.* 2023. № 46. С. 32–40. https://pbz.nlu.edu.ua/article/view/301295

22. Лахно М. В. Системний аналіз цифрових слідів у інформаційно-освітній системі університету. *Електронне фахове наукове видання «Кібербезпека: освіта, наука, техніка»* 2025. № 3(27). С. 72–86. https://doi.org/10.28925/2663-4023.2025.27.709

*23.* Полотай О. І. Використання комп'ютерної криміналістики для забезпечення ефективного розслідування інцидентів інформаційної та кібербезпеки. *Вісник Львівського державного університету безпеки*

*життєдіяльності.* 2023. № 28. С. 73–80. https://doi.org/10.32447/20784643.28.2023.07

*24.* Неділько Я. В. Поняття цифрової криміналістики та її місце в системі криміналістики. *Криміналістика і судова експертиза.* 2024. №. 69. С. 228–236. https://doi.org/10.33994/kndise.2024.69.21

*25.* Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. №. 85. ч. 4. С. 71–75. https://doi.org/10.24144/2307-3322.2024.85.4.10 (дата звернення: 10.02.2026).

*26.* Гора І. В., Колесник В. А., Попович І. І. Цифрова криміналістика в забезпеченні діяльності з протидії злочинності. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. № 85. ч. 4. С. 63–70. dspace.uzhnu.edu.ua

*27.* Степанюк Р. Л. Цифрова криміналістична розвідка: поняття та перспективи розвитку. *Право і безпека.* 2026. № 1(100). С. 34–45. dspace.univd.edu.ua

*28.* Діденко О. В. Цифрова криміналістика та міжнародна протидія кіберзлочинності (на прикладі електронної торгівлі). *Аналітично-порівняльне правознавство.* 2025. № 4. ч. 3. С. 184–192. https://doi.org/10.24144/2788-6018.2025.04.3.26

*29.* Гуцалюк М. В., Антонюк П. Є. Щодо сутності електронної (цифрової) інформації як джерела доказів у кримінальному провадженні. *Криміналістичний вісник.* 2020. № 1(33). С. 37–49. https://doi.org/10.37025/1992-4437/2020-33-1-37

30. Каланча І. Г., Гаркуша А. М. Копія електронної інформації як доказ у кримінальному провадженні: процесуальний та технічний аспекти. *Юридичний науковий електронний журнал.* 2021. № 8. С. 336–339. https://doi.org/10.32782/2524-0374/2021-8/77

*31.* Степанюк Р. Л., Гусєва В. О., Кікінчук В. В., Щербаковський М. Г. Криміналістика: криміналістична техніка: навчальний посібник. *Харківський національний університет внутрішніх справ.* 2023. № 4. С. 1–388.

https://dspace.univd.edu.ua/entities/publication/08bbafe6-82ba-40c4-9246-e32d7fb26a10

*32.* Богданов О., Чернігівський І. Типи цифрових криміналістичних артефактів в комп'ютерах під управлінням ОС Windows. *Кібербезпека: освіта, наука, техніка.* 2024. Т. 4. № 24. С. 221–228. https://doi.org/10.28925/2663-4023.2024.24.221228

33. Гайдук О., Звєрєв В. Аналіз кіберзагроз в умовах стрімкого розвитку інформаційних технологій. *Кібербезпека: освіта, наука, техніка.* 2024. № 3(23). С. 225–236. https://doi.org/10.28925/2663-4023.2024.23.225236.

34. Василенко В. М. Цифрова трансформація правоохоронних органів: ризики в умовах гібридних загроз та шляхи їх подолання. *Вісник Кримінологічної асоціації України.* 2024. № 2(32). С. 945–958. https://doi.org/10.32631/vca.2024.2.74

35. Демидова Є. Є. Цифрові сліди кримінального правопорушення: поняття та особливості. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2024. №. 85. Т. 4. С. 71–75. https://doi.org/10.24144/2307-3322.2024.85.4.10

36. Casino F., Pina C., López-Aguilar P., Batista E., Patsakis C. SoK: Cross-border Criminal Investigations and Digital Evidence. *arXiv*. 2022. С. 1–23. https://arxiv.org/abs/2205.12911

37. Tok Y. C., Chattopadhyay S. Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling. *arXiv*. 2023. Vol. 45. С. 1–14. https://arxiv.org/abs/2210.14692

38. Verdoliva L. Media Forensics and DeepFakes: an Overview. *arXiv*. 2020. С. 1–4. https://arxiv.org/abs/2001.06564

39. Шульга В., Калюжна Л. Електронні докази у кримінальному процесі: методи їх виявлення, дослідження та правове закріплення. *Теорія та практика судової експертизи і криміналістики.* 2025. №. 3(40). С. 136–152. https://doi.org/10.32353/khrife.3.2025.10.

40. Мілімко Л. В., Жидовцев Я. В. Електронні докази в кримінальному судочинстві України. *Науковий вісник Ужгородського національного*

*університету. Серія: Право.* 2025. №. 88. Т. 3. С. 302–308. https://doi.org/10.24144/2307-3322.2025.88.3.45.

41. Carrier B., Spafford E. H. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence.* 2003. Vol. 2. P. 1–20. https://www.utica.edu/academic/institutes/ecii/publications/articles/A0AC5A7A-FB6C-325D-BF515A44FDEE7459.pdf

*42.* Reith M., Carr C., Gunsch G. An Examination of Digital Forensic Models. *International Journal of Digital Evidence.* 2002. Vol. 1. P. 1–12. https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf

*43.* Balushi Y., Ashrafi M., Kumar B., et al. The Use of Machine Learning in Digital Forensics: Review Paper. *Advances in Computer Science Research.* 2023. Vol. 104. P. 96–113. https://doi.org/10.2991/978-94-6463-110-4_9

44. Kyei K., Zavarsky P., Lindskog D., Ruhl R. A review and comparative study of digital forensic investigation models. *Digital Forensics and Cyber Crime: Proceedings of ICDF2C. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering.* 2012. Vol. 114. P. 314–327. https://doi.org/10.1007/978-3-642-39891-9_20.

45. Garfinkel S. L. Digital forensics research: The next 10 years. *Digital Investigation.* 2010. Vol. 7. P. 64–73. https://doi.org/10.1016/j.diin.2010.05.009.

46. Garfinkel S. L., Farrell P., Roussev V., Dinolt G. Bringing science to digital forensics with standardized forensic corpora. *Digital Investigation.* 2009. Vol. 6. P. 2–11. https://doi.org/10.1016/j.diin.2009.06.016.

47. Kohn M. D., Eloff M. M., Eloff J. H. P. Integrated digital forensic process model. *Computers & Security.* 2013. Vol. 38. P. 103–115. https://doi.org/10.1016/j.cose.2013.05.001.

48. Case A., Richard G. G. Memory forensics: The path forward. *Digital Investigation.* 2017. Vol. 20. P. 23–33. https://doi.org/10.1016/j.diin.2016.12.004.

