Болгаренко В. М.
курсант ІІІ курсу
Дніпропетровського державного
університету внутрішніх справ

Бідняк Г. С.
кандидат юридичних наук, доцент,
доцент кафедри криміналістики
та домедичної підготовки
Дніпропетровського державного
університету внутрішніх справ

АНАЛІЗ ДАНИХ, ОТРИМАНИХ З ЕЛЕКТРОННИХ ПРИСТРОЇВ, ПІД ЧАС РОЗСЛІДУВАННЯ ЕКОНОМІЧНИХ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

В сучасному діджиталізованому світі, де використання електронних пристроїв стало необхідною частиною побуту та професійної діяльності, аналіз даних, отриманих з цих пристроїв, набуває великого значення в сфері розслідування економічних злочинів. За допомогою сучасних технологій та методів аналізу, що еволюціонували разом із швидким розвитком цифрових технологій, правоохоронці отримують унікальну можливість вивчення електронних слідів, які часто є важливими доказами у справах економічних правопорушень [1].

У роботі ми намагались розглянути сучасні методи та підходи до обробки та аналізу інформації, яку можна витягти з комп'ютерів, смартфонів та інших цифрових пристроїв у контексті економічних злочинів. Заглиблюючись у проблематику використання цифрових слідів у кримінальних розслідуваннях, робота висвітлює важливі аспекти та виклики, що стоять перед правоохоронними органами у цьому напрямі.

Електронні докази, які можуть використовуватися у розслідуванні економічних злочинів, охоплюють широкий спектр цифрових інформаційних слідів, збережених на електронних пристроях. Дослідники цієї категорії кримінальних правопорушень зазначають, що такі сліди залишаються в комп’ютерній техніці у вигляді проєктів документів, електронній переписці, в електронних гаджетах, сайтах відкритої інформації про закупівлі («Prozorro», «Держзакупівлі Online», «Zakupki UA» «Tender Online»). Використовуються для спілкування між співучасниками за допомогою месенджерів, IP-телефонії тощо [4].

Основні категорії електронних доказів включають:

- Електронну пошту: аналіз електронної пошти може розкрити комунікації між особами, угоди, фінансові транзакції та інші важливі деталі.
- Файли та документи: електронні пристрої містять файли та документи, які можуть свідчити про фінансові транзакції, контракти, звіти,

рахунки та інші економічні відносини.

- Інтернет-сліди: вивчення історії веб-перегляду, соціальних мереж, форумів та інших онлайн-активностей може розкрити зв'язки, інтереси та інші аспекти поведінки осіб.
- Метадані: інформація про час, місце та умови створення файлів, фотографій та відео може бути важливою у встановленні фактів і подій.
- Банківські дані: аналіз транзакцій на банківських рахунках, електронних платіжних системах та інших фінансових джерелах надає уявлення про фінансовий стан та операції осіб.
- Мобільні додатки: вміст та інформація з мобільних додатків, таких як банківські застосунки чи месенджери, може стати важливими доказами.
- Системні журнали: аналіз системних журналів комп'ютерів може допомогти встановити час та обставини роботи пристроїв, а також виявити потенційні атаки чи вторгнення [2].

Якщо під час обшуку виявлено увімкнений комп'ютер чи інші електронні пристрої, необхідно негайно провести огляд та вилучення комп'ютерних даних у реальному часі з метою запобігання можливості їх блокування, вимкнення чи зашифровування. В увімкнених пристроях містяться енергозалежні дані, які є нестійкими, їхнє незбереження може призвести до їх втрати. Зокрема, в оперативній пам'яті сучасних комп'ютерів може міститися значна кількість інформації, включаючи дані про процеси, сервіси, користувачів, відкриті порти, кеш ARP та DNS, інформація про автоматично завантажені додатки, незбережені документи та інші. Важливо враховувати, що доступ до таких даних регулюється законодавством країни, де фізично знаходиться пристрій. У деяких країнах може існувати заборона на виїмку такої інформації, навіть у режимі реального часу.

