УДК 343.982.41
https://doi.org/10.33994/kndise.2026.71.31

Юзишина Тетяна В'ячеславівна

провідний судовий експерт сектору криміналістичних та інженерно-технічних досліджень лабораторії криміналістичних, інженерно-технічних та військових досліджень Науково-дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України
https://orcid.org/0009-0005-7391-0413
uzyshina@gmail.com

Мірошник Руслан Олександрович

судовий експерт лабораторії досліджень об'єктів інформаційних технологій Науково-дослідного центру судової експертизи у сфері інформаційних технологій та інтелектуальної власності Міністерства юстиції України
https://orcid.org/0009-0004-8504-0489
ruslan_miroshnik@ukr.net

Бібліографічний опис статті: Юзишина Т.В., Мірошник Р.О. (2026). Комплексний підхід до виявлення монтажу в електронних і гібридних документах. *Криміналістика і судова експертиза, 71, 476-498*. doi: https://doi.org/10.33994/kndise.2026.71.31

КОМПЛЕКСНИЙ ПІДХІД ДО ВИЯВЛЕННЯ МОНТАЖУ В ЕЛЕКТРОННИХ І ГІБРИДНИХ ДОКУМЕНТАХ

В сучасних умовах завдяки розвитку технологій, електронні документи широко використовуються в різних сферах. Одним із найбільш поширених форматів електронних документів є формат PDF (Portable Document Format), який застосовується для створення, зберігання та передачі документів у незмінному вигляді. Водночас використання сучасних програмних засобів редагування електронних документів створює можливості для їх фальсифікації, зокрема шляхом монтажу текстових фрагментів, зміни реквізитів або їх додавання/зміни перед друком документа. У статті розглянуто питання виявлення монтажу в електронних і гібридних документах у контексті комплексного підходу шляхом проведення технічної експертизи документів та комп'ютерно-технічної експертизи. Особливу увагу

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

приділено дослідженню PDF-файлів як одного з найбільш поширених форматів електронних документів, що використовуються у сучасному документообігу. Проаналізовано можливості встановлення змін тексту, вставлення або зміна окремих реквізитів або графічних елементів документа, здійснених у цифровому середовищі перед його друком. **Метою дослідження** є аналіз сучасних підходів до виявлення монтажу в електронних і гібридних документах із застосуванням методів технічної експертизи документів та комп'ютерно-технічної експертизи. **Методологічну основу дослідження** становлять методи аналізу, узагальнення та криміналістичного дослідження документів, зокрема, аналіз графічних характеристик тексту, структури документа та метаданих електронних файлів. У роботі визначено характерні ознаки монтажу, що можуть бути встановлені під час дослідження як електронного PDF-файлу, так і паперового примірника документа. **Висновки.** Доведено, що комплексне використання методів комп'ютерно-технічної експертизи та технічної експертизи документів дає змогу ефективно встановлювати факти внесення змін до документа перед його друком та підвищує обґрунтованість експертних висновків.

Ключові слова: технічна експертиза документів; комп'ютерно-технічна експертиза; електронні документи; PDF-файли; монтаж.

Yuzyshina Tetyana

leading forensic expert of the forensic and engineering-technical research sector of the forensic, engineering-technical and military research laboratory of the Forensic Research Center in the field of information technology and intellectual property of the Ministry of Justice of Ukraine
https://orcid.org/0009-0005-7391-0413
uzyshina@gmail.com

Miroshnyk Ruslan

forensic expert of the research laboratory of information technology objects of the Scientific Research Center of Forensic Expertise in the field of information technology and intellectual property of the Ministry of Justice of Ukraine
https://orcid.org/0009-0004-8504-0489
ruslan_miroshnika@ukr.net

COMPREHENSIVE APPROACH TO DISCOVERING ASSEMBLY IN ELECTRONIC AND HYBRID DOCUMENTS

To cite this article: Yuzyshina T., Miroshnyk R. (2026). Kompleksnyi pidkhid do vyiavlennia montazhu v elektronnykh i hibrydnykh doku-

mentakh [A comprehensive approach to detecting montage in electronic and hybrid documents]. *Criminalistics and Forensics, 71, 476-498*. doi: https://doi.org/10.33994/kndise.2026.71.31

In the current context of rapid technological advancement, electronic documents are widely used across various domains. One of the most common formats of electronic documents is the PDF (Portable Document Format), which is utilized for creating, storing, and transmitting documents in a fixed-layout form. At the same time, the use of modern software tools for editing electronic documents creates opportunities for their falsification, in particular through document montage, including the insertion of textual fragments, alteration of document requisites, or their addition/modification prior to printing. This article addresses the detection of document montage in electronic and hybrid documents within the framework of a comprehensive approach involving both forensic document examination and computer forensic examination. Particular attention is paid to the examination of PDF files as one of the most widely used formats in contemporary document workflow. The study analyzes the possibilities of identifying text alterations, insertion or modification of individual requisites, and changes to graphical elements carried out in the digital environment prior to printing. **The purpose of the study** is to analyze contemporary approaches to the detection of document montage in electronic and hybrid documents through the application of methods of forensic document examination and computer forensic examination. **The methodological basis** of the research includes methods of analysis, generalization, and forensic examination of documents, in particular the analysis of graphical characteristics of text, document structure, and metadata of electronic files. The study identifies characteristic indicators of document montage that can be established both in the electronic PDF file and in the printed hard copy of the document. **The conclusions.** It is demonstrated that the combined application of computer forensic and forensic document examination methods enables effective detection of alterations introduced into a document prior to printing and enhances the evidential value and reliability of expert conclusions.

Keywords: forensic document examination; computer forensic examination; electronic documents; PDF files; document montage.

Постановка проблеми

Сучасний розвиток інформаційних технологій спричинив значні зміни у сфері документообігу. Більшість документів створюється, редагується та передається в електронному вигляді. Одним із найбільш поширених форматів електронних документів є PDF, який дозволяє зберігати структуру документа незалежно від операційної системи або програмного забезпечення.

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

Разом із тим використання цифрових технологій створює нові можливості для фальсифікації документів. Зокрема, монтаж тексту або реквізитів може здійснюватися шляхом внесення змін до електронного файлу перед його друком. У результаті можуть виникати так звані *гібридні документи*, які створюються у цифровому середовищі, але використовуються у паперовій формі.

Виявлення таких фальсифікацій є складним завданням, що потребує використання як методів комп'ютерно-технічної експертизи, так і методів технічної експертизи документів. Саме поєднання цих підходів дозволяє встановити спосіб виготовлення документа та можливі зміни, внесені до його змісту [1].

