Роль цифрової криміналістики в розслідуванні кіберзлочинів

Олена Джафарова

д-ка юрид. наук, проф., Харківський національний університет внутрішніх справ, м. Харків, Україна, ORCID: https://orcid.org/0000-0003-4201-0218

Даніїл Зінченко

Вінницьке районне управління поліції Головного управління національної поліції в Вінницькій обл., м. Вінниця, Україна, ORCID: https://orcid.org/0000-0002-8089-0511

У сучасному цифровому світі зростання кіберзлочинності спричиняє нові виклики до правоохоронних органів і спеціалістів із цифрової безпеки. У статті розглянуто сучасні методи та технології цифрової криміналістики, їх значення у розкритті злочинів в інтернеті.

Ключові слова: цифрова криміналістика; кіберзлочини; машинне навчання; програмне забезпечення; конфіденційність; кібербезпека.

The Role of Digital Forensics in Cybercrime Investigation

Olena Dzhafarova, Daniil Zinchenko

In today's digital world, the rise of cybercrime presents new challenges for law enforcement and digital security professionals. This article explores modern digital forensics methods and technologies and their significance in addressing crimes on the Internet.

Keywords: digital forensics; cybercrimes; machine learning; software; privacy; cybersecurity.

Із появою інтернету та швидким розвитком цифрових технологій з'явилися нові форми злочинності. Кіберзлочини можуть містити широкий спектр незаконних дій, від шахрайства з кредитними картками до кібертероризму. Цифрова криміналістика стала невід'ємною складовою розслідування, надаючи методи та інструменти для ефективного виявлення, аналізування та представлення доказів.

В епоху, коли цифровий світ стає дедалі більше взаємопов'язаним і складним, методи цифрової криміналістики відіграють вирішальну роль у захисті інформаційного простору та боротьбі з кіберзлочинністю [1]. Ця дисципліна, що поєднує знання інформатики, права та криміналістики, стає мостом між цифровими слідами та реальним правосуддям, розкриваючи злочини, скоєні в безмежному цифровому просторі. Поміж різноманіття методів цифрової криміналістики особливе місце займає форензичний аналіз, що дає змогу експертам відновлювати видалену або пошкоджену інформацію, виявляти приховані або зашифровані дані. Цей метод є критично важливим, оскільки злочинці часто намагаються замаскувати свою діяльність або знищити докази. Логічний аналіз — ще одна ключова стратегія, яка допомагає аналізувати дані без фізичного втручання в пристрій і дає можливість дослідникам ефективно збирати докази з різноманітних джерел (зокрема, хмарні сховища та онлайн-акаунти) без ризику пошкодити первинні докази або порушити їхню цілісність [2]. Криптоаналіз також відіграє важливу роль у викритті кіберзлочинів, допомагаючи розшифровувати захищену інформацію без використання ключа, його часто використовують для виявлення зашифрованих повідомлень між злочинцями або для доступу до конфіденційної інформації, яку вони намагаються приховати [3]. Також в арсеналі цифрової криміналістики є методи соціальної інженерії, що допомагають розкривати злочини, скоєні за допомогою маніпуляцій або обману. Експерти використовують знання про поведінку людини, щоб ідентифікувати слабкі місця в безпеці систем і виявити зловмисників.

На нашу думку, ці методи формують міцну основу для боротьби з кіберзлочинністю, даючи змогу ефективно виявляти, аналізувати та представляти докази у суді. Цифрова криміналістика продовжує розвиватися, адаптуючись до нових викликів, які постають перед суспільством через невпинний розвиток технологій, гарантуючи, що правосуддя здійсниться навіть у найбільш складних і прихованих цифрових світах.

У міру того, як цифровий світ розширює свої обрії, з'являються нові виклики для правопорядку та безпеки. Технології цифрової криміналістики відіграють вирішальну роль у реагуванні на ці виклики, надаючи правоохоронним органам потужні інструменти для розслідування та притягнення до відповідальності кіберзлочинців. Вони стають окулярами, через які можна розгледіти найдрібніші деталі в океані цифрових даних, перетворюючи невидиме на відчутне та зрозуміле.