49. Grajeda C., Breitinger F., Baggili I. Availability of datasets for digital forensics – And what is missing. *Digital Investigation.* 2017. Vol. 22. P. 94–105. https://doi.org/10.1016/j.diin.2017.06.004.

50. Beebe N. L., Clark J. G. Digital forensic text string searching: Improving information retrieval effectiveness by thematically clustering search results. *Digital Investigation.* 2007. Vol. 4. P. 49–54. https://doi.org/10.1016/j.diin.2007.06.005.

51. Horsman G. "I couldn't find it your honour, it mustn't be there!" – Tool errors, tool limitations and user error in digital forensics. *Science & Justice.* 2018. Vol. 58. No. 6. P. 433–440. https://doi.org/10.1016/j.scijus.2018.04.001.

52. Horsman G. Tool testing and reliability issues in the field of digital forensics. *Digital Investigation.* 2019. Vol. 28. P. 163–175. https://doi.org/10.1016/j.diin.2019.01.009.

53. Quick D., Choo K.-K. R. Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. *Future Generation Computer Systems.* 2018. Vol. 78. P. 558–567. https://doi.org/10.1016/j.future.2016.12.032.

54. Göbel T., Maltan S., Türr J., Baier H., Mann F. ForTrace – A holistic forensic data set synthesis framework. *Forensic Science International: Digital Investigation*. 2022. Vol. 40. P.1–14. https://doi.org/10.1016/j.fsidi.2022.301344

55. Dunsin D., Ghanem M. C., Ouazzane K., Vassilev V. A comprehensive analysis of the role of artificial intelligence and machine learning in modern digital forensics and incident response. *Forensic Science International: Digital Investigation.* 2024. Vol. 48. P. 1–22. https://doi.org/10.1016/j.fsidi.2023.301675.

56. Ngejane C. H., Eloff J. H. P., Sefara T. J., Marivate V. N. Digital forensics supported by machine learning for the detection of online sexual predatory chats. *Forensic Science International: Digital Investigation.* 2021. Vol. 36. https://doi.org/10.1016/j.fsidi.2021.301109

57. Le Q., Boydell O., Mac Namee B., Scanlon M. Deep learning at the shallow end: Malware classification for non-domain experts. *Digital Investigation.* 2018. Vol. 26. P. 118–126. https://doi.org/10.1016/j.diin.2018.04.024

58. Karbab E. B., Debbabi M., Derhab A., Mouheb D. MalDozer: Automatic framework for Android malware detection using deep learning. *Digital Investigation*. 2018. Vol. 24. P. 48–59. https://doi.org/10.1016/j.diin.2018.01.007.

59. Nowroozi E., Dehghantanha A., Parizi R. M., Choo K.-K. R. A survey of machine learning techniques in adversarial image forensics. *Computers & Security*. 2021. Vol. 100. https://doi.org/10.1016/j.cose.2020.102092.

60. Ferreira S., Antunes M., Correia M. E. A Dataset of Photos and Videos for Digital Forensics Analysis Using Machine Learning Processing. *Data*. 2021. Vol. 6(8). No. 87. P. 1–15. https://doi.org/10.3390/data6080087.

61. Breiman L. Random Forests. *Machine Learning*. 2001. Vol. 45. P. 5–32. https://doi.org/10.1023/A:1010933404324.

62. Cortes C., Vapnik V. Support-vector networks. *Machine Learning*. 1995. Vol. 20. P. 273–297. https://doi.org/10.1007/BF00994018.

63. Ester M. Kriegel H.-P. Sander J. Xu X. A density-based algorithm for discovering clusters in large spatial databases with noise. *Proceedings of the Second International Conference on Knowledge Discovery and Data Mining (KDD-96)*. 1996. P. 226–231. https://dl.acm.org/doi/10.5555/3001460.3001507.

64. Pedregosa F., Varoquaux G., Gramfort A. et al. Scikit-learn: Machine Learning in Python. *Journal of Machine Learning Research*. 2011. Vol. 12. P. 2825–2830. https://jmlr.org/papers/v12/pedregosa11a.html.

65. McKinney W. Data Structures for Statistical Computing in Python. *Proceedings of the 9th Python in Science Conference*. 2010. P. 56–61. https://doi.org/10.25080/Majora-92bf1922-00a.

66. Breitinger F., Hilgert J.-N., Hargreaves C., Sheppard J., Overdorf R., Scanlon M. DFRWS EU 10-year review and future directions in Digital Forensic Research. *Forensic Science International: Digital Investigation*. 2024. Vol. 48. P. 1–12. https://doi.org/10.1016/j.fsidi.2023.301685.

67. Zareen M. S., Aslam B., Tahir S., Rasheed I., Khan F. Unveiling the Dynamic Landscape of Digital Forensics: The Endless Pursuit. *Computers*. 2024. Vol. 13. No. 12. P. 1–34. https://doi.org/10.3390/computers13120333.

68. Adkins J., Al Bataineh A., Khalaf M. Identifying Persons of Interest in Digital Forensics Using NLP-Based AI. *Future Internet.* 2024. Vol. 16. No. 11. P. 1–19. https://doi.org/10.3390/fi16110426.

69. Hilgert J.-N., Lambertz M., Plohmann D. Extending The Sleuth Kit and its underlying model for pooled storage file system forensic analysis. *Digital Investigation*. 2017. Vol. 22. P. 76–85. https://doi.org/10.1016/j.diin.2017.06.003.

70. Plum J., Dewald A. Forensic APFS File Recovery. *Proceedings of the 13th International Conference on Availability, Reliability and Security (ARES 2018)*. 2018. No. 47. P. 1–10. https://doi.org/10.1145/3230833.3232808.

71. Nordvik R., Stoykova R., Franke K., Axelsson S., Toolan F. Reliability validation for file system interpretation. *Forensic Science International: Digital Investigation.* 2021. Vol. 37. P. 1–14. https://doi.org/10.1016/j.fsidi.2021.301174.

72. Palutke R., Freiling F. Styx: Countering robust memory acquisition. *Digital Investigation.* 2018. Vol. 24. P. 18–28. https://doi.org/10.1016/j.diin.2018.01.004.

73. Otsuki Y., Kawakoya Y., Iwamura M., Miyoshi J., Ohkubo K. Building stack traces from memory dump of Windows x64. *Digital Investigation.* 2018. Vol. 24. P. 101–110. https://doi.org/10.1016/j.diin.2018.01.013.

74. Palmbach D., Breitinger F. Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability. *Forensic Science International: Digital Investigation.* 2020. Vol. 32. P. 1–9. https://doi.org/10.1016/j.fsidi.2020.300920.

75. Göbel T., Baier H. Anti-forensics in ext4: On secrecy and usability of timestamp-based data hiding. *Digital Investigation.* 2018. Vol. 24. P. 111–120. https://doi.org/10.1016/j.diin.2018.01.014.