З метою збереження енергозалежних даних під час обшуку слід провести огляд та документування кожного пристрою, визначити, вилучити та фотографувати їх, а також ізолювати підозрюваних та інших осіб від комп'ютерного обладнання для запобігання можливих змін чи знищенню доказів. Отримання електронних доказів у ввімкнених пристроях повинно виконуватися кваліфікованим фахівцем, таким як працівник кіберполіції, з використанням спеціальних знань, засобів та програм. Проведений огляд та отримана інформація обов'язково реєструються у протоколі [2].

Отримання електронних доказів може бути спрощено за допомогою чіткої та систематизованої процедури. Пропонуємо алгоритм, який може полегшити цей процес:

1. Визначення цілей розслідування – сформулювати основні завдання та мету розслідування економічних злочинів.
2. Оцінка ризиків та підготовка – визначити можливі ризики та труднощі. Розробити план підготовки, включаючи ресурси та інструменти.
3. Одержання санкцій та дозволів – забезпечити юридичну легітимність, отримавши необхідні санкції та дозволи.

4. Ідентифікація джерел даних – визначити електронні пристрої для обстеження та ідентифікувати джерела цифрової інформації.

5. Захист інтегритету даних – зберегти цілісність існуючих даних та застосувати технічні засоби для їхнього захисту.

6. Здійснення копіювання та аналізу даних – копіювати дані з електронних пристроїв, використовуючи спеціальні програми. Використовувати аналітичні інструменти для ефективного аналізу інформації.

7. Збір метаданих – фіксувати метадані для встановлення обставин та доказової бази.

8. Документування та складання протоколу – систематизувати отримані докази та створити чіткий протокол проведених дій та результатів.

9. Експертна оцінка – залучити фахівців для проведення експертизи отриманих електронних доказів.

10. Підготовка для судового захисту – забезпечити юридичну валідність та придатність отриманих доказів для судового захисту.

Використання технологій отримання електронних доказів, зокрема, в контексті розслідування економічних злочинів, є вкрай корисним та ефективним підходом у сучасному правоохоронному процесі. Застосування алгоритму, який охоплює всі етапи отримання та аналізу цифрової інформації, дозволяє забезпечити систематичний та логічний підхід до збору електронних доказів. Зокрема, визначення цілей та оцінка ризиків розслідування, правильне отримання санкцій та дозволів, а також ефективна ідентифікація та захист джерел даних стають провідними факторами успішного проведення розслідувань. Систематичний аналіз метаданих та документування отриманих результатів забезпечують якість та достовірність електронних доказів [3]. Залучення фахівців для проведення досліджень та підготовка отриманих доказів для судового захисту підкреслюють важливість глибокого розуміння та високої кваліфікації в цій області. Використання цих технологій дозволяє зробити розслідування економічних злочинів більш ефективним, точним та відповідним до сучасних викликів у сфері правоохоронної діяльності.

Список використаних джерел:

1. Романюк Б.В. Сучасні криміналістичні та правові проблеми використання спеціальних знань у досудовому слідстві: Автореф. дис.... к.ю.н.: 12.00.09 // Національна академія внутрішніх справ України. – К., 2002. – 20 с.

2. Стащак М. В. Особливості взаємодії оперативних підрозділів органів внутрішніх справ України з органами досудового розслідування під час протидії злочинам у сфері економіки. Право і безпека. 2012. № 5 (47). С.186–189.

3. Алєксєєва О. О. Розслідування окремих видів злочинів: навч. посіб. 2-ге вид. перероб. та доп. / О. О. Алєксєєв, В. В. Веселовський, В. В. Пясецький. – К.: Центр навчальної літератури, 2014. – 320 с.

4. Бідняк В. А., Бідняк Г. С., Чаплинський К. О. Теоретичні, правові та праксеологічні засади використання спеціальних знань під час розслідування злочинів, пов'язаних із державним фінансуванням в галузі охорони здоров'я: монографія. Одеса: Видавничий дім Гельветика, 2021, 260 с.