запобігання як виключення з доказування практичних операцій з формування доказів (а отже, і їх недооцінка), так й ігнорування правил логіки доказування й зумовлені цим спроби визначити достатність доказів на рівні інтуїції, усвідомленні посадовою особою.

Література:

1. Кримінальний процесуальний кодекс України [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/4651–17

2. Степаненко А. С. Стандарт доказування «поза розумним сумнівом» у кримінальному провадженні : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09, Одеса, 2017. 20 с.

3. Трофименко В. М. Теоретичні та правові основи диференціації процесуальноїформи у кримінальному судочинстві : монографія. Харків : ТОВ «Оберіг», 2016. 304 с.

4. Удалова Л. Д., Токаренко К. В. Закриття кримінального провадження: Монографія. Київ : Видавничийцентр «Кафедра», 2016. 168 с.

5. Шейфер С.А. Доказательства и доказывание по уголовным делам: проблемы теории и правового регулирования : монография. Москва : Норма, 2009. 239 с.

6. Строгович М.С. Курс советского уголовного процесса. Москва, 1971. Т. 1. 470 с.

DOI https://doi.org/10.36059/978-966-397-287-9-109

ДЕЯКІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ В УКРАЇНІ ПІД ЧАС ВОЄННОГО СТАНУ

Дунаєва Тетяна Євгенівна

кандидат юридичних наук,
науковий співробітник відділу дослідження проблем
кримінального процесу та судоустрою
Науково-дослідного інституту вивчення проблем злочинності
імені академіка В. В. Сташиса
Національної академії правових наук України
м. Харків, Україна

При розслідуванні кримінальних проваджень у сфері кіберзлочинності є важливим проведення всебічного та швидкого досудового розслідування для подальшого встановлення наявності або відсутності вини особи.

Виявлення та розслідування кіберзлочинів становить цілу програму поетапно здійснених заходів, передбачених кримінально-процесуальним законодавством. Нові звіти та цифрові інформаційні агентства свідчать про зростання кіберзлочинності, що свідчить, що розслідування кіберзлочинів відіграє вирішальну роль у забезпеченні безпеки Інтернету.

Слід зазначити, що законодавець вніс такі зміни у кримінальне процесуальне законодавство, як: у абз. 2 ч. 6 ст. 236 КПК передбачається, що під час обшуку слідчий, прокурор зможе отримувати доступ до комп'ютерних систем або їх частин, мобільних терміналів систем зв'язку без попереднього дозволу, за умови, що інформація, яка на них міститься, має значення для встановлення обставин у кримінальному провадженні. Так, у ч. 2 ст. 237 КПК зазначено, що огляд комп'ютерних даних проводиться слідчим, прокурором шляхом відображення у протоколі огляду інформації, яку вони містять, у формі, придатній для сприйняття їх змісту (фото, відео тощо). А ст. 245-1 КПК запроваджується нова слідча (розшукова) дія – зняття показань технічних приладів та технічних засобів, що мають функції фото-, кінозйомки, відеозапису, чи засобів фото-, кінозйомки, відеозапису, яка проводиться на підставі постанови слідчого, прокурора. У ч. 5 ст. 268 КПК зазначається, що установлення місцезнаходження радіообладнання (радіоелектронного засобу) тепер за заявою його власника не потребує дозволу слідчого судді [1].

Велику увагу під час проведення досудового розслідування у кримінальному провадженні займають особливості доказування кіберзлочинів, встановлення механізму доказування та визначення джерел доказів.

Слід зазначити, що діяльність, яку виконує розслідувач комп'ютерних злочинів, включає відновлення файлових систем зламаних комп'ютерів, отримання даних, які можуть бути використані як докази для переслідування злочинів, написання звітів для використання в судочинстві та дача свідчень на судових засіданнях.

Методи розслідування кіберзлочинів включають: перевірку даних, збір інформації, проведення цифрової криміналістики, відстеження авторів кіберзлочинів.

Перевірка даних – це встановлення того, коли, де та хто вчинив злочин, створює основу для розслідування. Ця техніка використовує публічні та приватні записи та бази даних, щоб з'ясувати історію осіб, потенційно причетних до злочину.

Збір інформації – цей метод є одним із найважливіших у розслідуванні кіберзлочинів. Основою для успішного розслідування є відповіді на запитання: які докази можна знайти і який рівень доступу до джерел ми маємо для збору доказів?

Проведення цифрової криміналістики – коли розслідувачі кіберзлочинності використовують свої цифрові та технологічні навички для проведення криміналістики, яка передбачає використання технологій і наукових методів для збору, збереження й аналізу доказів під час розслідування. Дані судової експертизи можуть бути використані для підтвердження доказів або підтвердження причетності підозрюваного до злочину.

Відстеження авторів кіберзлочинів: маючи в руках інформацію про кіберзлочини, слідчі з кіберзлочинності співпрацюють з інтернет-провайдерами, телекомунікаційними та мережевими компаніями, щоб визначити, які веб-сайти та протоколи використовувалися під час злочину. Ця техніка також корисна для моніторингу майбутньої діяльності за допомогою цифрового спостереження. Дозвіл на здійснення таких видів діяльності слідчі повинні отримувати через ухвали суду.

До органів, що проводять розслідування кіберзлочинів належать: органи кримінальної юстиції, органи національної безпеки, приватні охоронні агенції [2].

Отже, серед особливостей розслідування кіберзлочинів, їх ефективного та продуктивного переходу на місце цифрового злочину потрібні вірно вибрані різні інструменти і методи розслідування. Це сприятиме збереженню нормальної роботи нашій підприємств та установ нашої державі, критичної інфрастурктури, а також захистить майно та права людини та громадянина.

Література:

1. Єрема М., Борисенко А. Боротьба з кіберзлочинністю в умовах дії воєнного стану: Закон 2149-IX. *Юрліга. 13.04.2022.* URL: https://jurliga.ligazakon.net/analitycs/210562_borotba-z-kberzlochinnstyu-v-umovakh-d-vonnogo-stanu-zakon-2149-ix.

2. Естебан Борхес. Пояснення інструментів і методів розслідування кіберзлочинів. *Securitytrails.* URL: https://securitytrails.com/blog/cyber-crime-investigation.