Аналіз останніх досліджень і публікацій

В умовах дослідження електронних і гібридних документів важливого значення набуває правильне розуміння базових понять, визначених чинним законодавством України.

Відповідно до Закону України «Про електронні документи та електронний документообіг», електронний документ — це документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа [2].

Оригіналом електронного документа є електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним підписом автора або підписом, прирівняним до власноручного підпису відповідно до Закону України «Про електронну ідентифікацію та електронні довірчі послуги» [2].

Електронний документообіг визначається як сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів [2].

Наведені визначення є базовими для розуміння правової природи електронних документів та особливостей їх функціонування.

Проблематика дослідження документів та встановлення фактів їх підроблення є одним з усталених напрямів експертних досліджень, висвітлених у розділі криміналістики «Криміналістична техніка» як її окрема підгалузь – «Криміналістичне документознавство». У межах цього напряму особливе місце посідає технічна експертиза документів, яка спрямована на встановлення способу виготовлення документа, виявлення змін у його змісті, а також визначення послідовності нанесення окремих реквізитів [3; 10].

У працях українських учених-криміналістів значну увагу приділено питанням дослідження документів як джерел доказової інформації. Так, В. Ю. Шепітько зазначає, що технічна експертиза документів охоплює широкий спектр дослідницьких завдань, серед яких важливе місце займає встановлення способу виготовлення

документа, визначення технічних засобів, використаних для його створення, а також виявлення змін, внесених до первинного змісту документа [3].

В. Т. Білоус підкреслює, що дослідження документів у криміналістиці повинно здійснюватися з урахуванням як матеріальних, так і інформаційних характеристик документа. На думку дослідника, документ слід розглядати як складну систему, що поєднує текстову інформацію, графічні елементи та матеріальний носій [4].

Питання технічної експертизи документів детально розглядаються у працях Н. І. Клименко, яка зазначає, що основними завданнями технічної експертизи документів є встановлення способу виготовлення документа, виявлення підробок, а також дослідження змін, внесених до документа після його створення [5; 9]. У своїх дослідженнях автор підкреслює, що сучасні способи підроблення документів часто пов'язані із використанням цифрових технологій.

З розвитком електронного документообігу значно зросла кількість документів, створених у цифровому середовищі. У зв'язку з цим у криміналістиці сформувався новий напрям досліджень, пов'язаний із вивченням електронних документів та цифрових доказів. У таких випадках об'єктом дослідження можуть бути не лише паперові примірники документів, але й електронні файли, у яких зберігається первинна інформація про документ.

Зокрема, у сучасних дослідженнях значна увага приділяється аналізу електронних документів у форматі PDF, який широко використовується у діловому та юридичному документообігу. Як зазначають дослідники, PDF-файли мають складну внутрішню структуру, що містить різні об'єкти, зокрема текстові елементи, графічні об'єкти, шрифти та метадані [6].

Метадані документа можуть містити важливу інформацію про автора документа, дату його створення, програмне забезпечення, за допомогою якого було створено або змінено файл. Аналіз таких даних дозволяє встановити обставини створення документа та виявити можливі ознаки його редагування.

У дослідженнях з цифрової криміналістики також підкреслюється, що встановлення фактів монтажу в електронних документах часто потребує комплексного аналізу як електронного файлу, так і паперового примірника документа [7]. Такий підхід дозволяє зіставити результати дослідження цифрових характеристик документа з результатами дослідження його матеріального носія.

Разом із тим у сучасній експертній практиці особливу актуальність набуває дослідження так званих *гібридних документів*, які створюються у цифровому середовищі, але використовуються у паперовій формі після їх друку. У таких випадках монтаж може здійснюватися шляхом внесення змін до електронного файлу перед його друком.

У працях, присвячених проблемам комп'ютерно-технічної екс-

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

пертизи, зазначається, що виявлення монтажу у PDF-документах може здійснюватися шляхом аналізу структури файлу, дослідження метаданих та порівняння параметрів текстових об'єктів документа [8].

Таким чином, аналіз наукових джерел свідчить про те, що дослідження монтажу в електронних і гібридних документах потребує комплексного використання методів технічної експертизи документів та комп'ютерно-технічної експертизи. Поєднання цих підходів дозволяє більш ефективно встановлювати факти внесення змін до документів та визначати спосіб їх підроблення.

Мета дослідження

Метою дослідження є аналіз можливостей виявлення монтажу в електронних і гібридних документах із застосуванням методів технічної експертизи документів у поєднанні з підходами комп'ютерно-технічної експертизи. Основну увагу приділено встановленню ознак внесення змін до електронних документів, зокрема у форматі PDF, які могли бути здійснені у цифровому середовищі до моменту їх друку, а також визначенню можливостей виявлення таких змін під час дослідження паперових примірників документів.

Дослідження спрямоване на визначення характерних ознак монтажу, що можуть проявлятися у структурі електронного документа, його метаданих та графічних характеристиках тексту, а також на встановлення можливостей їх виявлення за допомогою методів технічної експертизи документів та комп'ютерно-технічної експертизи. Особлива увага приділяється поєднанню інструментів комп'ютерно-технічної експертизи з традиційними криміналістичними методами дослідження документів, які застосовуються під час судово-експертного дослідження.

Методологічною основою дослідження є комплексний підхід, що поєднує загальні положення криміналістики, технічної експертизи документів та комп'ютерно-технічної експертизи.

У процесі дослідження використано загальнонаукові та спеціальні методи. До загальнонаукових методів належать аналіз, синтез, узагальнення та порівняння, які застосовувалися для опрацювання наукових джерел, систематизації підходів до дослідження електронних документів та формування теоретичних висновків.

Серед спеціальних методів використано методи технічної експертизи документів, спрямовані на дослідження графічних характеристик тексту, виявлення ознак внесення змін у паперових примірниках документів, а також методи комп'ютерно-технічної експертизи, що передбачають аналіз структури електронних файлів, дослідження метаданих та встановлення ознак модифікації документів у цифровому середовищі.

Окрему увагу приділено інструментальним методам досліджен-

ня PDF-документів, зокрема із застосуванням спеціалізованого програмного забезпечення для аналізу метаданих, структури файлів та графічного вмісту. Це дозволило виявити характерні ознаки монтажу та встановити можливі способи внесення змін до документів.

Виклад основного матеріалу

Особливості створення електронних та гібридних документів. Сучасний документообіг характеризується активним використанням електронних документів, які створюються за допомогою різних програмних засобів. Найбільш поширеними серед них є текстові редактори, системи електронного документообігу, а також програмне забезпечення для створення та редагування PDF-файлів.