76. Hitchcock B., Le-Khac N.-A., Scanlon M. Tiered forensic methodology model for Digital Field Triage by non-digital evidence specialists. *Digital Investigation.* 2016. Vol. 16. P. 75–85. https://doi.org/10.1016/j.diin.2016.01.010.

77. Gogia G., Rughani P. H. An ML based digital forensics software for triage analysis through face recognition. *Journal of Digital Forensics, Security and Law.* 2023. Vol. 17. No. 2. P. 1–13 https://doi.org/10.58940/1558-7223.1772.

78. Nayerifard T., Amintoosi H., Ghaemi Bafghi A., Dehghantanha A. Machine Learning in Digital Forensics: A Systematic Literature Review. *arXiv* 2023. P. 99. https://doi.org/10.48550/arXiv.2306.04965.

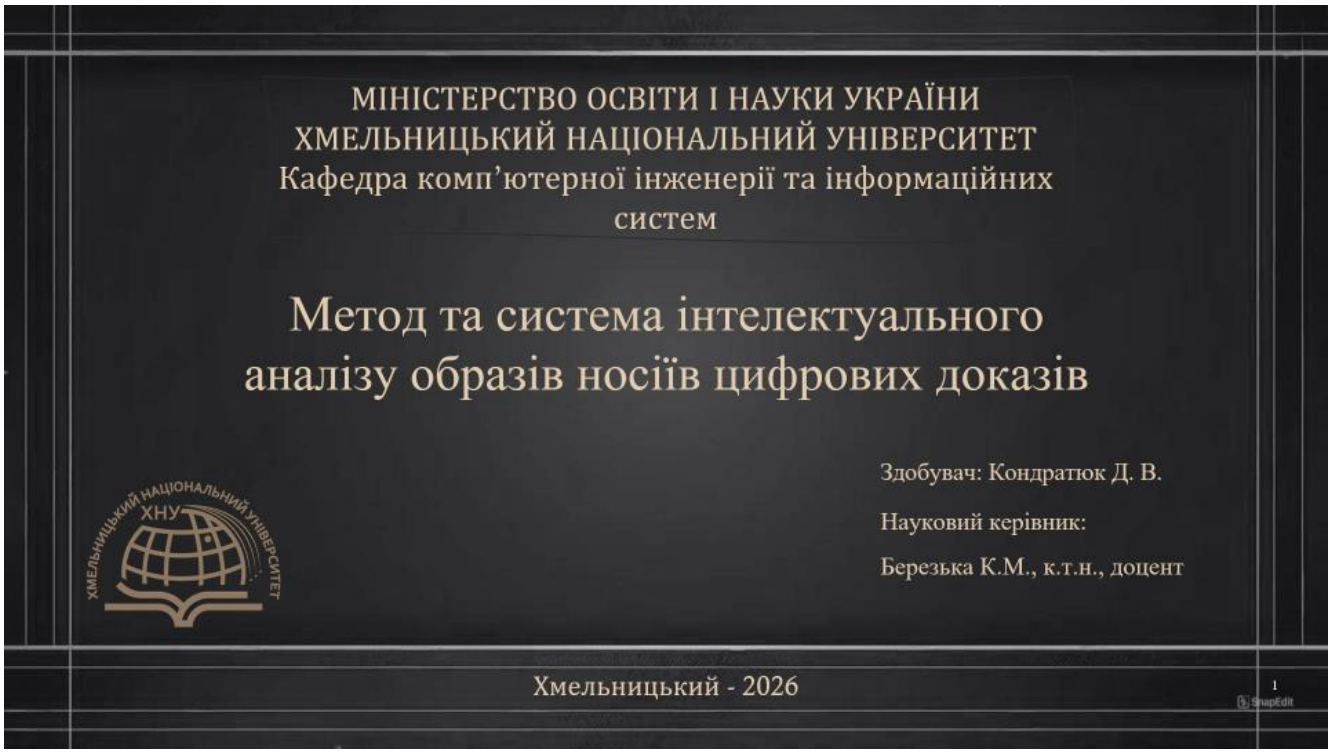
79. Lillis D., Becker B., O'Sullivan T., Scanlon M. Current challenges and future research areas for digital forensic investigation. *Proceedings of the 11th ADFSL Conference on Digital Forensics, Security and Law (CDFSL 2016)*. 2016. P. 1–11. https://doi.org/10.48550/arXiv.1604.03850.

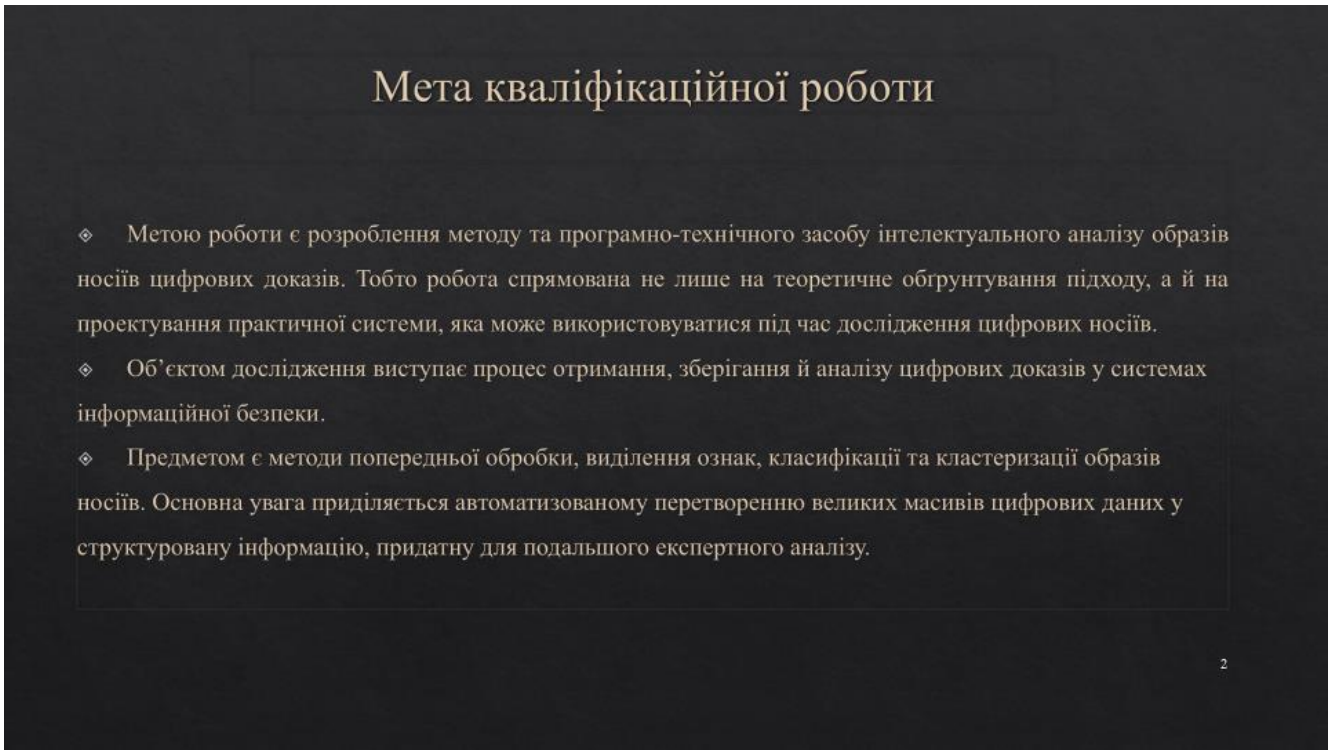
80. Roussev V. Data Fingerprinting with Similarity Digests. Advances in *Digital Forensics VI*. 2010. Vol. 337. P. 207–226. https://doi.org/10.1007/978-3-642-15506-2_15.