Однією з передових технологій у цій сфері є штучний інтелект (ШІ), який революціонізує способи виявлення та аналізування даних [4]. Алгоритми машинного навчання можуть виявляти зразки та аномалії у значних масивах даних зі швидкістю та точністю, недосяжними для людини. Це дає змогу швидко ідентифікувати потенційні загрози та сліди кіберзлочинів, значно скорочуючи час, необхідний для розслідувань. Блокчейн-технології також знайшли своє застосування в цифровій криміналістиці, надаючи неперевершену прозорість і безпеку у зберіганні доказової бази [5]. Використання розподілених реєстрів дає змогу створити незмінну та перевірену історію даних, що є критично важливим для підтримання справедливості та довіри до судової системи. До того ж технології віртуальної та доповненої реальності відкривають нові можливості для реконструкції подій та місць злочинів, що не тільки допомагає слідчим краще зрозуміти обставини справи, а й надає суду можливість наочно ознайомитися з доказовою базою, підвищуючи якість та об'єктивність судових рішень. Інструменти цифрової криміналістики (зокрема, сучасне програмне забезпечення для аналізування даних, спеціалізоване обладнання для зчитування інформації з різноманітних носіїв, системи виявлення та запобігання кібератак) стали невід'ємною складовою арсеналу правоохоронних органів. Вони дають змогу не тільки розкривати злочини, а й прогнозувати потенційні загрози, захищаючи суспільство від можливих атак.

Ми вважаємо, що технології цифрової криміналістики є фундаментом для створення більш безпечного цифрового середовища. Вони не тільки сприяють виявленню та розслідуванню злочинів, а й відіграють ключову роль у формуванні безпечного майбутнього, у якому технології служать закону та справедливості, захищаючи права та свободи кожної особи в цифровому світі.

Отже, цифрова криміналістика — це незамінний інструмент у боротьбі з кіберзлочинністю, що надає правоохоронним органам необхідні засоби для ефективного розслідування та притягнення до відповідальності зловмисників. Вона використовує передові технології та методики для аналізування цифрових даних, виявляючи, збираючи та аналізуючи докази злочинів, скоєних в цифровому просторі. Розвиток цифрової криміналістики сприяє не лише виявленню та розслідуванню злочинів, а й підвищує загальний рівень кібербезпеки, зміцнюючи захист інформаційних систем і баз даних від несанкціонованого доступу або зловмисних атак. Ця сфера постійно розвивається, адаптуючись до нових викликів і загроз, що з'являються в результаті швидкого розвитку цифрових технологій. Отже, роль цифрової криміналістики в розслідуванні кіберзлочинів є критично важливою для забезпечення правопорядку та безпеки в сучасному цифровому світі, що вимагає від правоохоронних органів постійного розвитку знань, умінь та інструментів для ефективної відповіді на кіберзагрози.

Перелік джерел посилання

1. Звірянський Г. В. Нормативно-правовове регулювання психологічного забезпечення службової діяльності працівників поліції. Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів. Київ, 2023. С. 20—22.
2. Зінченко Д. А. Засоби юридичної техніки в контексті захисту прав людини. *Мова і право*. Дніпро, 2023. С. 87—89.
3. Зінченко Д. А. Стратегія боротьби з кіберзлочинністю в умовах глобалізації інформаційних просторів. *Застосування інформаційних технологій у правоохоронній діяльності* : мат-ли кругл. столу. Харків, 2023. С. 105—107.
4. Зінченко Д. А., Макарова О. П. Аналіз ризиків і стратегій захисту від кібератак у сучасному цифровому світі / Протидія кіберзлочинності та торгівлі людьми. Вінниця, 2023. С. 118—121.
5. Зінченко Д. А., Сидоренко В. М. Загальний розвиток використання міжнародного досвіду працівниками поліції у сфері протидії кіберзлочинам і торгівлі людьми. Там само. С. 44—46.