У більшості випадків документ створюється у текстовому редакторі (наприклад, Microsoft Word або аналогічних програмах), після чого експортується у формат PDF для подальшого використання або передачі. Такий формат забезпечує збереження структури документа незалежно від програмного забезпечення та операційної системи.

Разом із тим можливість редагування PDF-документів за допомогою спеціалізованих програм дозволяє вносити зміни до документа після його створення. У таких випадках можуть змінюватися окремі текстові фрагменти, реквізити документа або графічні елементи.

У результаті виникають так звані *гібридні документи*, які створюються у цифровому середовищі, але використовуються у паперовій формі після їх друку. Особливістю таких документів є поєднання ознак електронного документа та матеріального носія інформації.

Під час технічної експертизи документів такі об'єкти розглядаються з урахуванням як цифрових характеристик документа, так і ознак його паперового примірника.

Типові способи монтажу в електронних файлах формату PDF. Монтаж в електронних документах може здійснюватися різними способами залежно від програмного забезпечення, яке використовується для редагування документа.

Найбільш поширеними способами фальсифікації документів є:

- редагування тексту документа;
- вставлення графічних елементів;
- заміна окремих сторінок документа;
- додавання реквізитів документа після його створення.

Основні способи монтажу у PDF-документах та їх характеристика наведені нижче у таблиці 1.

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

Таблиця 1. Основні способи монтажу у PDF-документах та їх характеристика

Спосіб	**Характеристика**
редагування тексту	зміна змісту документа
вставлення графічних елементів	додавання підписів або печаток
комбінування сторінок	формування документа з різних джерел
вставлення реквізитів	додавання фрагментів іншого документа

У практиці технічної експертизи документів подібні способи монтажу можуть проявлятися у вигляді різних ознак, які виявляються під час дослідження паперового примірника документа.

Зокрема, можуть спостерігатися розбіжності шрифтів; розбіжності у товщині штрихів і мікроструктурі літер та знаків; порушення інтервалів між словами та літерами; порушення розташування рядків (нахил, викривлення); змістова та логічна неузгодженість реквізитів тексту.

Такі ознаки можуть свідчити про внесення змін у документ шляхом монтажу його окремих елементів.

У практиці комп'ютерно-технічної експертизи, дослідження PDF-файлів для виявлення слідів цифрового втручання фокусується на методах верифікації цілісності документа, аналізі його структури на предмет аномалій та інтерпретації метаданих.

Ключові аспекти, що підлягають розгляду:

Ідентифікація. Встановлення програмного забезпечення та пристроїв, на яких було створено або модифіковано документ.

Хронологія змін. Аналіз механізму інкрементальних оновлень для відтворення попередніх версій документа.

Автентифікація. Виявлення ознак монтажу, підміни сторінок або зміни реквізитів документа.

Кібербезпека. Виявлення прихованого шкідливого функціоналу (експлойтів), що використовують вразливості PDF-рідерів.

Аналіз структури PDF-файлів.

PDF-файли мають складну внутрішню структуру, яка складається з різних типів об'єктів. З технічної точки зору, це складний контейнер, здатний містити не лише текст і графіку, а й мультимедійні об'єкти, метадані, сценарії (JavaScript), вкладені файли та цифрові підписи. Така структура, з одного боку, відкриває широкі можливості для зловмисників (приховування інформації, монтаж, вбудовування шкідливого коду), а з іншого – вимагає від судового експерта застосування специфічного інструментарію та глибокого розуміння специфікацій формату (зокрема стандарту ISO 32000).

Електронні файли формату PDF (Portable Document Format) слід розглядати не як лінійний потік даних (як, наприклад, текстовий файл .txt), а як ієрархічну об'єктно-орієнтовану базу даних. Згідно зі специфікацією ISO 32000, PDF базується на форматі COS (Carousel Object System), який забезпечує незалежність відображення доку-

мента від апаратного та програмного забезпечення.

Критично важливим є розрізнення двох рівнів представлення файлу: фізична структура: як байти організовані у файлі на диску; логічна структура: як об'єкти пов'язані між собою для формування сторінок, навігації та контенту.

Фізична структура PDF-файлу складається з чотирьох обов'язкових секцій, розміщених послідовно: заголовок (Header), тіло (Body) (містить об'єкти: текст, зображення, шрифти, метадані), таблиця перехресних посилань (Cross-Reference Table - xref) та кінцівка (Trailer). Порушення цієї послідовності або наявність аномалій у ній є першою ознакою можливої модифікації або пошкодження файлу [12]. Структура PDF-файлу наведена на рис. 1.

Рис. 1. Структура PDF-файлу

Заголовок (Header) – це перший рядок файлу, який ідентифікує формат та версію специфікації.

- *Синтаксис:* %PDF-1.x (де x – номер версії, наприклад, 1.7).
- *Експертне значення:* Дозволяє визначити, які функціональні можливості підтримуються документом. Якщо у заголовку вказана стара версія, а файл містить об'єкти новішої специфікації, це може свідчити про штучну зміну заголовка (спуфінг версії) для обходу систем безпеки [13].

Тіло файлу (Body) – найбільша частина файлу, що містить набір непрямих об'єктів (Indirect Objects), які формують зміст документа (шрифти, зображення, текст, сценарії).

- *Синтаксис.* Об'єкти розміщуються між ключовими словами obj та endobj.
- *Особливість.* Об'єкти у тілі можуть бути розміщені у довільному порядку. Їхня послідовність не впливає на порядок відображення сторінок [13].

Таблиця перехресних посилань (Cross-Reference Table, або xref) – це «мапа» файлу. Вона містить інформацію про байтове зміщення

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

(offset) кожного об'єкта відносно початку файлу.

◆ *Функція.* Дозволяє програмі-переглядачу швидко знаходити потрібні дані без читання всього файлу.

◆ *Експертне значення.* Аналіз xref дозволяє виявити дані, які фізично присутні у тілі файлу, але на які немає посилань у таблиці. Такі об'єкти часто використовуються зловмисниками для приховування шкідливого коду або секретної інформації (стеганографія) [13].

Трейлер (Trailer) – завершальна частина файлу, яка дозволяє програмі почати обробку документа. Вона містить посилання на таблицю xref та кореневий об'єкт (/Root).

◆ *Ключові елементи:*

/Root. Вказує на каталог документа (Document Catalog).

/ID. Унікальний ідентифікатор файлу (масив з двох хеш-сум), що дозволяє відстежувати оригінал та його модифікації.

