відходи) небезпечні відходи IV класу небезпеки розділено на 2 окремих підкласи: малонебезпечні та малонебезпечні нетоксичні відходи гірничої промисловості із різними ставками податку. У Податковому кодексі України та пов'язаних із ним нормативно-правових актах відсутнє визначення терміну малонебезпечні нетоксичні відходи гірничої промисловості та порядок віднесення відходів до цього підкласу.

Такий розподіл за класами небезпеки підтверджено Кодифікатором відходів (Додаток 9 Податкової декларації екологічного податку, затвердженої наказом Міністерства фінансів України). Ним не враховано, що відповідно до вітчизняного природоохоронного законодавства в разі неможливості встановлення класу небезпеки відходів, вони автоматично належать до 1-го класу небезпеки.

У державному статистичному спостереженні щодо утворення та поводження з відходами (форма № 1-в річна) [4] слід зазначати клас небезпеки відходів.

Згідно з роз'ясненнями Державної служби статистики України [5], клас небезпеки відходів, визначений відповідно до чинних нормативних документів, розподілено на 4 класи за Законом «Про відходи». Отже, відходи розподіляють на чотири класи небезпеки і поняття «токсичності» відходів відсутнє.

Враховуючи наведене вище, можна дійти висновку, що розподіл небезпечних відходів за класами небезпеки з метою оподаткування за розміром ставки екологічного податку за розміщення відходів суперечить розподілу з метою державних статистичних спостережень та Закону України «Про відходи». Слід враховувати, що Податковий кодекс України та Закон України «Про відходи» є законодавчими актами одного рівня.

Але сам Податковий кодекс вказує шлях усунення цього протиріччя на практиці. Згідно з п. 4.1.4 Податкового Кодексу України «презумпція правомірності рішень платника податку в разі, якщо норма закону чи іншого нормативно-правового акта, виданого на підставі закону, або якщо норми різних законів чи різних нормативно-правових актів припускають неоднозначне (множинне) трактування прав та обов'язків платників податків або контролюючих органів, внаслідок чого є можливість прийняти рішення на користь як платника податків, так і контролюючого органу». Тому виробник відходів має право відповідно до вимог ст. 34 Закону України «Про відходи» самостійно визначати відповідний клас небезпеки у спосіб, що не заперечить вимогам законодавства України з відповідним зазначенням його у державних статистичних спостереженнях. Але цей шлях іноді породжує конфлікт з фіскальними органами, який можуть вирішуватися у судовому порядку. У цьому випадку роль судової екологічної експертизи стає визначальною.

Список використаних джерел

1. Податковий кодекс України від 02.05.2010 р. № 2755-VI (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2755-17/ed20210225 (дата звернення: 26.02.2021).
2. Про відходи : Закон України від 05.03.1998 р. № 187/98-ВР (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/187/98-вр (дата звернення: 26.02.2021).
3. Державні санітарні правила та норми 2. Комунальна гігієна. 2.7. Грунт, очистка населених місць, побутові та промислові відходи, санітарна охорона грунту. «Гігієнічні вимоги щодо поводження з промисловими відходами та визначення їх класу небезпеки для здоров'я населення». ДСанПіН 2.2.7.029-99. { Щодо зупинення дії Постанови з 16.09.2014 див. Повідомлення Державної служби України з питань регуляторної політики та розвитку підприємництва (n0009773-14) від 20.09.2014 р.}. Постанова Головного державного санітарного лікаря України від 01.07.1999 р. № 29. URL: https://zakon.rada.gov.ua/rada/show/v0029588-99?lang=ru (дата звернення: 26.02.2021).
4. Про затвердження форми державного статистичного спостереження № 1-відходи (річна) «Утворення та поводження з відходами» : наказ Державної служби статистики України від 19.06.2020 р. № 190 (зі змін. та допов.). URL: https://zakon.rada.gov.ua/rada/show/v0190832-20 (дата звернення: 26.02.2021).
5. Роз'яснення щодо форми державного статистичного спостереження № 1-відходи (річна) «Утворення та поводження з відходами» від 21.08.2020 р. № 19.1.2-12/25-20. URL: http://www.ukrstat.gov.ua/metaopus/2021/3_01_00_02_2021.htm (дата звернення: 26.02.2021).