# ДОДАТОК А

(обов’язковий)

Презентація



# Задачі дослідження

**Поставленої мети досягають шляхом розв'язання таких основних завдань:**

- проаналізувати сучасний стан цифрової криміналістики та інструменти роботи з доказами;
- формалізувати задачу інтелектуального аналізу образів носіїв;
- розробити метод попередньої обробки та виділення інформативних ознак;
- розробити метод класифікації і кластеризації образів;
- спроектувати архітектуру ПЗ, базу даних та модулі системи;
- провести тестування системи на контрольних наборах даних.

3

# Наукова новизна і практична цінність отриманих результатів

Наукова новизна:

- Розроблено метод інтелектуального аналізу зображень носіїв цифрових доказів.
- Запропоновано підхід до автоматизованого виявлення та інтерпретації цифрових слідів.
- Підвищено точність обробки та класифікації цифрової інформації.

Практична цінність:

- Можливість застосування в криміналістичній експертизі.
- Підвищення ефективності аналізу цифрових доказів.
- Скорочення часу обробки великих обсягів даних.
- Використання в системах інформаційної безпеки.

4

## Актуальність дослідження

- Обсяги цифрових доказів швидко зростають: диски, мобільні пристрої, хмари, мережеві журнали;
- Ручний аналіз образів носіїв є тривалим і залежить від кваліфікації експерта;
- Зловмисники використовують шифрування, приховування файлів і знищення слідів;
- Потрібні автоматизовані методи швидкого пошуку релевантних артефактів без порушення цілісності доказів.


5

## Життєвий цикл роботи з цифровими доказами


Основний принцип полягає в тому, що експерт працює не з оригінальним носієм, а з його побітовою копією. На етапі створення копії обчислюються, щоб забезпечити відтворюваність аналізу та збереження ланцюжка доказове хеш-значення, наприклад MD5 або SHA-256, які надалі використовуються для перевірки цілісності. Усі дії експерта повинні записуватися звіт до журналу, щоб забезпечити відтворюваність аналізу та збереження ланцюжка доказовості.

6

# Методи та засоби отримання доказів

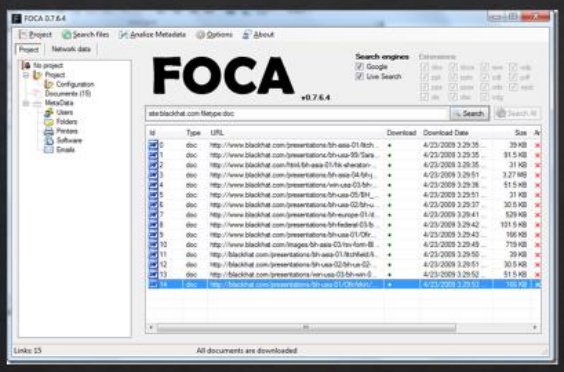
Форензичне копіювання

- форензичне копіювання носіїв без внесення змін в оригінальні дані;
- відновлення видалених файлів та data carving за сигнатурами;
- аналіз метаданих документів, фото й відео;
- комплексні платформи: EnCase, FTK, Magnet AXIOM, Cellebrite UFED.

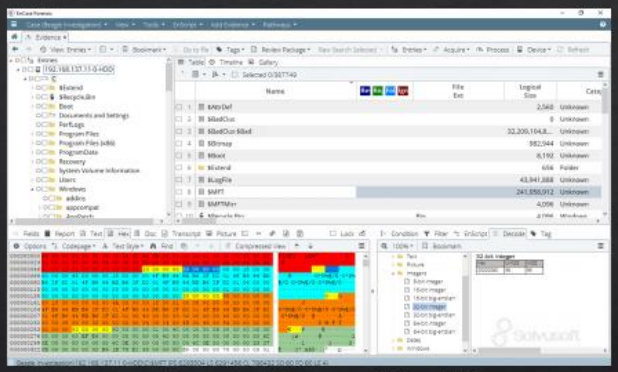

Відновлення даних

7

# Аналіз метаданих та комплексні платформи




Програмне забезпечення FOCA: аналіз метаданих



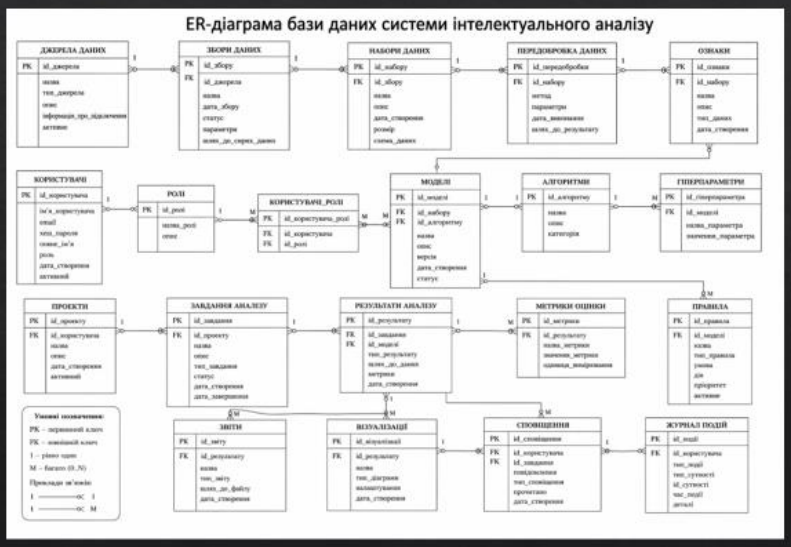
Програмне забезпечення EnCase/FTK: індексування, пошук, реконструкція подій

- метадані встановлюють часові межі та походження файлів;
- індексація дає швидкий пошук по ключових словах;
- візуалізація зв'язків спрощує аналіз великих масивів даних.