Startxref. Вказує точне зміщення таблиці перехресних посилань.

%%EOF. Маркер кінця файлу [13].

Фізична структура PDF-файлу з інкрементальними оновленнями наведена на рис. 2.

Рис. 2. Фізична структура PDF-файлу з інкрементальними оновленнями

Аналіз метаданих PDF-документів. Окрему й надзвичайно важливу роль у структурі PDF відіграють метадані, які забезпечують контекстуальну інформацію про документ та його походження.

Метадані PDF-файлів – це службова інформація, що описує властивості документа, умови його створення, характеристики вмісту та параметри відтворення. Базові метадані традиційно зберігаються у словнику *Info Dictionary*, який містить текстові описи: дані про назву документа, автора, тему, ключові слова, дату створення (*CreationDate*), дату останньої модифікації (*ModDate*) та назву програмного забезпечення, що створило файл (*Producer*). Ці записи

закладаються автоматично під час формування файлу, однак їхній вміст може змінюватися вручну або сторонніми інструментами. Незважаючи на це, первинні відомості в *Info Dictionary* часто використовують як відправну точку для визначення програмного середовища, у якому створено документ, що має значення як у дослідницькому, так і в криміналістичному аналізі.

Сучасні стандарти PDF передбачають використання розширених метаданих у форматі XMP (Extensible Metadata Platform). Це структурований блок інформації на основі XML, який містить значно ширший набір дескрипторів, зокрема відомості про творця документа, формат, мову, історію редагування, технічні параметри файлу та використовувані ресурси. XMP-метадані інтегруються у PDF як окремий потоковий об'єкт. Завдяки цьому XMP стає універсальним механізмом документування життєвого циклу PDF-файлу.

Метадані також містять службову інформацію, що стосується шрифтів, кольорових профілів, інтерактивних елементів, цифрових підписів та особливостей відтворення сторінок. У стандартах PDF/A, спрямованих на довгострокове збереження електронних документів, значення метаданих є критичним, оскільки саме вони забезпечують можливість реконструкції контексту документа через тривалий термін незалежно від змін у програмному забезпеченні чи форматах зберігання. У таких випадках метадані виступають гарантом інтерпретованості документа та його відповідності архівним вимогам.

У сфері комп'ютерно-технічної експертизи метадані PDF мають особливе значення, оскільки нерідко відображають сліди редагування, використаних програм, часових позначок, невідповідностей між різними версіями документа та інших показників, що вказують на модифікації. Наприклад, розбіжність між датою створення у словнику *Info Dictionary* та часовими мітками об'єктів у структурі файлу може свідчити про маніпуляції. Наявність кількох наборів метаданих у XMP-блоках може вказувати на перекодування або повторне збереження документа різними застосунками. У сукупності ці відомості дозволяють формувати більш повну картину походження PDF-файлу, а також виявляти можливі сліди комп'ютерного монтажу [14].

Ознаки монтажу у технічній експертизі документів та комп'ютерно-технічній експертизі. Під час дослідження паперових примірників документів експерт може виявити різні ознаки, що свідчать про можливе редагування документа у цифровому середовищі [5;11].

До таких ознак належать:

- розбіжності шрифтів (кегля, гарнітури, пропорцій, форми та відображення мілких деталей елементів літер та знаків)
- розбіжності у товщині штрихів літер, знаків та їх елементів;
- розбіжності мікроструктури елементів літер та знаків;
- порушення інтервалів між словами, а також між літерами в словах;

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

- розташування ліній рядків під кутом відносно основного тексту, викривлення ліній рядків;
- відсутність логічного зв'язку між реквізитами документа;
- неузгодженість слів в однині та множині, порушення змістової цілісності тексту.

Виявлення таких ознак може свідчити про внесення змін у документ шляхом монтажу, зокрема редагування тексту, додавання або заміни окремих реквізитів.

Невід'ємною складовою сучасного методологічного інструментарію судової комп'ютерно-технічної експертизи PDF-файлів є використання консольних утиліт, таких як ExifTool, pdf-parser та pdfimages.

Застосування консольної утиліти ExifTool для аналізу метаданих PDF-документів. ExifTool – це кросплатформна бібліотека та консольна утиліта, призначена для читання, запису та редагування метаінформації. У контексті дослідження PDF-файлів, ExifTool є критично важливим інструментом для неруйнівного дослідження, оскільки дозволяє отримати доступ до службової інформації без відкриття файлу у візуальних редакторах, що мінімізує ризик випадкової зміни часових міток доступу. Основна цінність утиліти полягає у здатності зчитувати два паралельні потоки метаданих, які існують у PDF:

Класичні атрибути PDF (Info Dictionary). Стандартні поля (Author, Title, Created).

XMP (Extensible Metadata Platform). Метадані на основі XML, які часто містять історію редагування та детальнішу інформацію про програмне забезпечення.

Для проведення експертного дослідження рекомендується використовувати розширений режим виводу інформації. Базова команда для дослідження має наступний вигляд: «exiftool -a -u -g1 file.pdf».

Під час аналізу результатів роботи ExifTool необхідно звернути увагу на наступні групи атрибутів для виявлення ознак комп'ютерного монтажу.

Ідентифікація програмного забезпечення (Creator vs Producer):

Creator (або XMP: CreatorTool). Програма, в якій було створено оригінальний документ (наприклад, Microsoft Word).

Producer. Програма або бібліотека, яка здійснила конвертацію у формат PDF (наприклад, Microsoft Print to PDF або iText Library).

Ознака фальсифікації: Якщо в полі Producer зазначено бібліотеку для програмної генерації PDF (наприклад, iText, FPDF, JasperReports) у документі, що має виглядати як скан-копія, це свідчить про штучне створення файлу, а не сканування.

Хронологічний аналіз (Dates) ExifTool дозволяє порівняти дату створення та модифікації з точністю до секунди та часового поясу.

CreateDate. Дата первинної генерації файлу.

ModifyDate. Дата останньої зміни.

Ознака фальсифікації. Ситуація, коли CreateDate пізніша за ModifyDate або коли дата створення у блоці PDF Info відрізняється від дати у блоці XMP History.

Аналіз унікальних ідентифікаторів (DocumentID). Атрибут PDF: ID складається з двох частин: <OriginalID> та <ModifiedID>.У новоствореному файлі ці два значення ідентичні.

Якщо файл було відкрито та збережено (навіть без видимих змін), друге значення зміниться. Це дозволяє встановити факт перезбереження файлу після його створення.

Виявлення слідів "очищення" метаданих. Однією з технік є видалення метаданих. ExifTool дозволяє виявити це за непрямими ознаками:

Відсутність стандартних тегів Producer або Creator.

