

МЕТОДИКА ОБРОБЛЕННЯ КОМП'ЮТЕРНИХ ДАНИХ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Вінницький національний технічний університет

Анотація

У роботі розглянуто особливості методики оброблення комп'ютерних даних під час розслідування кіберзлочинів. Проаналізовано основні джерела цифрових доказів, а також етапи роботи з комп'ютерною інформацією, зокрема збір, копіювання, аналіз та відновлення даних. Особливу увагу приділено використанню спеціалізованих інструментів цифрової криміналістики, які дозволяють ефективно досліджувати інформацію та встановлювати обставини кіберзлочинів. Визначено значення правильного оброблення комп'ютерних даних для забезпечення достовірності цифрових доказів та підвищення ефективності розслідування.

Ключові слова: кіберзлочини, комп'ютерні дані, цифрові докази, цифрова криміналістика, кібербезпека, розслідування кіберзлочинів.

Abstract

The paper examines the methodology of computer data processing during the investigation of cybercrimes. The main sources of digital evidence and the stages of working with computer information are analyzed, including data collection, copying, analysis, and recovery. Special attention is paid to the use of digital forensic tools that enable effective investigation of information and identification of cybercrime circumstances. The importance of proper computer data processing for ensuring the reliability of digital evidence and improving the efficiency of cybercrime investigations is determined.

Keywords: cybercrime, computer data, digital evidence, digital forensics, cybersecurity, cybercrime investigation.

Вступ

У сучасному інформаційному суспільстві цифрові технології активно використовуються в усіх сферах життя. Разом із розвитком інформаційних систем зростає і кількість кіберзлочинів. До таких злочинів належать несанкціонований доступ до інформаційних систем, викрадення персональних даних, поширення шкідливого програмного забезпечення та інші протиправні дії у кіберпросторі. Розслідування кіберзлочинів значною мірою залежить від правильного збору, збереження та аналізу комп'ютерних даних. Саме тому особливого значення набуває методика оброблення цифрових доказів. Від точності та правильності виконання цих процедур залежить можливість встановлення обставин злочину та притягнення винних осіб до відповідальності.

Результати дослідження

У сучасному інформаційному суспільстві цифрові технології відіграють важливу роль у функціонуванні держави, економіки та повсякденного життя людини. Водночас активне використання інформаційно-комунікаційних технологій призводить до зростання кількості кіберзлочинів, що створює нові виклики для правоохоронних органів та фахівців у сфері інформаційної безпеки. У зв'язку з цим особливого значення набуває дослідження методик оброблення комп'ютерних даних під час розслідування кіберзлочинів. Кіберзлочини - це протиправні дії, що здійснюються з використанням комп'ютерних систем, мереж або інформаційних технологій з метою отримання неправомірної вигоди, викрадення інформації чи порушення нормального функціонування інформаційних систем. До найбільш поширених видів кіберзлочинів належать несанкціонований доступ до інформаційних ресурсів, поширення шкідливого програмного забезпечення, викрадення персональних даних, шахрайство у мережі Інтернет та інші види протиправної діяльності у кіберпросторі [1]. У процесі розслідування таких правопорушень важливу роль відіграють комп'ютерні або цифрові дані. Під цифровими даними розуміють інформацію, що

створюється, обробляється, зберігається або передається за допомогою комп'ютерних систем і може бути використана як доказ під час розслідування. Джерелами таких даних можуть виступати персональні комп'ютери, мобільні пристрої, сервери, мережеве обладнання, електронна пошта, журнали подій інформаційних систем, а також хмарні сервіси.

Таким чином, важливо проаналізувати основні етапи методики оброблення комп'ютерних даних у процесі розслідування кіберзлочинів. Ефективність такого процесу безпосередньо залежить від дотримання принципів законності, збереження цілісності цифрових доказів та їх належної фіксації.

Першим етапом є виявлення та збір цифрових доказів. На цьому етапі здійснюється пошук джерел інформації, які можуть містити сліди протиправної діяльності. До таких джерел належать персональні комп'ютери, ноутбуки, сервери, мобільні пристрої, зовнішні накопичувачі, хмарні сховища, мережеве обладнання, а також облікові записи користувачів у різних інформаційних системах. Важливим завданням є забезпечення збереження цілісності даних та недопущення їх зміни або пошкодження. Для цього можуть застосовуватися спеціальні засоби блокування запису (write-blockers), а також здійснюватися фото- та відеофіксація процесу вилучення носіїв інформації. Наприклад, під час розслідування випадків несанкціонованого доступу до інформаційної системи може бути вилучено системний блок або сервер для подальшого дослідження його в лабораторних умовах.