8

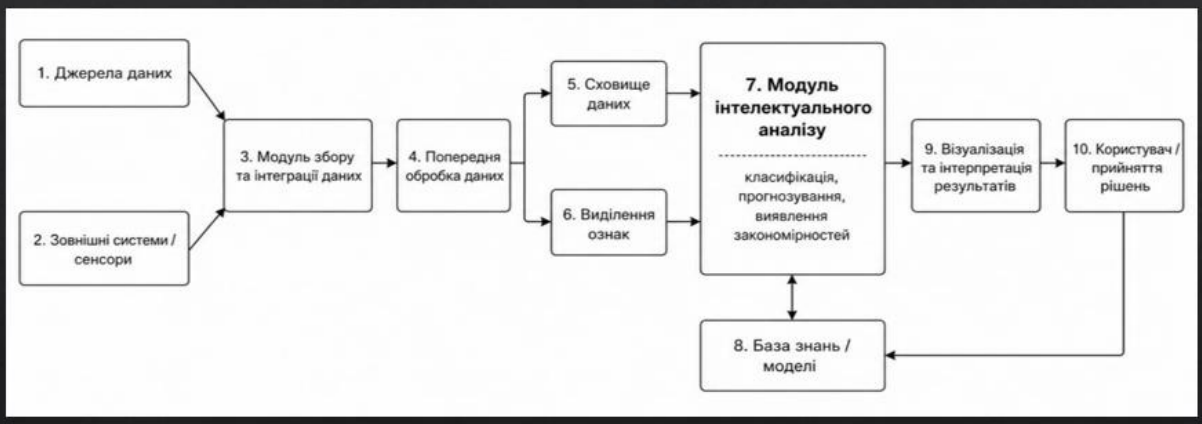
# Проектування бази даних

- основні сутності: носій, образ, файл, хеш, метадані, результат аналізу;
- зберігається не оригінальний доказ, а описові дані та посилання;
- структура БД підтримує відтворюваність і аудит дій експерта.






# Узагальнена архітектура системи інтелектуального аналізу



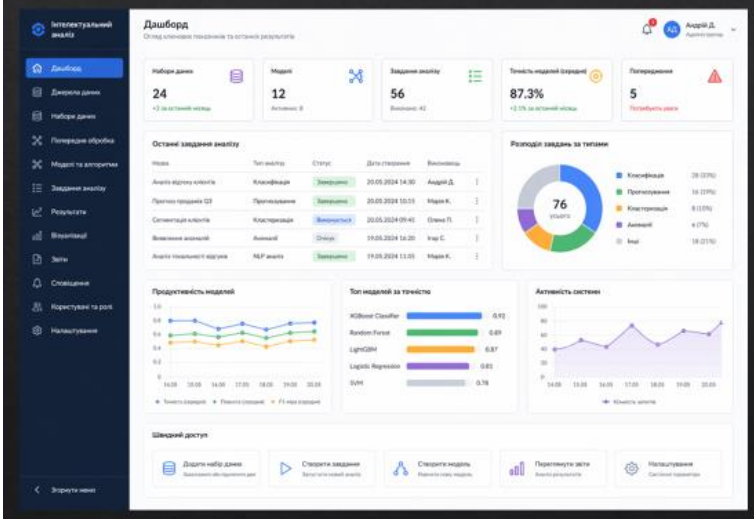

**Алгоритмічний конвеєр обробки**

# Попередня обробка та виділення ознак

- монтування образу у безпечному режимі «тільки читання»;
- обчислення хешів файлів та контроль дублювання;
- нормалізація метаданих і часових міток;
- векторизація ознак: тип файлу, розмір, ентропія, сигнатури, ключові слова, часові інтервали.


11

# Користувацький інтерфейс

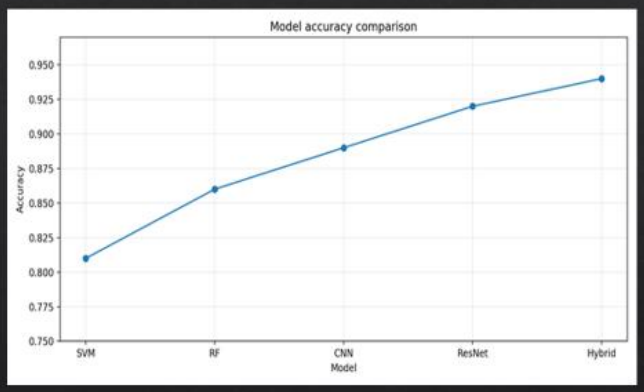



- перегляд завантажених образів та статусів аналізу;
- фільтрація артефактів за типом, датою, класом і рівнем ризику;
- виведення статистики й формування звіту для експерта;
- мінімізація ручних дій під час первинного аналізу.

12

# Тестування системи

- функціональне тестування модулів імпорту, хешування, витягнення ознак і формування звітів;
- перевірка стабільності на образах із різними файловими системами;
- оцінка швидкодії за часом індексації та кількістю оброблених файлів;
- перевірка коректності класифікації на контрольних наборах.




**Приклад графіка якості/збіжності**

13

# Захист та зберігання цифрових доказів

- • зберігання доказів має гарантувати конфіденційність, цілісність і доступність;
- • небезпечні або підозрілі файли аналізуються в ізольованому середовищі;
- • журналювання дій забезпечує доказовість результатів аналізу.

**Шифрування** | **Контроль доступу** | **Аудит дій** | **Резервування** | **Ізоляція коду**

14

# ВИСНОВКИ

Мета кваліфікаційної роботи була повністю досягнута. Для досягнення поставленої мети проекту було успішно реалізовано ряд завдань, які включали:

- застосування інтелектуального аналізу скорочує час первинного перегляду образів носіїв;
- поєднання хеш-контролю, журналювання та модульної архітектури забезпечує доказовість результатів;
- класифікація і кластеризація дозволяють швидко виділяти потенційно значущі артефакти;
- подальший розвиток доцільно спрямувати на розширення моделей ML і підтримку нових типів носіїв та хмарних джерел.

15

# ПУБЛІКАЦІЇ

Кондратюк Д.К. Система інтелектуального аналізу образів носіїв цифрових доказів. Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки : матеріали VI Міжнар. наук. конф. (м. Тернопіль, 2026). Тернопіль : ТНТУ, 2026. С. 145–147. URL: tntu.edu.ua (дата звернення: 26.04.2026).

16

# ДОДАТОК Б

(обов’язковий)

Публікація

Кондратюк Д.В. Система інтелектуального аналізу образів носіїв цифрових доказів. Воєнні конфлікти та техногенні катастрофи: історичні та психологічні наслідки : матеріали VI Міжнар. наук. конф. (м. Тернопіль, 2026). Тернопіль : ТНТУ, 2026. С. 145–147. URL: tntu.edu.ua (дата звернення: 26.04.2026).

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.

