УДК 004.056:343.9

О. А. Пецентій
О. П. Войтович

МЕТОДОЛОГІЯ ЗБОРУ ЦИФРОВИХ ДОКАЗІВ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Вінницький національний технічний університет;

Анотація

Розглянуто методологію збору цифрових доказів під час розслідування кіберзлочинів. Окреслено основні етапи роботи з цифровими доказами: ідентифікацію джерел даних, їх належне здобуття, збереження, аналіз та представлення результатів у кримінальному провадженні. Акцентовано на необхідності дотримання стандартів цифрової криміналістики, принципів забезпечення цілісності доказів і ланцюга їх збереження.

Ключові слова: цифрові докази, кіберзлочини, цифрова криміналістика, методологія розслідування кіберінцидентів, ланцюг збереження доказів, форензіка.

Abstract

The methodology of collecting digital evidence in the investigation of cybercrimes is examined. The main stages of handling digital evidence are outlined, including identification of data sources, proper acquisition, preservation, analysis, and presentation of results in criminal proceedings. Special attention is paid to compliance with digital forensic standards, ensuring the integrity of evidence and the chain of custody.

Keywords: digital evidence, cybercrime, digital forensics, investigation methodology of cybercrime investigation, chain of custody, forensic analysis.

Вступ

Методологія збору цифрових доказів у розслідуванні кіберзлочинів формується на перетині цифрової криміналістики та практик кібербезпеки й реагування на інциденти. На відміну від фізичних доказів, цифрові артефакти є волатильними, що вимагає спеціалізованих технічних процедур фіксації стану ІТ-середовища [1].

Нормативною базою первинних дій із цифровими доказами є ДСТУ ISO/IEC 27037, який визначає принципи ідентифікації, збирання, отримання та збереження цифрових доказів із мінімальним втручанням у джерело даних і з обов'язковим забезпеченням цілісності та простежуваності ланцюга зберігання (chain of custody). Стандарт фіксує ролі учасників процесу, вимоги до документування та контролю цілісності, що зменшує ризик спотворення доказової бази та підвищує процесуальну придатність результатів цифрової криміналістики. Цифрові докази охоплюють дані з комп'ютерів, мобільних пристроїв, мережних пристроїв, хмарних сервісів та систем моніторингу (SIEM), що перетворює процес збору доказів на інженерну задачу роботи з розподіленими цифровими середовищами [2].

Результати дослідження

Методологія реалізується як послідовність взаємопов'язаних етапів із визначеними методами та засобами на кожному кроці.

Етап ідентифікації джерел доказів передбачає виявлення релевантних носіїв і логічних джерел даних (кінцеві пристрої, сервери, мережеві вузли, хмарні журнали, телеметрія SIEM). Методи включають інвентаризацію активів, аналіз контексту інциденту та зіставлення з відомими техніками атак; засоби – системи моніторингу безпеки, журнали подій, кореляційні механізми [2], [4].

Етап збирання та фіксації полягає у мінімально інвазивному вилученні даних відповідно до принципів ДСТУ ISO/IEC 27037 із пріоритетом волатильних артефактів. Застосовуються методи статичної форензіки (створення образів дисків, файлових систем) і динамічної форензіки (live-forensics: зняття оперативної пам'яті, фіксація активних процесів і мережевих з'єднань). Технічні засоби включають форензичні інструменти створення копій та засоби контролю цілісності на основі криптографічних хеш-функцій для верифікації незмінності даних [3].

Етап збереження та забезпечення цілісності передбачає документування ланцюга зберігання, контроль доступу до носіїв із доказами та повторну перевірку хеш-значень на всіх стадіях обробки. Реалізується принцип роботи з цифровими копіями, що знижує ризик зміни первинних артефактів [3].

Етап аналізу та кореляції спрямований на відновлення хронології подій і причинно-наслідкових зв'язків між артефактами з різних джерел. Методи включають мережну форензіку (аналіз трафіку, журналів маршрутизаторів, міжмережних екранів, IDS/IPS), кореляцію подій у SIEM та зіставлення виявлених слідів із техніками кібератак, систематизованими в базі знань MITRE ATT&CK [4].