Наявність тегів PTEX (вказує на використання системи LaTeX) або специфічних тегів редакторів PDF (наприклад, GPL Ghostscript).

Невідповідність часу файлової системи (FileModifyDate) внутрішнім часовим міткам документа.

Утиліта pdf-parser є спеціалізованим інструментом для проведення статичного структурного аналізу PDF-документів, яка дозволяє працювати безпосередньо з об'єктною моделлю файлу (COS-структурою). Утиліта pdf-parser надає унікальну можливість оцінити архітектуру файлу на рівні його фізичної організації. На відміну від стандартних програм-переглядачів, які відображають лише фінальну (актуальну) версію документа, pdf-parser дозволяє виявити та проаналізувати всі попередні редакції файлу, базуючись на статистиці ключових структурних маркерів: таблиць перехресних посилань (xref), трейлерів (trailer) та точок входу (startxref). Первинним етапом дослідження є отримання зведеної статистики об'єктів. Співвідношення кількості маркерів xref, trailer та startxref є головним індикатором цілісності та історії редагування файлу.

Нормативна модель (Single Revision). У новоствореному або повністю перезаписаному файлі кожен із цих показників дорівнює 1. Це свідчить про лінійну структуру без збереженої історії змін.

Модель інкрементальних оновлень (Multiple Revisions). Наявність значень >1 (наприклад, 2, 3 і більше) є прямою ознакою того, що файл містить кілька версій. Кожен набір «xref + trailer» відповідає окремій сесії збереження документа.

Детальна характеристика досліджуваних елементів. Таблиця перехресних посилань (XREF). Це карта розміщення об'єктів усередині файлу. pdf-parser дозволяє аналізувати кожну таблицю окремо.

- *Експертне завдання:* Порівняння таблиць xref різних версій дозволяє встановити, які саме об'єкти були додані, змінені або помічені як «видалені» у процесі редагування документа.
- *Аномалії.* Якщо pdf-parser виявляє об'єкти, які фізично присутні у тілі файлу, але не згадуються в жодній таблиці xref, це може свідчити про спробу приховання інформації (стеганографія) або

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

про пошкодження файлу.

Трейлер (Trailer). Трейлер є критично важливим блоком, оскільки містить метадані про структуру файлової системи документа.

- *Ключ /Prev*. Головний об'єкт пошуку при наявності кількох трейлерів. Цей ключ містить зміщення (offset) попереднього трейлера. Його наявність підтверджує нерозривність ланцюжка змін.
- *Ключ /Root*. Вказує на каталог об'єктів. Зміна об'єкта /Root у новому трейлері може означати кардинальну зміну структури документа (наприклад, підміну сторінок).
- *Ключ /ID.* Масив ідентифікаторів. Порівняння ID у різних трейлерах одного файлу дозволяє підтвердити, що всі версії належать одному й тому ж документу.

Точка входу (Startxref) – це останній елемент, що зчитується рідером. Він вказує адресу останньої актуальної таблиці xref.

- *Експертне значення.* Якщо у файлі присутні дані після останнього маркера %%EOF (End of File), на який вказує startxref, це є класичною ознакою дописування шкідливого коду або прихованих даних, які ігноруються звичайними програмами, але виявляються при парсингу.

Застосування pdf-parser для аналізу тріади xref-trailer-startxref дозволяє не лише констатувати факт модифікації файлу, але й технічно обґрунтувати хронологію цих змін, відновити попередні редакції тексту та виявити спроби маніпуляції структурою документа, які неможливо помітити при візуальному огляді.

Утиліта pdfimages (входить до пакета poppler-utils або xpdf) є спеціалізованим інструментом для роботи з графічними об'єктами, інкапсульованими в PDF-контейнер. Pdfimages виконує бітове вилучення оригінального потоку даних, який зберігається всередині файлу. Це дозволяє експерту отримати зображення у його первинному стані – з оригінальною роздільною здатністю, колірним профілем та метаданими, без внесення додаткових артефактів стиснення чи інтерполяції [15].

Інвентаризація графічних об'єктів (Режим – list). Першим кроком дослідження є отримання технічного зведення про всі зображення у документі без їх фізичного вилучення. Команда: «pdfimages – list file.pdf». Аналіз параметрів для виявлення монтажу: здійснюється аналіз таблиці за такими критеріями:

- Image. Номер зображення. Якщо на сторінці, яка візуально виглядає як суцільний скан, виявлено кілька окремих зображень (фрагментів), це може свідчити про накладання тексту або перенесення відтиску печатки.
- Res (ppi). Роздільна здатність.

Ознака підробки. Відмінність у роздільній здатності. Наприклад, основний текст має 300 ppi (сканер), а фрагмент з підписом – 72 або 96 ppi (скриншот з екрана).

- Enc. Метод стиснення.

Ознака підробки. Різні алгоритми стиснення на одній сторінці (наприклад, Ccitt для тексту та jpeg для вставленого фото).

Застосування pdfimages дозволяє відокремити графічну складову документа від його програмної оболонки. Бітове вилучення растрових зображень у їхньому оригінальному форматі дозволяє виявити ознаки комп'ютерного монтажу (накладання масок, розбіжності у роздільній здатності та алгоритмах стиснення), які неможливо зафіксувати при аналізі відрендереної сторінки документа [15].

Алгоритм експертного дослідження гібридних документів.

Для підвищення ефективності дослідження гібридних документів та електронних файлів формату PDF доцільно використовувати алгоритмічний підхід.

Таблиця 2. Алгоритм експертного дослідження

Етап	**Зміст**
1	Дослідження електронного файлу
2	Аналіз метаданих документа
3	Дослідження структури PDF
4	Дослідження паперового примірника
5	Порівняльний аналіз результатів
6	Формування експертного висновку

Такий підхід дозволяє систематизувати процес експертного дослідження та забезпечити більш обґрунтоване формування експертного висновку [9].

Покроковий алгоритм проведення експертного комп'ютерно-технічного дослідження PDF-файлів.

Етап 1. Підготовчий (Забезпечення цілісності об'єктів дослідження).

Фіксація стану: Розрахунок криптографічних хеш-сум (MD5, SHA-256) оригінального файлу. Це гарантує, що об'єкт дослідження не був випадково змінений під час дослідження.

Створення робочої копії: Копіювання файлу на АРМ експерта (або побітове копіювання образу диска).

Ізоляція середовища: Запуск файлу або інструментів аналізу у безпечному, ізольованому середовищі (наприклад, віртуальна машина на базі Linux або WSL під Windows), щоб запобігти випадковому виконанню шкідливого коду.