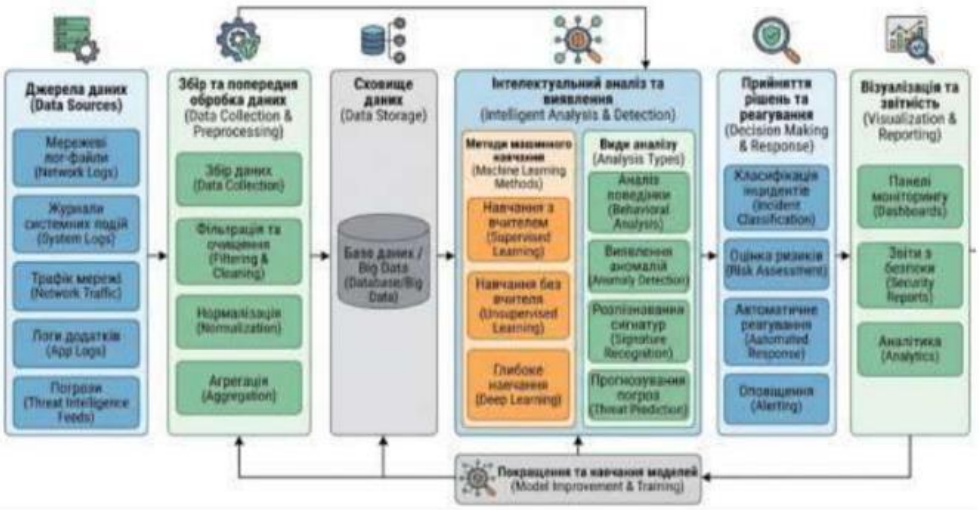



*Рис. 1 – Узагальнена архітектура системи інтелектуального аналізу образів носіїв цифрових доказів*

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.

# ДОДАТОК В

(обов'язковий)

Лістинг програмного забезпечення виявлення кібер-загроз в на основі еволюційних алгоритмів, цифрового підпису, шифрування, анонімізації персональних даних, контролю доступу, аудиту, ізольованого аналізу та сканування загроз

Формат пояснення: кожний логічний рядок коду подано окремо, а поруч описано його призначення, роль у програмі та важливі зауваження щодо роботи або можливих помилок.

1. Методи та засоби забезпечення кібербезпеки системи: хешування образів

```
import hashlib
from typing import Dict, List

class ForensicHasher:
    """Криптографічне хешування образів носіїв"""

    def __init__(self):
        self.algorithms = ['sha256', 'sha512', 'md5']

    def calculate_hashes(self, image_path: str,
                         block_size: int = 65536) -> Dict[str, str]:
        """Розрахунок множинних хеш-сум"""
        hashers = {alg: hashlib.new(alg) for alg in self.algorithms}

        with open(image_path, 'rb') as f:
            while chunk := f.read(block_size):
                for hasher in hashers.values():
                    hasher.update(chunk)

        return {alg: hashers[alg].hexdigest()
                for alg in self.algorithms}
```

```
    def verify_integrity(self, image_path: str,
                         expected_hashes: Dict[str, str]) -> bool:
        """Перевірка цілісності образу"""
        current_hashes = self.calculate_hashes(image_path)

        for alg in self.algorithms:
            if current_hashes[alg] != expected_hashes.get(alg):
                return False
        return True

    def calculate_piecewise_hash(self, image_path: str,
                                 piece_size: int = 4096) -> List[str]:
        """Розрахунок хешів по блоках для швидкої перевірки"""
        hashes = []

        with open(image_path, 'rb') as f:
            while piece := f.read(piece_size):
                hash_obj = hashlib.sha256(piece)
                hashes.append(hash_obj.hexdigest())

        return hashes
```

2. Електронний цифровий підпис: підписання образів і метаданих

```
from cryptography.hazmat.primitives import hashes, serialization
from cryptography.hazmat.primitives.asymmetric import rsa
from cryptography.hazmat.primitives import padding
import datetime
import json

class ForensicSigner:
    """Підписання образів та метаданих"""

    def __init__(self):
        self.private_key = rsa.generate_private_key(
            public_exponent=65537,
            key_size=4096
        )
```

```
        self.public_key = self.private_key.public_key()

    def sign_image_metadata(self, metadata: dict) -> bytes:
        """Підписання метаданих образу"""
        metadata['timestamp'] = datetime.utcnow().isoformat()
        message = json.dumps(metadata, sort_keys=True).encode()

        signature = self.private_key.sign(
            message,
            padding.PSS(
                mgf=padding.MGF1(hashes.SHA256()),
                salt_length=padding.PSS.MAX_LENGTH
            ),
            hashes.SHA256()
        )
        return signature

    def verify_signature(self, metadata: dict, signature: bytes) -> bool:
        """Перевірка підпису"""
        message = json.dumps(metadata, sort_keys=True).encode()

        try:
            self.public_key.verify(
                signature,
                message,
                padding.PSS(
                    mgf=padding.MGF1(hashes.SHA256()),
                    salt_length=padding.PSS.MAX_LENGTH
                ),
                hashes.SHA256()
            )
            return True
        except:
            return False
```

3. Захист конфіденційності: шифрування образів при зберіганні

```
from cryptography.fernet import Fernet
```

```
from cryptography.hazmat.primitives.kdf.pbkdf2 import PBKDF2HMAC
from cryptography.hazmat.primitives import hashes
import os
import base64

class ImageEncryption:
    """Шифрування образів носіїв"""

    def __init__(self, password: str):
        self.password = password.encode()
        self.salt = os.urandom(16)
        self.key = self._derive_key()
        self.cipher = Fernet(self.key)

    def _derive_key(self) -> bytes:
        """Деривація ключа з пароля"""
        kdf = PBKDF2HMAC(
            algorithm=hashes.SHA256(),
            length=32,
            salt=self.salt,
            iterations=100000,
        )
        key = base64.urlsafe_b64encode(kdf.derive(self.password))
        return key

    def encrypt_image(self, input_path: str, output_path: str,
                      chunk_size: int = 64*1024):
        """Шифрування образу по блоках"""
        with open(input_path, 'rb') as fin:
            with open(output_path, 'wb') as fout:
                # Записуємо salt
                fout.write(self.salt)

                while chunk := fin.read(chunk_size):
                    encrypted_chunk = self.cipher.encrypt(chunk)
                    # Записуємо розмір зашифрованого блоку
                    fout.write(len(encrypted_chunk).to_bytes(4, 'big'))
```

```
                        fout.write(encrypted_chunk)

        def decrypt_image(self, input_path: str, output_path: str):
            """Розшифрування образу"""
            with open(input_path, 'rb') as fin:
                salt = fin.read(16)

                with open(output_path, 'wb') as fout:
                    while True:
                        chunk_size_bytes = fin.read(4)
                        if not chunk_size_bytes:
                            break
                        chunk_size = int.from_bytes(chunk_size_bytes, 'big')
                        encrypted_chunk = fin.read(chunk_size)
                        decrypted_chunk = self.cipher.decrypt(encrypted_chunk)
                        fout.write(decrypted_chunk)
```