Етап інтерпретації та подання результатів полягає у формуванні технічно обґрунтованих висновків з відтворюваними процедурами, що підвищує доказову цінність у правозастосовній практиці [5].

Методологія збору цифрових доказів безпосередньо залежить від типу кіберзагрози, оскільки різні способи здійснення атак формують різні категорії цифрових слідів. Зокрема, обманні повідомлення з посиланнями або вкладеннями залишають сліди в поштових журналах, журналах вебдоступу та файловій системі; переміщення між вузлами мережі фіксується у журналах автентифікації та мережних з'єднань; спроби незаконного підвищення прав доступу відображаються у системних журналах і змінах облікових записів. Керування зараженими системами з віддалених серверів супроводжується характерними мереженими з'єднаннями та повторюваними зверненнями до зовнішніх ресурсів. Систематизація технік кібератак у MITRE ATT&CK дозволяє цілеспрямовано визначати перелік артефактів для вилучення та аналізу під час конкретного інциденту [4].

У сучасних інформаційно-комунікаційних системах дедалі більшого значення набувають хмарні та розподілені обчислювальні середовища, де фізичний доступ до носіїв обмежений. За таких умов методологія зміщується від вилучення фізичних накопичувачів до аналізу журналів доступу, подій безпеки, службових записів взаємодії між сервісами та метаданих автентифікації користувачів [5]. Критичною стає кореляція подій між компонентами хмарної інфраструктури для відновлення послідовності дій зловмисника за відсутності прямого доступу до фізичних ресурсів зберігання.

Висновки

Методологія збору цифрових доказів у кіберзлочинах є технічно орієнтованою системою практик, що поєднує цифрову криміналістику, мережну безпеку, аналіз волатильних даних і реагування на інциденти. Її ефективність визначається дотриманням послідовності етапів (ідентифікація - збирання - збереження - аналіз - інтерпретація) та здатністю фіксувати цифрові сліди в динамічному IT-середовищі без порушення цілісності даних.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. NIST Technical Series Publications. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf (дата звернення: 11.02.2026).

2. Кіберзлочинність та електронні докази: навч. посібник / [Б. М. Головкін, О. І. Денькович, В. В. Луцик, Д. М. Цехан] ; за ред. канд. юрид. наук, доц. Ольги Денькович, д-р права, проф. Габріеле Шмельце – Електрон. вид. – Львів : ЛНУ ім. Івана Франка, 2022. – 298 с. –URL: https://law.lnu.edu.ua/wp-content/uploads/2023/08/Cybercrime-and-Digital-Evidence.pdf (дата звернення: 09.02.2026).

3. File System Forensic Analysis. Brian Carrier: Digital Investigation / Forensics and Evidence Research. URL: https://www.digital-evidence.org/fsfa/ (date of access: 11.02.2026).

4. MITRE ATT&CK®. MITRE ATT&CK®. URL: https://attack.mitre.org/ (date of access: 11.02.2026).

5. Техніко-криміналістичне забезпечення розслідування кіберзлочинів [Текст] : навч. посіб. / Л. Майданевич, О. Войтович, Г. Шелепало; Вінниц. нац. техн. ун-т. - Вінниця : ВНТУ, 2025. - 116 с. : рис., табл. - Бібліогр.: с. 112-116. - ISBN 978-617-7417-27-8.

Пецентій Олександр – студент групи 1БС-24мз, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, email: petsentiyalex@gmail.com.

Petsenty Oleksandr – student of group 1BS-24mz, Faculty of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, email: petsentiyalex@gmail.com.

Науковий керівник: **Войтович Олеся** – к. т. н., доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця, e-mail voytovych.olesya@vntu.edu.ua

Supervisor: **Voytovych Olesya** – Ph.D., Associate Professor of the Department of Information Protection, Vinnytsia National Technical e-mail voytovych.olesya@vntu.edu.ua