Етап 2. Первинний огляд.

Сканування сигнатур: Перевірка початку файлу (%PDF-) для підтвердження того, що це дійсно PDF, а не перейменований виконуваний файл.

Пошук аномалій (утиліта pdfid): Швидке сканування на наявність підозрілих ключових слів:

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

- /JavaScript, /JS (активні скрипти).
- /OpenAction, /Launch (автоматичний запуск дій при відкритті).
- Наявність невідповідностей між кількістю об'єктів та потоків.

Етап 3. Хронологічний та атрибутивний аналіз метаданих (інструмент: exiftool).

Повний дамп метаданих: Виконання команди exiftool -a -u -g1 -s файл.pdf.

Аналіз дат: Порівняння CreateDate та ModifyDate у різних словниках (PDF Info та XMP-xmp).

Ознака підробки. Розбіжність дат у різних блоках або якщо дата створення є пізнішою за дату модифікації.

Ідентифікація походження. Аналіз полів Creator, Producer, CreatorTool та XMPToolkit для встановлення програмного забезпечення, яким створювався та редагувався документ.

Аналіз життєвого циклу. Перевірка DocumentID та InstanceID для визначення спорідненості з іншими документами.

Етап 4. Глибокий структурний аналіз (Аналіз COS-архітектури, інструмент: pdf-parser).

Аналіз трейлерів та перехресних посилань. Виконання команди pdf-parser -a файл.pdf.

Підрахунок об'єктів XREF, Trailer та StartXref. Якщо їх більше одного – файл перезберігався (інкрементальні оновлення).

Аналіз версійності. Визначення, які саме об'єкти (особливо /Page та /Metadata) змінювалися від версії до версії. Це показує, чи змінювався візуальний контент після першого створення.

Виявлення об'єктів, на які немає посилань у фінальній таблиці XREF.

Етап 5. Дослідження графічного та текстового контенту (інструмент: pdfimages).

Аналіз роздільної здатності (PPI). Вилучення списку зображень командою pdfimages -list файл.pdf.

Ознака підробки. Різка відмінність PPI (Pixels Per Inch) між різними об'єктами на одній сторінці (наприклад, основа 300 PPI, а підпис 72 PPI).

Екстракція графіки. Вилучення всіх зображень та масок (smask) для детального візуального аналізу на предмет артефактів стиснення.

Аналіз текстового шару. Вилучення чистого тексту. Пошук тексту, який візуально прихований (білий шрифт на білому тлі) або знаходиться за межами видимого поля сторінки.

Етап 6. Узагальнення та формування висновку.

Аналіз результатів дослідження. Зіставлення знайдених аномалій (наприклад, «Невідповідність дат у метаданих» + «Наявність 3-х версій у структурі» + «Аномальний PPI підпису»).

Формування висновків. Формулювання категоричного або ймовірного висновку щодо цілісності, автентичності та походження

файлів.

Практичний приклад експертного дослідження.

До експертної установи надійшов запит на проведення комплексної судової технічної експертизи документів та судової комп'ютерно-технічної експертизи.

На дослідження було надано паперовий примірник Акта приймання-передачі та електронний файл цього документа у форматі PDF.

Перед експертами було поставлене запитання: «Чи виготовлено наданий документ шляхом монтажу за допомогою комп'ютерної або копіювально-розмножувальної техніки?»

У межах проведення судової технічної експертизи документів було проведено візуальне та інструментальне дослідження паперового примірника документа. У ході огляду встановлено, що зображення підписів та відбитків печаток відрізняються від основного тексту документа за рядом ознак, а саме:

– мають різну структуру зображення;

– відрізняються чіткістю контурів, зокрема при збільшенні спостерігається згладжування країв;

– мають різну насиченість та відтінок порівняно з основним текстом;

– у місцях розташування зображень підписів та відбитків печаток спостерігаються незначні особливості відтворення фону;

– розміри та розташування цих зображень не повністю узгоджуються із загальною структурою документа.

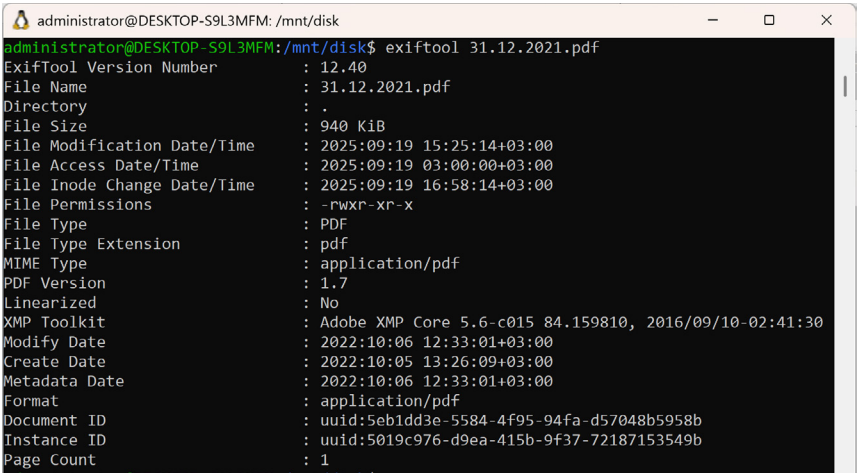

Рис. 3. Зображення електронного файлу з метаданими «31.12.2021.pdf»

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

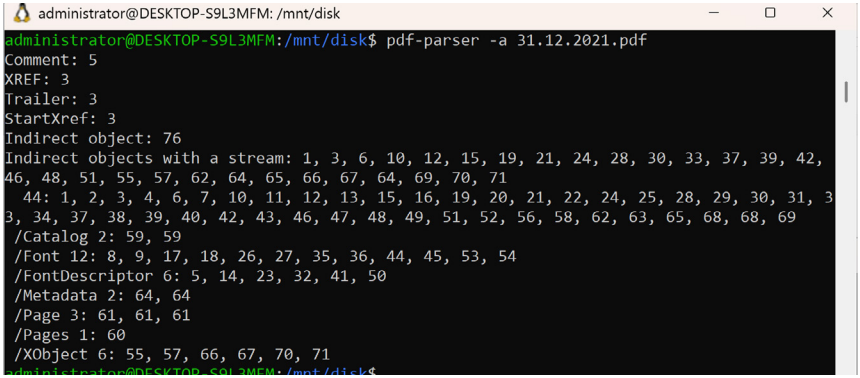

Рис. 4. Зображення структури електронного файлу «31.12.2021.pdf»

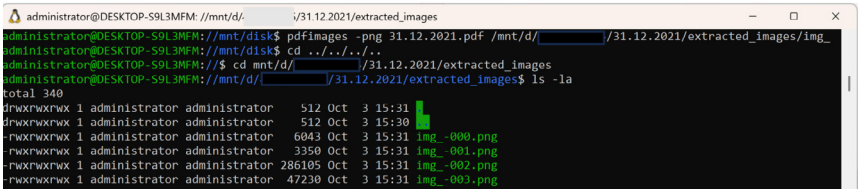

Рис. 5. Зображення електронного файлу «31.12.2021.pdf»

Подібні ознаки у практиці технічної експертизи документів можуть свідчити про можливе внесення змін у документ шляхом монтажу, зокрема додавання окремих реквізитів (зображень підписів та відбитків печаток).