4. Захист конфіденційності: анонімізація персональних даних

```
import re
from typing import List, Dict
import hashlib

class PIIAnonymizer:
    """Анонімізація персональних даних в образах"""

    def __init__(self):
        self.patterns = {
            'email': r'[A-Za-z0-9._%+-]+@[A-Za-z0-9.-]+\.[A-Z|a-z]{2,}',
            'phone':      r'\+?\d{1,3}?[-.\s]?\(?\d{1,4}?\)?[-.\s]?\d{1,4}[-
.\s]?\d{1,9}',
            'ssn': r'\b\d{3}[-.]?\d{2}[-.]?\d{4}\b',
            'credit-card': r'\b\d{4}[-.\s]?\d{4}[-.\s]?\d{4}[-.\s]?\d{4}\b'
        }

    def anonymize_text(self, text: str, replacement_type: str = 'hash') ->
str:
        """Анонімізація тексту"""
```

```
        result = text

        for pii_type, pattern in self.patterns.items():
            matches = re.finditer(pattern, result)
            for match in matches:
                original = match.group()

                if replacement_type == 'hash':
                    replacement = self._hash_pii(original, pii_type)
                elif replacement_type == 'mask':
                    replacement = self._mask_pii(original, pii_type)
                else:
                    replacement = f'[REDACTED_{pii_type.upper()}]'

                result = result.replace(original, replacement)

        return result

    def _hash_pii(self, value: str, pii_type: str) -> str:
        """Хешування PII для збереження унікальності"""
        hash_obj = hashlib.sha256(value.encode())
        return f'{{{pii_type.upper()}_{hash_obj.hexdigest()[:8]}}}'

    def _mask_pii(self, value: str, pii_type: str) -> str:
        """Маскування PII"""
        if pii_type == 'email':
            parts = value.split('@')
            return f'{parts[0][:2]}***@{parts[1]}'
        elif pii_type == 'phone':
            return f'+***-***-****{value[-4:]}'
        elif pii_type == 'credit-card':
            return f'****-****-****-{value[-4:]}'
        return '****'
```

5. Система контролю доступу

```
from enum import Enum
from typing import Set, Dict, List
```

```
from datetime import datetime
import sqlite3

class Permission(Enum):
    CREATE_IMAGE = "create_image"
    READ_IMAGE = "read_image"
    ANALYZE_IMAGE = "analyze_image"
    DELETE_IMAGE = "delete_image"
    EXPORT_RESULTS = "export_results"
    MANAGE_USERS = "manage_users"
    VIEW_AUDIT = "view_audit"

class Role(Enum):
    ANALYST = "analyst"
    SENIOR_ANALYST = "senior_analyst"
    ADMINISTRATOR = "administrator"
    AUDITOR = "auditor"

class AccessControl:
    """Система контролю доступу"""

    def __init__(self, db_path: str):
        self.db_path = db_path
        self.role_permissions = self._define_role_permissions()
        self._init_database()

    def _define_role_permissions(self) -> Dict[Role, Set[Permission]]:
        return {
            Role.ANALYST: {
                Permission.READ_IMAGE,
                Permission.ANALYZE_IMAGE
            },
            Role.SENIOR_ANALYST: {
                Permission.CREATE_IMAGE,
                Permission.READ_IMAGE,
                Permission.ANALYZE_IMAGE,
                Permission.EXPORT_RESULTS
```

```
                },
                Role.ADMINISTRATOR: set(Permission),
                Role.AUDITOR: {
                    Permission.READ_IMAGE,
                    Permission.VIEW_AUDIT
                }
            }

        def check_permission(self, user_id: str, permission: Permission) -> bool:
            """Перевірка дозволу користувача"""
            user_roles = self._get_user_roles(user_id)

            for role in user_roles:
                if permission in self.role_permissions.get(role, set()):
                    self._log_access(user_id, permission, True)
                    return True

            self._log_access(user_id, permission, False)
            return False

        def _log_access(self, user_id: str, permission: Permission, granted:
bool):
            """Логування спроб доступу"""
            with sqlite3.connect(self.db_path) as conn:
                conn.execute("""
                    INSERT INTO access_log
                    (user_id, permission, granted, timestamp)
                    VALUES (?, ?, ?, ?)
                """, (user_id, permission.value, granted,
datetime.utcnow().isoformat()))
```

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

# РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ МАГІСТРА

Здобувач: Кондратюк Даніїл Вікторович _____

Тема: Метод та система інтелектуального аналізу образів носіїв цифрових доказів

Спеціальність: 123 «Комп'ютерна інженерія»

Обсяг кваліфікаційної роботи магістра:

Кількість листів креслень ___; кількість сторінок записки ___

1. Короткий зміст роботи та прийнятих рішень Представлена кваліфікаційна робота магістра присвячена розробці методів та програмно-апаратної системи для інтелектуального аналізу образів носіїв цифрових доказів з акцентом на забезпечення кібербезпеки та захисту інформації. Тема роботи є актуальною та відповідає сучасним потребам у галузі цифрової криміналістики, інформаційної безпеки та судової експертизи комп'ютерних систем.

2. Висновок про відповідність роботи дипломному завданню.

Кваліфікаційна робота магістра повністю відповідає виданому завданню.

3. Характеристика виконання кожного розділу, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі проведено огляд сучасного стану проблематики аналізу цифрових доказів у контексті інформаційної безпеки. У другому розділі здобувач коректно формалізував задачу аналізу з використанням математичного моделювання та аналізу, розробці методу інтелектуального аналізу образів носіїв, проте в розділі недостатньо уваги приділено питанням впровадженню результатів роботи моделей глибокого навчання. У третьому розділі запропоновано метод описує проектування та реалізацію системи інтелектуального аналізу. У четвертому розділі запропоновано порівняльному аналізу методів захисту та зберігання цифрових доказів і є найбільш оригінальним внеском здобувача.

4. Позитивні сторони роботи: Запропонована система інтелектуального аналізу образів носіїв цифрових доказів демонструє комплексний підхід до вирішення актуальної проблеми. На відміну від існуючих рішень, що зосереджуються на

окремих аспектах криміналістичного аналізу або захисту даних, здобувач інтегрував обидва напрямки в єдину кіберфізичну систему.

5. Негативні сторони роботи: Перелік використаних джерел міг би бути ширшим. У роботі переважають посилання на технічну документацію та онлайн-ресурси, тоді як бракує посилань на наукові статті з провідних конференцій та журналів у галузі цифрової криміналістики та інформаційної безпеки та комп'ютерних наук. Також у роботі бракує розділу, присвяченого обмеженням розробленої системи та напрямкам подальших досліджень.

6. Оцінка графічного оформлення та пояснювальної записки роботи: –

7. Відгук про роботу в цілому: В загальному робота виконана на достатньому рівні.

8. Інші зауваження: –

9. Оцінка кваліфікаційної роботи магістра:

Розглянувши позитивні та негативні сторони представленої кваліфікаційної роботи магістра вважаю, що робота заслуговує оцінки «добре» 75 С

Рецензент (прізвище, ім'я, по батькові, посада, місце роботи) Барлюк Олександр Валентинович, д.т.н., проф., зав. каф. КН ХНУ

"5 травня" 2026р.

