DOI https://doi.org/10.30525/978-9934-26-558-7-78

EFFECTIVENESS OF COMPUTER FORENSICS METHODS IN INVESTIGATING CYBERCRIMES AT CRITICAL INFRASTRUCTURE FACILITIES

ЕФЕКТИВНІСТЬ МЕТОДІВ КОМП'ЮТЕРНОЇ КРИМІНАЛІСТИКИ У РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ НА ОБ'ЄКТАХ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗАХИСТУ

Bozhyk V. I.
PhD in Law,
Interregional Academy of Personnel Management,
Kyiv, Ukraine
ORCID ID: 0000-0003-3162-0125

Божик В. І.
кандидат юридичних наук,
Міжрегіональна академія управління персоналом,
м. Київ, Україна
ORCID ID: 0000-0003-3162-0125

Цифровізація фінансового, роздрібного та технологічного секторів критичної інфраструктури суттєво змінила характер сучасної кіберзлочинності. Несанкціоновані втручання в інформаційні системи, шахрайство з електронними платежами, витоки конфіденційних даних, викрадення цифрових активів та використання шкідливого програмного забезпечення дедалі частіше стають предметом кримінальних проваджень. Такі кіберзлочини характеризуються високою латентністю, транскордонністю та значною технічною складністю, що ускладнює їх розслідування без використання спеціалізованих криміналістичних методів.

У сучасних дослідженнях цифрова криміналістика розглядається як один із ключових інструментів протидії кіберзлочинності. Klasén, Fock та Forchheimer звертають увагу на появу так званих «невидимих цифрових доказів» – слідів, що існують виключно в електронному середовищі [1]. Це змінює підходи як до процесу доказування, так і до методів криміналістичного аналізу. Irons та Lallie зазначають, що традиційні підходи до цифрових розслідувань уже не відповідають сучасному рівню розвитку кіберзлочинності, тому особливого значення набувають аналітичні та проактивні методи виявлення цифрових загроз [2].

Особливої актуальності проблема набуває щодо об’єктів критичної інфраструктури. Порушення роботи фінансових систем, електронних торговельних платформ або технологічних мереж може призводити не лише до економічних збитків, а й створювати ризики для національної безпеки держави. У зв’язку з цим ефективність методів комп’ютерної криміналістики безпосередньо впливає на здатність держави протидіяти сучасним кіберзагрозам.

Окрему проблему становить використання злочинцями спеціальних способів приховування цифрових слідів. Адже знищення метаданих, стеганографія та інші способи протидії цифровій експертизі суттєво ускладнюють встановлення обставин кримінального правопорушення. У зв'язку з цим питання забезпечення цілісності та автентичності електронних доказів набуває особливого значення не лише у технічному, а й у процесуальному аспекті.

Попри значну кількість наукових праць, ефективність окремих криміналістичних методів щодо різних секторів критичної інфраструктури залишається недостатньо дослідженою. Більшість досліджень аналізують цифрову криміналістику без урахування галузевої специфіки або не містять практичної перевірки на реальних матеріалах кримінальних проваджень. Саме тому актуальним є дослідження результативності окремих методів цифрової криміналістики у фінансовому, роздрібному та технологічному секторах.

Емпіричну основу дослідження становили матеріали 50 задокументованих випадків кіберзлочинів у фінансовому, роздрібному та технологічному секторах. Для аналізу використовувалися цифрові артефакти, системні журнали, лабораторні звіти та матеріали міжнародних організацій у сфері кібербезпеки. Додатково проведено напівструктуровані інтерв'ю зі слідчими, криміналістами та спеціалістами з IT-безпеки.

Результати дослідження показали, що найбільш ефективними методами комп'ютерної криміналістики є відновлення даних; аналіз журналів подій; статистичний аналіз цифрової активності; захоплення образів дисків; мережевий аналіз трафіку.