У межах проведення судової комп'ютерно-технічної експертизи проводилось дослідження електронного файлу формату PDF.

На першому етапі дослідження за допомогою багатофункціональної, кросплатформенної утиліти командного рядка для читання, запису та редагування метаданих «ExifTool», здійснено перегляд метаданих електронного файлу «31.12.2021.pdf», рис. 3.

За результатами аналізу метаданих електронного файлу «31.12.2021.pdf», виявлено наступне: первинна дата створення електронного файлу «Create Date: 2022:10:05», дата модифікації «Modify Date: 2022:10:06», це значить, що документ був редагований і збережений наступного дня, редагування відбувалося за допомогою програмного забезпечення на базі інструментарію Adobe «XMP Toolkit: Adobe XMP Core 5.6-c015». Тобто за результатами аналізу на рівні метаданих (ExifTool), можна зробити висновок, що даний електронний файл був модифікований.

На наступному етапі дослідження за допомогою утиліти «pdf-parser», яка являється інструментом командного рядка та використо-

вується для низькорівневого аналізу структури PDF-файлів, здійснено детальний структурний аналіз електронного файлу «31.12.2021.pdf», рис. 4.

За результатами аналізу структури електронного файлу «31.12.2021.pdf» виявлено по 3 секції таблиці перехресних посилань XREF (XREF: 3), по 3 секції трейлера пов'язані із 3-ма таблицями XREF (Trailer: 3), по 3 записи startxref (StartXref: 3), що свідчить про здійснення трьох циклів збереження або редагування електронного файлу, в результаті чого кожен раз у кінець електронного файлу додавалося нове значення xref, trailer і startxref. Значення «StartXref: 3», «XREF: 3» та «Trailer: 3» свідчать, що електронний файл був модифікований і збережений інкрементно (поетапно) щонайменше двічі після початкового створення.

В подальшому, експертами було застосовано утиліту «pdfimages», яка використовується для вилучення (екстракції) вбудованих зображень із файлів формату «*.PDF». За результатами виконання команди виявлено, що електронний файл «31.12.2021.pdf» містить 4 вбудовані зображення, які були успішно витягнуті та збережені у форматі «*.PNG», рис. 5. Вміст PDF-документа «31.12.2021.pdf» наведено на рис. 6. Вміст електронних файлів, які були вилучені з PDF-документа «31.12.2021.pdf», а саме: «img_0002.png», «img_0003.png», наведено на рис. 7, 8.

Рис. 6. Зображення вмісту PDF-документу «31.12.2021.pdf»

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

Рис. 7. Зображення вмісту електронного файлу «img_0002.png»

Рис. 8. Зображення вмісту електронного файлу «img_0003.png»

За результатами аналізу на рівні метаданих (ExifTool), на рівні структури (pdf-parser), на рівні графічного вмісту (pdfimages), електронний файл «31.12.2021.pdf» містить ознаки комп'ютерного монтажу (модифікації). Зображення підпису та печатки, які являються вмістом електронних файлів «img_0002.png» та «img_0003.png», були додані (вбудовані) у PDF-документи у процесі їх редагування/модифікації (інкрементних оновлень) шляхом електронної компіляції (монтажу).

Підсумовуючи, слід зазначити, що поєднане використання консольних утиліт ExifTool, Pdf-parser та Pdfimages дозволяє здійснити аналіз PDF-документів на рівні метаданих, структури (програмного коду) та графічного вмісту (візуального контенту).

Зіставлення результатів дослідження паперового примірника документа та електронного PDF-файлу дозволило встановити, що окремі реквізити документа, а саме зображення відбитків печаток та підписів, були внесені у документ шляхом монтажу за допомогою комп'ютерної техніки.

Таким чином, результати проведеного дослідження підтверджують, що комплексне застосування методів комп'ютерно-технічної експертизи та технічної експертизи документів дозволяє ефективно встановлювати факти монтажу в електронних і гібридних документах.

Висновки

Проведене дослідження показало, що стрімкий розвиток цифрових технологій та широке використання електронного документообігу сприяли появі нових способів фальсифікації документів. Зокрема, монтаж текстових фрагментів або реквізитів у електронних доку-

ментах може здійснюватися за допомогою різноманітних програмних засобів до моменту друку документа. У результаті формуються так звані гібридні документи, які мають цифрове походження, але використовуються у паперовій формі. Такі документи становлять особливий інтерес для судово-експертного дослідження, оскільки поєднують ознаки як електронних, так і традиційних документів.

Під час дослідження встановлено, що ефективне виявлення монтажу у таких документах можливе за умови комплексного застосування методів комп'ютерно-технічної експертизи та технічної експертизи документів. Методи цифрової криміналістики у поєднанні інструментів ExifTool, pdf-parser та pdfimages дозволяють дослідити структуру електронного файлу, проаналізувати метадані документа, встановити програмне забезпечення, за допомогою якого було створено або відредаговано документ, а також визначити можливі зміни у його структурі. Водночас методи технічної експертизи документів дають змогу дослідити матеріальні та графічні особливості паперового примірника документа.

У низці випадків ознаки монтажу можуть бути встановлені лише шляхом зіставлення результатів дослідження паперового примірника документа з результатами аналізу електронного PDF-файлу.

Таким чином, результати проведеного дослідження підтверджують, що встановлення фактів монтажу в електронних і гібридних документах потребує комплексного використання методів технічної експертизи документів та комп'ютерно-технічної експертизи. Поєднання цих методів дозволяє підвищити ефективність виявлення фальсифікацій та забезпечити більш високий рівень обґрунтованості експертних висновків.