В. С. Бондар,

кандидат юридичних наук, доцент, докторант ННЦ «ІСЕ ім. Засл. проф. М. С. Бокаріуса», декан факультету підготовки фахівців для підрозділів Національної поліції України Луганського державного університету внутрішніх справ імені Е. О. Дідоренка, м. Сєвєродонецьк, Україна,

ORCID: https://orcid.org/0000-0003-1552-4555, e-mail: bondarlivd@gmail.com

ОСОБЛИВОСТІ ВИРІШЕННЯ ТЕХНІКО-КРИМІНАЛІСТИЧНИХ ЗАВДАНЬ ДОСУДОВОГО РОЗСЛІДУВАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ

Анотація. *Досліджено сутність техніко-криміналістичної ситуації та висвітлено особливості вирішення техніко-криміналістичних завдань досудового розслідування кримінальних правопорушень. Виокремлено елементи дій спеціалістів у типових техніко-криміналістичних ситуаціях для подальшого їх використання як криміналістичних алгоритмів і програм досудового розслідування конкретних видів (груп) кримінальних правопорушень.*

Ключові слова: *досудове розслідування, кримінальне провадження, криміналістична алгоритмізація, матеріальні сліди-відображення, техніко-криміналістичні завдання, техніко-криміналістична ситуація.*

Abstact. *The essence of the technical and forensic situation is investigated and the features of the solution of technical and forensic tasks of the pre-trial investigation of criminal offenses are revealed. The elements of the actions of specialists in typical technical and forensic situations are highlighted, with the aim of their further use in the form of forensic algorithms and programs for pre-trial investigation of specific types (groups) of criminal offenses.*

Keywords: *pre-trial investigation, criminal proceedings, forensic algorithmization, material traces-mapping, technical and forensic tasks, technical and forensic situation.*

Аннотация. *Исследована сущность технико-криминалистической ситуации и раскрыты особенности решения технико-криминалистических задач досудебного расследования уголовных правонарушений. Выделены элементы действий специалистов в типичных технико-криминалистических ситуациях с целью дальнейшего их использования в виде криминалистических алгоритмов и программ досудебного расследования конкретных видов (групп) уголовных правонарушений.*

Ключевые слова: *досудебное расследование, уголовное производство, криминалистическая алгоритмизация, материальные следы-отображения, технико-криминалистические задачи, технико-криминалистическая ситуация.*

Оптимізація діяльності з виявлення та розслідування кримінальних правопорушень, створення сучасних криміналістичних методик і технологій тісно пов'язані з аналізом її структури, тобто виокремленням з її складу важливих елементів і наявних між ними інформаційних та функціональних зв'язків [1; 2; 4].

Системний аналіз слідчої, судово-експертної й техніко-криміналістичної діяльності базується на тріаді: завдання — об'єкт — метод. Система завдань у будь-якій системі діяльності є інтегральним елементом, який визначає структуру діяльності. У криміналістичній літературі для позначення подібних ситуацій послуговуються терміном «техніко-криміналістична ситуація», який визначають як обстановку, що склалася на певний момент розслідування й зумовлює необхідність застосування під час розслідування конкретних науково-технічних засобів і методів, а також виявляється у специфічному характері криміналістичних завдань, вирішуваних у такій ситуації. Як приклад наведемо ситуації, у яких фахівці вирішують техніко-криміналістичні завдання в кримінальних провадженнях, коли досліджують комп'ютерну інформацію: а) наявність об'єктів кримінально-протиправних посягань у вигляді фальсифікованих даних бухгалтерського або іншого обліку, наявність захисних програмних засобів з ознаками злому, скоригованих або змінених персональних даних тощо; б) комп'ютерна інформація та техніка є засобами вчинення кримінального правопорушення або засобами зв'язку; в) комп'ютерна інформація (техніка) характеризує певний об'єкт у кримінальному провадженні, при цьому не є об'єктом кримінально-протиправного впливу або засобом учинення кримінального правопорушення (дані з відеокамер спостереження, відеореєстраторів та інших технічних засобів руху транспортних засобів тощо).