Наступним етапом є створення точних копій носіїв інформації. Для проведення подальшого аналізу використовуються спеціальні методи копіювання, зокрема побітове (forensic imaging) створення образу диска, яке дозволяє отримати ідентичну копію даних без внесення змін до оригінального носія. Такий підхід забезпечує можливість повторної перевірки результатів дослідження та збереження первинних даних як цифрового доказу. При цьому обов'язково розраховується та фіксується контрольна хеш-сума (наприклад, за алгоритмами MD5 або SHA-256), що дозволяє підтвердити ідентичність оригіналу та його копії.

Третім етапом є аналіз отриманої інформації. На цьому етапі досліджуються файлові системи, журнали подій операційної системи, мережевий трафік, електронна кореспонденція, історія вебперегляду, метадані файлів та інші цифрові сліди, які можуть містити інформацію про дії користувача або факт здійснення кіберзлочину. Наприклад, аналіз журналів подій може допомогти встановити час несанкціонованого входу до системи, а дослідження мережевого трафіку — виявити передачу конфіденційних даних на сторонні ресурси. У деяких випадках проводиться також відновлення видалених або прихованих файлів, що дозволяє отримати додаткові відомості про обставини правопорушення, зокрема файли журналів, тимчасові документи або зашифровані контейнери даних.

Окрему роль у процесі оброблення комп'ютерних даних відіграють спеціалізовані інструменти цифрової криміналістики. Використання відповідного програмного забезпечення дозволяє автоматизувати процес пошуку інформації, здійснювати аналіз великого обсягу даних, виявляти приховані файли, проводити кореляцію подій та відновлювати видалену інформацію. Застосування таких інструментів суттєво підвищує ефективність розслідування, скорочує час опрацювання матеріалів та сприяє більш повному встановленню обставин кіберзлочину. Крім того, результати аналізу повинні бути належним чином задокументовані для забезпечення їх допустимості як доказів у судовому процесі [2].

Таким чином, кожен етап оброблення комп'ютерних даних — від виявлення та збору доказів до створення точних копій і детального аналізу, є невід'ємною частиною комплексного процесу розслідування кіберзлочинів. Пропуск або недбале виконання будь-якого з цих етапів може призвести до втрати важливої інформації, спотворення доказів або їхньої недопустимості у суді. Лише послідовне та методично обґрунтоване виконання всіх процедур забезпечує надійність, достовірність і повноту отриманих даних, що дозволяє не тільки встановити обставини правопорушення, а й ефективно притягнути винних до відповідальності.

Висновки

У результаті проведеного дослідження було встановлено, що ефективність розслідування кіберзлочинів значною мірою залежить від правильної організації процесу оброблення комп'ютерних даних. Цифрові дані виступають важливим джерелом доказової інформації, оскільки вони можуть містити відомості про дії користувачів, використані програмні засоби та інші обставини вчинення

кіберзлочину. Проведений аналіз показав, що методика оброблення комп'ютерних даних включає декілька послідовних етапів, серед яких виявлення та збір цифрових доказів, створення копій носіїв інформації, аналіз отриманих даних та відновлення видаленої інформації. Дотримання зазначених процедур дозволяє забезпечити цілісність та достовірність цифрових доказів, що є важливою умовою їх подальшого використання у процесі розслідування. Крім того, встановлено, що застосування сучасних інструментів цифрової криміналістики значно підвищує ефективність аналізу інформації та сприяє швидшому виявленню слідів протиправної діяльності у комп'ютерних системах. Отже, удосконалення методик оброблення комп'ютерних даних є важливим напрямом розвитку практики розслідування кіберзлочинів та забезпечення інформаційної безпеки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Техніко-криміналістичне забезпечення розслідування кіберзлочинів : навч. посіб. / Л. О. Майданевич, О. П. Войтович, Г. В. Шелепало. Вінниця : ВНТУ, 2025. 117 с.

2. Степанюк Р. Л., Перлін С. І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка. 2022. № 99. С. 283–284.

Гаврилюк Катерина Миколаївна – студентка групи ЗКІТС-24б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м. Вінниця.

Салієва Ольга Володимирівна – доктор філософії з кібербезпеки (PhD), доцент кафедри менеджменту та безпеки інформаційних систем, e-mail: salieva8257@vntu.edu.ua;

Kateryna Havryliuk – Faculty of Faculty of Management and Information Security, Vinnytsia National Technical University, Vinnytsia.

Salieva Olha V. – Doctor of Philosophy in Cybersecurity (PhD), Associate Professor of the Department of Management and Information Systems Security, e-mail: salieva8257@vntu.edu.ua;