Перспективним напрямом подальших досліджень у цій сфері є розроблення спеціалізованих методичних рекомендацій щодо дослідження електронних та гібридних документів у судово-експертній практиці, а також удосконалення програмних інструментів аналізу структури PDF-файлів. Це сприятиме підвищенню ефективності експертних досліджень та забезпеченню належного рівня доказової сили експертних висновків у судовому процесі.

Список використаних джерел:

1. Кейсі Е. Цифрові докази та комп'ютерні злочини. Київ : Юрінком Інтер, 2018. 528 с.
2. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. Відомості Верховної Ради України. 2003. № 36. 12 с.
3. Криміналістика : підручник : у 2 т. Т. 1 / В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін. ; за ред. В. Ю. Шепітька. Харків : Право, 2019. 456 с.
4. Білоус В. Т. Криміналістика : навч. посіб. Київ : Атіка, 2014. 495 с.
5. Клименко Н. І. Судова експертиза документів. Київ : Юрінком

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

Інтер, 2017. 272 с.

6. Simson L., Garfinkel S. Digital forensics research: The next 10 years. Digital Investigation. 2010. P. S64–S73. DOI: https://doi.org/10.1016/j.diin.2010.05.009.

7. Carrier B. File System Forensic Analysis. Boston : Addison-Wesley, 2005. 600 p.

8. Casey E. Digital Evidence and Computer Crime. Academic Press, 2011. 840 p.

9. Клименко Н. І., Пиріг І. В. Судово-експертні дослідження документів. Київ : КНДІСЕ, 2015. 256 с.

10. Шепітько В. Ю., Коновалова В. О. Криміналістика: методологія та практика. Харків : Право, 2018. 464 с.

11. Пелюшок В. Г. Дослідження документів, виготовлених технічним монтажем: методичні рекомендації. Київ: ДНДЕКЦ МВС України, 2022. 19 с.

12. Whitington J. PDF Explained. O'Reilly Media, Inc., 2011. 140 p. URL: https://learning.oreilly.com/library/view/pdf-explained/9781449321581/ (дата звернення: 19.03.2026).

13. Rosenthol L. Developing with PDF. O'Reilly Media, Inc., 2013. 215 p. URL: https://learning.oreilly.com/library/view/developing-with-pdf/9781449327903/ (дата звернення: 19.03.2026).

14. Nissim N., Cohen A., Glezer C., Elovici Y. Detection of malicious PDF files and directions for enhancements. Computers & Security. 2016. Vol. 48. P. 239–248. DOI: https://doi.org/10.1016/j.cose.2014.10.014.

15. Afandi M., Amrulloh R., Isnaini K. N., Suhartono D. Analisis Forensik Pemalsuan Dokumen PDF Menggunakan Metode National Institute of Justice (NIJ). Jurnal Resistor. 2024. Vol. 7, № 3. P. 162–170. DOI: https://doi.org/10.31598/jurnalresistor.v7i3.1460.

References:

1. Casey E. (2018). Tsyfrovi dokazy ta kompiuterni zlochyny [Digital evidence and computer crime]. Kyiv: Yurinkom Inter. 528 p. [in Ukrainian].

2. Verkhovna Rada of Ukraine. (2003). Pro elektronni dokumenty ta elektronnyi dokumentoobih: Zakon Ukrainy vid 22.05.2003 № 851-IV [On electronic documents and electronic document management: Law of Ukraine dated 22.05.2003 No. 851-IV]. Vidomosti Verkhovnoi Rady Ukrainy, 36, 12 p. [in Ukrainian].

3. Shepitko V.Yu., Zhuravel V.A., Konovalova V.O. et al. (2019). Kryminalistyka: pidruchnyk: u 2 t. T. 1 [Criminalistics: textbook: in 2 vols. Vol. 1]. Shepitko V.Yu. (Ed.). Kharkiv: Pravo. 456 p. [in Ukrainian].

4. Bilous V.T. (2014). Kryminalistyka: navchalnyi posibnyk [Criminalistics: study guide]. Kyiv: Atika. 495 p. [in Ukrainian].

5. Klymenko N.I. (2017). Sudova ekspertyza dokumentiv [Forensic examination of documents]. Kyiv: Yurinkom Inter. 272 p. [in Ukrainian].

6. Simson L., Garfinkel S. (2010). Digital forensics research: The next 10 years. Digital Investigation, S64–S73. DOI: 10.1016/j.diin.2010.05.009 [in

English].

7. Carrier B. (2005). File System Forensic Analysis. Boston: Addison-Wesley. 600 p. [in English].

8. Casey E. (2011). Digital Evidence and Computer Crime. Academic Press. 840 p. [in English].

9. Klymenko N.I., Pyrih I.V. (2015). Sudovo-ekspertni doslidzhennia dokumentiv [Forensic expert studies of documents]. Kyiv: KNDISE. 256 p. [in Ukrainian].

10. Shepitko V.Yu., Konovalova V.O. (2018). Kryminalistyka: metodolohiia ta praktyka [Criminalistics: methodology and practice]. Kharkiv: Pravo. 464 p. [in Ukrainian].

11. Peliushok V. H. Doslidzhennya dokumentiv, vyhotovlenykh tekhnichnym montazhem: metodychni rekomendatsiyi. [Examination of Documents Produced by Technical Montage: Methodological Recommendations]. Kyiv: State Research Forensic Center of the Ministry of Internal Affairs of Ukraine, 2022. 19 p. [in Ukrainian].

12. Whitington J. (2011). PDF Explained. O'Reilly Media, Inc. 140 p. URL: https://learning.oreilly.com/library/view/pdf-explained/9781449321581/ (accessed: 19.03.2026) [in English].

13. Rosenthol L. (2013). Developing with PDF. O'Reilly Media, Inc. 215 p. URL: https://learning.oreilly.com/library/view/developing-with-pdf/9781449327903/ (accessed: 19.03.2026) [in English].

14. Nissim N., Cohen A., Glezer C., Elovici Y. (2016). Detection of malicious PDF files and directions for enhancements. Computers & Security, 48, 239–248. DOI: 10.1016/j.cose.2014.10.014 [in English].

15. Afandi M., Amrulloh R., Isnaini K. N., Suhartono D. Analisis Forensik Pemalsuan Dokumen PDF Menggunakan Metode National Institute of Justice (NIJ). Jurnal Resistor. 2024. Vol. 7, № 3. P. 162–170. DOI: https://doi.org/10.31598/jurnalresistor.v7i3.1460.

Надійшла до редакції / Received: 20.03.2026
Отримана після доопрацювання / Received after revision: 14.04.2026
Прийнято до друку / Accepted for publication: 14.04.2026
Опубліковано / Published: 29.05.2026

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