МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ В. Н. КАРАЗІНА

НАУКОВІ ДОСЛІДЖЕННЯ МОЛОДІ З ПРОБЛЕМ ЄВРОПЕЙСЬКОЇ ІНТЕГРАЦІЇ

Збірник тез доповідей
XIV Міжнародної науково-практичної конференції
молодих учених та студентів

(4 квітня 2025 року, м. Харків, Україна)

Електронний ресурс

Харків – 2025

Яненко О.С.,
здобувач першого (бакалаврського) рівня вищої освіти
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна;
науковий керівник: д. т. н., професор Гороховатський В.О.,
ННІ «Каразінський банківський інститут» ХНУ імені В.Н. Каразіна

ЦИФРОВА КРИМІНАЛІСТИКА ЯК ЗАСІБ ІДЕНТИФІКАЦІЇ КІБЕРЗЛОЧИНІВ

Цифрова криміналістика – це галузь судової експертизи, яка займається виявленням, збором, аналізом та інтерпретацією електронних доказів. Вона охоплює методи дослідження інформації, отриманої з комп'ютерних систем, мобільних пристроїв, мережевого трафіку та інших цифрових джерел [1-3].

До основних напрямів цифрової криміналістики належать:

- Комп’ютерна криміналістика (аналіз жорстких дисків, відновлення видалених файлів).
- Мережева криміналістика (дослідження трафіку, аналіз лог-файлів).
- Мобільна криміналістика (отримання даних з мобільних пристроїв).
- Криміналістика хмарних сервісів (аналіз віддалених серверів та хмарних середовищ).

Розглянемо основні функціонали, аспекти впровадження та сферу практичних задач, для вирішення яких застосовуються засоби цифрової криміналістики.

Роль цифрової криміналістики у боротьбі з кіберзлочинами. Цифрова криміналістика відіграє ключову роль у виявленні та розслідуванні кіберзлочинів, таких як шахрайство, несанкціонований доступ до даних, зломи інформаційних систем. Вона дозволяє відстежувати сліди злочинців у цифровому просторі та надавати докази, які можуть бути використані в суді.

Методи збору та аналізу цифрових доказів. Криміналісти використовують спеціалізоване програмне забезпечення, таке як EnCase, FTK та Autopsy, для збереження та аналізу електронних доказів. Важливим аспектом є забезпечення їхньої цілісності та неможливості підробки. Застосовується хешування даних, створення образів дисків та аналіз системних журналів подій. При цьому впроваджуються сучасні підходи штучного інтелекту та розпізнавання візуальних образів [4-6].

Відновлення видалених та зашифрованих даних. Багато зловмисників намагаються приховати свої сліди, видаляючи або шифруючи файли. Проте за допомогою спеціальних алгоритмів можна відновити інформацію навіть після її знищення або шифрування. Це особливо важливо при розслідуванні справ, пов’язаних з фінансовими махінаціями або порушеннями авторських прав.

Протидія анонімізації та методам приховування слідів. Зловмисники часто використовують анонімні мережі (Tor), VPN та проксі-сервери для приховування своєї активності. Сучасні методи цифрової криміналістики

дозволяють виявляти джерело трафіку за допомогою аналізу кореляцій мережевих даних, часових міток та цифрових підписів.

Автоматизація криміналістичних досліджень за допомогою ШІ. Штучний інтелект дозволяє значно прискорити процес аналізу лог-файлів, виявлення аномальної поведінки у системах та класифікації загроз. Це зменшує навантаження на фахівців та підвищує ефективність розслідувань.

Юридичні та етичні аспекти використання цифрових доказів. Отримані цифрові докази повинні відповідати вимогам міжнародного та національного законодавства, зокрема GDPR, законів про кібербезпеку та кримінально-процесуальних норм. Також важливо дотримуватися етичних принципів, щоб уникнути незаконного втручання в приватне життя громадян.

З кожним роком методи цифрової криміналістики вдосконалюються, інтегруючись з технологіями великих даних, блокчейном та кіберрозвідкою. Використання хмарних сервісів дозволяє швидко обробляти великі обсяги інформації, а квантові обчислення у майбутньому можуть розвинути перспективу новітніх методів дешифрування даних.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Casey E. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. – Academic Press, 2011.
2. L. Rogers, "Applying Machine Learning to Digital Forensics," in Journal of Digital Investigation, vol. 35, 2022.
3. Mahalik R. Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes. – CRC Press, 2020.
4. Gorokhovatskyi, V., Gadetska, S., & Stiahlyk, N. (2023). Accelerating Image Classification based on a Model for Estimating Descriptor-to-Class Distance. International Journal of Computing, 22(4), 485-492.
5. S. V. Gadetska, V. O. Gorokhovatskyi, N. I. Stiahlyk, and N. V. Vlasenko, Statistical data analysis tools in image classification methods based on the description as a set of binary descriptors of key points, Radio Electronics, Computer Science, Control, no. 4, pp. 58–68, 2021, doi: 10.15588/1607-3274-2021-4-6.
6. Gorokhovatskyi V., Tvoroshenko I., Yakovleva O., and Hudáková M. (2025) Image description compression in classification structural methods, IEEE Access, vol. 13, pp. 43631-43641, doi: 10.1109/ACCESS.2025.3548910.
7. Gorokhovatskyi, V., Gadetska, S., Stiahlyk, N. (2024) Classification of images based on distance assessment. Information Technology and Implementation (Satellite): Conference Proceedings, November 21, 2024, Kyiv, Ukraine / V. Snytyuk (Editor). – Kyiv: Publishing House «Caravela», 22-24.