Сучасна слідча й судова практика містить численні приклади успішного використання в доказуванні вини осіб, які вчинили кримінальні правопорушення інформації, здобутої від операторів мобільного зв'язку. Утім, і злочинці, обізнані із сучасними можливостями органів правопорядку, вживають відповідні заходи для приховування своєї кримінально-протиправної діяльності: використовують методи шифрування інформації із застосуванням спеціалізованих програмних продуктів типу *TrueCrypt, Steganos Safe*, за допомогою яких флеш-накопичувач або жорсткий диск перетворюється на захищене зашифроване сховище, у якому конфіденційна інформація прихована від сторонніх. Ця обставина, зі свого боку, формує систему техніко-криміналістичних завдань, орієнтовану на ситуацію протидії нормальному перебігу кримінального провадження. Для прикладу наведемо деякі завдання спеціаліста під час вилучення електронних носіїв інформації:

- надання консультативної допомоги під час вироблення тактики слідчої (розшукової) дії на етапі її планування та підготовки — із метою отримання компетентних роз'яснень щодо доступності електронних доказів і необхідності вжиття заходів для їх збереження;
- виявлення слідів екстреного знешкодження інформації;
- визначення способів нейтралізації засобів екстреного знешкодження інформації;
- виявлення ознак застосування мережевих «хмарних» технологій зберігання даних (*iCloud*);
- виявлення засобів шифрування даних і криптографічних контейнерів, фіксування їх змісту;
- виявлення систем дублювання та резервного зберігання інформації;
- надання допомоги слідчому (дізнавачеві) під час складання протоколу в описі об'єктів;
- копіювання даних, пошук і вилучення конкретної значущої інформації;
- фіксування інформації з видалених мережевих ресурсів, виявлення ідентифікаційних даних;
- визначення криміналістично значущих даних про використовувану операційну систему та програмне забезпечення;
- виявлення відомостей про підключені раніше до комп'ютера електронні носії.

Звідси випливає й «необхідний мінімум» програмного забезпечення та пристроїв, потрібний для проведення слідчої (розшукової) дії: програми для зняття знімка (дампу) оперативної пам'яті (наприклад, *Belkasoft RAM Capturer, ProcDump*); пристрої, які дають змогу вивчати зміст файлової системи в режимі «тільки читання»; пристрої-блокіратори для копіювання НЖМД/*SSD*, які виключають можливість внесення змін на вихідний диск.

Особливої актуальності останнім часом також набуває поширення кримінальних правопорушень, фігуранти яких активно послуговуються мобільними засобами зв'язку для координації своїх дій. Найбільш надійним та ефективним засобом здійснення кримінально-протиправної діяльності таких осіб є застосування месенджерів (*Telegram*), які забезпечують конфіденційне спілкування в таємних чатах із застосуванням ефективних алгоритмів шифрування даних. Водночас у разі визначення списку контактів на вилученому пристрої особи, запідозреної в причетності до кримінального правопорушення, можна виявити її потенційних учасників та отримати доступ до

їхнього листування за допомогою алгоритму ідентифікації користувачів у мережі.

Уявімо, що в результаті реалізації матеріалів оперативно-розшукової діяльності відбулося затримання фігуранта, під час якого у цієї особи вилучено мобільний пристрій зі встановленим на ньому месенджером, що використовує схему шифрування на основі алгоритмів Діффі-Хелмана (*Diffie-Hellman Key Exchange, DHKE*), Ель-Гамаля, *MTI/A(0), STS*. У подібній техніко-криміналістичній ситуації послідовність дій спеціаліста відповідного фаху може бути такою:

- отримання доступу до пристрою за наявності початкових елементів захисту (паролів, *PIN*-кодів) за допомогою відповідних програмно-апаратних комплексів;
- вилучення даних (діалогів) зі встановленого месенджеру, з'ясування списку користувачів, яких перевіряють;
- ініціювання запиту до компанії, яка є власником месенджеру, для отримання наявних відомостей про користувачів (рівень активності, *IP*-адреса, інформація про пристрій, із якого здійснюється вхід, місце розташування тощо);
- побудова ймовірнісних зв'язків між користувачами (створення соціального графа), визначення даних з'єднання. Через те, що технологія кінцевого шифрування передбачає часту зміну ключів (зазвичай із періодичністю від 10 хвилин до 1 години), то саме така тактика дасть змогу здобути максимальну кількість інформації;
- на підставі статистичних характеристик трафіку, який передається з обох сторін, здійснюють їхній аналіз та обчислюють обсяг даних, переданих за одиницю часу. Подібні дії повторюють із масивом даних передавання трафіка інших користувачів, виявляють зв'язки;
- встановлення контролю за каналом зв'язку фігурантів. Може бути запроваджений за допомогою програмних продуктів і модифікацій (налаштування мережевого моста, *root*-керування шлюзом тощо) та програмно-апаратних засобів перехоплення й аналізу трафіку (створені з використанням технологій *DPI* (англ. *Deep Packet Inspectiom*)), які дають змогу здійснити глибокий аналіз пакетів, що проходять у мережі;
- реалізація атаки «людина посередині» (англ. *Man-in-the-Middle, MITM*), яка полягає у впровадженні клієнта-посередника між двома користувачами, що комунікують. У такий спосіб листування підозрюваних із визначеного кола користувачів може бути розшифровано стороннім спостерігачем у межах негласної слідчої розшукової дії (ст. 263 КПК України «Зняття інформації з транспортних телекомунікаційних мереж»);
- фіксування відомостей, відображення їх у висновку експерта (спеціаліста).

Список використаних джерел

1. Головин А. Ю., Баранов М. В., Головина Е. В. Решение ситуационных задач предварительного расследования (теория, механизм, ошибки) : монография / под общ. ред. докт. юрид. наук А. Ю. Головина. Москва : Юрлитинформ, 2017. 200 с.
2. Сегай М. Я., Бондар В. С. Інтегративна модель використання спеціальних криміналістичних знань у кримінальному судочинстві. Вісник академії адвокатури України. 2008. Вип. 13. С. 92—95.
3. Шаталов А. С. Алгоритмизация и программирование расследования преступлений в системе криминалистической методики // Право. Журнал Высшей школы экономики. 2017. № 2. С. 155—172.
4. Шепітько В. Ю. Предмет криміналістичної тактики: історія формування, зміст та тенденції // Теорія та практика судової експертизи і криміналістики : зб. наук. пр. Харків, 2019. № 19. С. 8—20.

І. І. Бордакова,
головний судовий експерт Сумського НДЕКЦ МВС України, м. Суми, Україна,
ORCID: https://orcid.org/0000-0003-0997-2685, e-mail: bordachok.2011@ukr.net

СУЧАСНИЙ СТАН ФОРМУВАННЯ І РЕАЛІЗАЦІЇ ЕКСПЕРТНИХ ТОВАРОЗНАВЧИХ ДОСЛІДЖЕНЬ

Анотація. *Ефективність та якість експертного забезпечення правосуддя України залежать від чіткої законодавчої регламентації діяльності з питань призначення і проведення судової експертизи та відповідності цих норм іншим актам законодавства України. Розглянуто декілька проблемних моментів під час призначення товарознавчих експертиз з посиланням на нормативно-правову базу.*

Ключові слова: *продукція, товар, якість, вартість, ринок, правопорушення.*

Abstract. *The efficiency and quality of forensic expert support of justice in Ukraine depend on clear legislative regulation of activities on appointment and conduct of forensic examination and compliance of these rules with other acts of Ukrainian legislation. Several problematic points in the appointment of forensic commodity examinations with reference to regulatory framework are considered.*

Keywords: *products, goods, quality, value, market, offense.*

Аннотация. *Эффективность и качество экспертного обеспечения правосудия Украины зависят от чёткой законодательной регламентации деятельности по вопросам назначения и проведения судебной экспертизы и соответствия этих норм другим актам законодательства Украины. Рассмотрено несколько проблемных моментов при назначении товароведческой экспертизы со ссылкой на нормативно-правовую базу.*

Ключевые слова: *продукция, товар, качество, стоимость, рынок, правонарушение.*