Зав. кафедри КІС
д-р. філософії Ользі ПАВЛОВІЙ

Даніїл КОНДРАТЮК
ПІБ здобувача вищої освіти

ФІТ, 4 курсу, групи КІ2м-24-2

ЗАЯВА

З правилами чинного Положення про систему забезпечення академічної доброчесності у Хмельницькому національному університеті, згідно з яким виявлення академічного плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту і застосування заходів академічної відповідальності, ознайомлений (а). Про використання спеціалізованих програмних засобів (СПЗ) StrikePlagiarism та Anti-Plagiarism для перевірки кваліфікаційних робіт здобувачів вищої освіти на наявність академічного плагіату оповіщений (а). Надаю університету право на передачу моєї роботи для обробки та збереження в базах даних СПЗ і використання роботи для виявлення академічного плагіату в інших роботах, які перевіряються СПЗ.

Також надаю свою згоду на обробку й збереження університетом моєї роботи в Інституційному репозитарії Хмельницького національного університету.

Робота надається для перевірки в електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

15 травня 2026 року

# РІШЕННЯ ЕКСПЕРТНОЇ КОМІСІЇ

## КАФЕДРИ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ ТА ІНФОРМАЦІЙНИХ СИСТЕМ ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Назва кваліфікаційної роботи Метод та система інтелектуального аналізу образів носіїв цифрових доказів
Автор Даніїл КОНДРАТЮК
Освітня програма Інформаційні системи та технології
Рівень вищої освіти другий (магістерський)
Спеціальність 123 Комп'ютерна інженерія
Науковий керівник: к.т.н., доцент Катерина БЕРЕЗЬКА

На основі аналізу кваліфікаційної роботи на дотримання вимог академічної доброчесності (у т.ч. відсутності ознак академічного плагіату) з урахуванням результатів перевірки роботи спеціалізованим програмним засобом(ами) комісія зробила такий висновок:

| № | Висновок | Позначка про відповідність |
|---|---|---|
| 1 | Ознаки академічного плагіату | |
| 1.1 | Запозичення, виявлені в роботі, є законними і не є академічним плагіатом (далі – зазначаються підстави віднесення запозичень до правомірних, якщо потрібно). Робота приймається до захисту. | відповідає |
| 1.2 | Виявлені запозичення не є академічним плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи (далі – зазначаються детальні та аргументовані підстави віднесення запозичень до правомірних). Робота приймається до захисту, але має бути відкоригована. | |
| 1.3 | Виявлені запозичення не є академічним плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. Робота може бути допущена до захисту після того як буде відкоригована та доопрацьована і успішно пройде повторну перевірку на академічний плагіат. | |
| 1.4 | Робота містить навмисні текстові спотворення, передбачувані спроби укриття текстових запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту. | |
| 2 | Інші види порушень академічної доброчесності | |

Підтвердження:

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1) усі запозичення фрагментарні, або мають належним чином оформленні посилання;

2) окремі виявлені збіги є загальновживаними фразами або виразами, про що свідчить посилання системи на збіг з джерелами на один фрагмент речення;

3) всі зафіксовані системою ознаки модифікації тексту відносяться до комбінування латинських символів зі україномовними скороченнями індексів в формулах, що не є модифікацією тексту.

4) значна частина знайденого плагіату відноситься до списку використаних джерел

Сумарний обсяг всіх запозичень, визначений системою виявлення збігів/ ідентичності/схожості StrikePlagiarism, складає 3.98% і адресується до 80 першоджерела; та системою Anti-Plagiarism складає 32.0%, що, з урахуванням наведених обґрунтувань, відповідає характеру наукового дослідження і свідчить на користь кваліфікаційної роботи.

15.12.2025

Завідувач кафедри _____ Ольга ПАВЛОВА
Підпис Ім'я, ПРІЗВИЩЕ

Гарант освітньої програми _____ Олег САВЕНКО
Підпис Ім'я, ПРІЗВИЩЕ

Керівник кваліфікаційної роботи _____ Катерина БЕРЕЗЬКА
Підпис Ім'я, ПРІЗВИЩЕ

**Протокол аналізу звіту подібності експертом**

Заявляю, що я ознайомився (-лась) з Повним звітом подібності, який був згенерований Системою виявлення і запобігання плагіату щодо роботи:

**Автор:** Даніїл КОНДРАТЮК

**Співавтор:**

**Назва:** 8Магістерська_дипломна_робота_Кондратюк_Д_В_КІ2м_24_2_–_плагіат

**Експерт:** Катерина БЕРЕЗЬКА

**Підрозділ:** Кафедра комп'ютерної інженерії та інформаційних систем

**Коефіцієнт подібності 1:**3.98%

**Коефіцієнт подібності 2:**1.79%

**Мікропробіли:** 11

**Заміна букв:** 4

**Інтервали:** 0

**Білі знаки:** 6

**Дата створення звіту:** 2026-05-06 07:24:04.0

**Після аналізу Звіту подібності констатую наступне:**

☒ **Запозичення, виявлені в роботі є законними і не є плагіатом. Рівень подібності не перевищує допустимої межі. Таким чином робота незалежна і приймається.**

☐ **Запозичення не є плагіатом, але перевищено граничне значення рівня подібностей. Таким чином робота повертається на доопрацювання.**

☐ **Виявлено запозичення і плагіат або навмисні текстові спотворення (маніпуляції), як передбачувані спроби укриття плагіату, які роблять роботу невідповідною вимогам законодавства (Ст. 32. ЗУ Про вищу освіту, пункт 3.1, Ст. 42. ЗУ Про освіту) та вимог НАЗЯВО (Критерій 5), а також кодексу етики і процедурам. Таким чином робота не приймається.**

Обгрунтування:

2026-05-06 Доцент Андрій Нічепорук

*Дата* експерт

Wed May 06 08:06:48 EEST 2026, Медзатий Дмитро Миколайович, Хмельницький національний університет, ХНУ

# Anti-Plagiarism (http://ap.km.ua) v-15.701

**Максимальне співпадіння з одним документом 32.0%**

Словники перевірки: en_US, ru_RU, ua_UA. **Помилок в документах: 9%**

| | Документ | | Сумарний збіг по Базі Даних | |
|---|---|---|---|---|
| ID: 271056<br>Назва: МКР Метод та система інтелектуального аналізу образів носіїв цифрових доказів<br>Додано в БД: 2026-05-06<br>Автора: Даніїл КОНДРАТЮК<br>Керівники: Катерина БЕРЕЗЬКА<br>Консультанти:<br>Опоненти: | Символи | Лексеми | Символи | Лексеми |
| | 121845 | 837 | 42540 (35%) | 261 (31%) |

Джерело плагіату

| ID | Опис | Наявність плагіату в документі | |
|---|---|---|---|
| | | Символи | Лексеми |
| 269895 | Назва: Звіт з НДП Метод та система інтелектуального аналізу образів носіїв цифрових доказів (Digtal Forenssic Imaging Analysis<br>Додано в БД: 2026-03-21<br>Автора: Кондратюк Д.В.<br>Керівники: Павлову О.О<br>Консультанти:<br>Опоненти: | 39130 (32.0%) | 257 (31.0%) |