Метод відновлення даних виявився особливо ефективним у випадках видалення або навмисного приховування інформації. Саме цей метод дозволяв відновлювати журнали транзакцій, історію доступу користувачів та інші цифрові сліди, необхідні для реконструкції механізму кіберзлочину.

Аналіз журналів подій забезпечував можливість встановлення хронології несанкціонованого доступу, визначення часу втручання в систему та послідовності дій користувачів. У багатьох випадках саме системні журнали ставали ключовим джерелом доказової інформації.

Статистичний аналіз цифрової активності дозволяв виявляти аномальні операції, підозрілі поведінкові моделі та взаємозв'язки між окремими подіями в інформаційній системі. Особливого значення цей метод набуває у фінансовому секторі, де обсяг цифрових транзакцій є надзвичайно великим.

Проведене дослідження підтвердило, що комбіноване використання кількох криміналістичних методів суттєво підвищує результативність розслідування. Статистичний аналіз результатів засвідчив наявність

сильного позитивного зв'язку між кількістю застосованих криміналістичних методів та ефективністю кримінального переслідування у справах про кіберзлочини. Поєднання аналізу журналів подій, відновлення даних та дослідження цифрової активності забезпечує більш повну реконструкцію механізму кримінального правопорушення та підвищує якість доказової бази. Аналогічні висновки містяться і в роботах Wüllenweber та Giles, які наголошують на ефективності комплексного використання різних видів криміналістичних доказів [3].

Дослідження також дозволило визначити основні проблеми сучасної цифрової криміналістики: значний обсяг цифрових даних; нестача підготовлених фахівців; дефіцит технічних ресурсів; відсутність уніфікованих процедур роботи з електронними доказами; складність міжнародного обміну цифровими доказами.

Більшість опитаних фахівців вказали, що ефективність цифрових розслідувань безпосередньо залежить від рівня підготовки криміналістів та технічного забезпечення правоохоронних органів. Окрім цього, значні труднощі виникають під час обробки великих масивів цифрової інформації, особливо у випадках транскордонних кіберзлочинів.

Перспективним напрямом розвитку цифрової криміналістики є використання інструментів штучного інтелекту та предиктивної аналітики для автоматизованого аналізу цифрових даних, виявлення аномальної активності та прогнозування кіберзагроз. Korystin, Svyrydiuk та Mitina зазначають, що алгоритми прогнозування ризиків можуть використовуватися для раннього виявлення підозрілої цифрової активності та автоматизованого аналізу великих масивів даних [4].

Особливого значення це набуває в умовах адаптації українського законодавства до стандартів ЄС щодо електронних доказів та цифрової безпеки. У сучасних умовах ефективність розслідування кіберзлочинів значною мірою залежить не лише від технічних можливостей правоохоронних органів, але й від рівня нормативного регулювання роботи з цифровими доказами.

Отримані результати підтверджують необхідність подальшого вдосконалення криміналістичних методик розслідування кіберзлочинів, розроблення галузево-специфічних протоколів роботи з цифровими доказами та системної підготовки фахівців у сфері комп'ютерної криміналістики.

Література:

1. Klasén L., Fock N., Forchheimer R. The invisible evidence: Digital forensics as key to solving crimes in the digital age. *Forensic Science International*. 2024. Vol. 362. Art. 112133. DOI: 10.1016/j.forsciint.2024.112133.

2. Irons A., Lallie H. Digital forensics to intelligent forensics. *Future Internet*. 2014. Vol. 6, no. 3. P. 584–596. DOI: 10.3390/fi6030584.

3. Wüllenweber S., Giles S. The effectiveness of forensic evidence in the investigation of volume crime scenes. Science & Justice. 2021. Vol. 61. Iss. 5. P. 542–554. DOI: 10.1016/j.scijus.2021.06.008

4. Korystin O., Svyrydiuk N., Mitina O. Risk forecasting of data confidentiality breach using linear regression algorithm. *International Journal of Computer Network and Information Security*. 2022. Vol. 14. No. 4. P. 1–13. DOI: 10.5815/ijcnis.2022.04.01.