УДК 004.056:343.9

СУЧАСНІ ПІДХОДИ ДО ВИЯВЛЕННЯ АНОМАЛІЙ СТРУКТУРИ ДИСКОВИХ НАКОПИЧУВАЧІВ У ЦИФРОВІЙ КРИМІНАЛІСТИЦІ

Алфьоров С.П.
e-mail: serhii.alforov@nure.ua
Харківський національний університет радіоелектроніки,
каф. ІКІ ім. В.В. Поповського
м. Харків, Україна

The study of structural anomalies in digital storage systems represents an important direction in contemporary digital forensics. Structural inconsistencies in disk geometry, partition tables, and file system metadata may indicate attempts to hide or manipulate digital evidence. This study examines approaches to identifying such anomalies, focusing on the analysis of low-level disk parameters and file system metadata as indicators of concealed information and suspicious disk configurations in digital forensic investigations.

Цифрова криміналістика відіграє ключову роль у розслідуванні кіберінцидентів та аналізі цифрових доказів. Одним із основних джерел інформації під час криміналістичного аналізу є цифрові носії даних, зокрема жорсткі диски та твердотільні накопичувачі. Проте розвиток антикриміналістичних технологій призводить до появи нових методів приховування інформації [1], що суттєво ускладнює процес експертного дослідження таких носіїв.

На відміну від традиційних методів приховування даних, сучасні антикриміналістичні підходи часто спрямовані не на створення окремих прихованих областей, а на модифікацію внутрішніх структур файлових систем та параметрів накопичувачів [1]. Такі модифікації можуть призводити до виникнення аномалій у структурі дискового простору, які не завжди очевидні при використанні стандартних інструментів аналізу.

Аномалії структури дискових накопичувачів можуть проявлятися у різних формах. До них належать невідповідності між логічною та фізичною геометрією накопичувача [2], порушення структури таблиць розділів, аномальні значення метаданих файлової системи, а також наявність неконсистентних або невикористаних областей дискового простору. Подібні ознаки можуть свідчити про використання антикриміналістичних технік або про спроби приховати цифрові дані.

Особливу складність становлять випадки, коли зловмисники змінюють службові структури файлової системи [3] для маскування інформації. У таких ситуаціях дані можуть залишатися фізично присутніми на носії, проте їх логічне представлення у файловій системі навмисно модифікується. Це призводить до появи так званих «осиротілих» структур даних або неконсистентних записів у метаданих файлової системи.

Одним із перспективних напрямів у цифровій криміналістиці є аналіз аномалій у структурі дискових накопичувачів. Такий підхід передбачає дослідження низькорівневих параметрів носія інформації та порівняння їх із очікуваними характеристиками файлової системи. У разі виявлення значних відхилень від стандартної структури можна припустити використання методів антикриміналістики або наявність прихованих даних.

Для реалізації такого підходу застосовуються методи низькорівневого аналізу носіїв інформації, які включають дослідження секторної структури диска, аналіз таблиць розділів, перевірку цілісності файлових систем та дослідження метаданих [2]. Додатково використовуються методи статистичного аналізу та аналізу ентропії даних, що дозволяє виявляти аномальні області, які можуть містити приховану інформацію.

Сучасні інструменти цифрової криміналістики надають можливість автоматизованого аналізу великих масивів даних, проте вони не завжди здатні ефективно виявляти складні антикриміналістичні маніпуляції [4]. У зв’язку з цим актуальним напрямом досліджень є розробка нових методів аналізу дискових структур, які дозволяють ідентифікувати нетипові конфігурації файлових систем та аномальні області дискового простору.

Аналіз сучасних досліджень у сфері цифрової криміналістики свідчить, що попри розвиток інструментів цифрового аналізу, традиційні методи виявлення прихованих даних переважно орієнтовані на ідентифікацію відомих технік приховування, таких як приховані розділи, альтернативні потоки даних або модифікації таблиць розділів [1,3]. Такий підхід є ефективним насамперед у випадках використання вже відомих механізмів маскування інформації, однак розвиток антикриміналістичних технологій зумовлює появу складніших способів модифікації файлових систем і дискових структур, що можуть не залишати очевидних ознак конкретної техніки приховування.

У зв’язку з цим підхід, заснований на аналізі аномалій структури дискового простору, є більш універсальним інструментом криміналістичного дослідження. На відміну від традиційних методів, він дозволяє виявляти нетипові конфігурації дискових накопичувачів, включаючи аномальні значення метаданих, порушення логічної структури файлових систем або невідповідності між фізичними та логічними параметрами носія, незалежно від конкретного механізму маскування. Це підвищує ймовірність виявлення прихованих даних навіть у випадках застосування нових або модифікованих антикриміналістичних методів.

Таким чином, аналіз аномалій структури дискових накопичувачів є перспективним напрямом розвитку цифрової криміналістики. Використання комплексного підходу, що поєднує аналіз метаданих файлових систем, дослідження геометрії диска та статистичні методи аналізу даних, дозволяє підвищити ефективність виявлення прихованих даних та антикриміналістичних маніпуляцій.

Список використаних джерел:

1. González Arias, R., Bermejo Higuera, J., Rainer Granados, J.J., Bermejo Higuera, J.R., Sicilia Montalvo, J.A. Systematic Review: Anti-Forensic Computer Techniques // Applied Sciences. 2024. Vol. 14, no. 12.

2. Ilhami M. R., Cahyani N. D., Jadied E.M. Analysis Technique Data hiding using HPA DCO on SATA Hard Drive // Jurnal Dan Penelitian Teknik Informatika. 2024. Vol. 8, no. 4.

3. Göbel T., Baier H., Türr J. Generating Usable and Assessable Datasets Containing Anti-Forensic Traces at the Filesystem Level // IFIP Advances in Information and Communication Technology. 2025. Vol. 724, P. 225–246.

4. Lim M. C. E., Chow B. C. H., Lim L. Y., Shanbagamaran T., Lim D. Y. J., Hlaing N. W., Rafsanjani A. S. Analysis of Forensic Disk Imaging Tools for Data Acquisition and Preservation // Journal of Informatics and Web Engineering. 2025. Vol. 4, no 2. P. 158–181.