Судова експертиза в умовах воєнного стану

Тетяна Заікіна
завідувачка відділу комп'ютерно-технічних
та телекомунікаційних досліджень, Науково-дослідний центр
незалежних судових експертиз Мін'юсту України, м. Київ, Україна,
ORCID: https://orcid.org/000-0002-3839-5859, e-mail: zaikina.tv@ukr.net

Розглянуто проблеми й виклики в судово-експертній діяльності внаслідок збройної агресії рф проти України. Запропоновано застосування новітніх цифрових технологій, застосування мобільних лабораторій та інноваційних методів дослідження для підвищення ефективності судових експертиз в умовах воєнного стану, зокрема, у районах ведення активних бойових дій. Досліджено важливість цифрової криміналістики для опрацювання значних обсягів даних (зокрема, із застосуванням технологій штучного інтелекту).
Ключові слова: *судова експертиза; воєнний стан; цифрова криміналістика; мобільні лабораторії; кіберінциденти; штучний інтелект.*

Forensic Examination in Martial Law Context

Tetiana Zaikina

Primary concerns of this paper are problems and challenges in forensic expert activities due to the Russian Federation's armed aggression against Ukraine. It is proposed to utilize state-of-the-art digital technologies, mobile laboratories, and innovative research methods to enhance the efficiency of forensic examinations under martial law, specifically in areas of active hostilities. The author explores the importance of digital forensics for processing large data amounts (in particular, using artificial intelligence technologies).
Keywords: *forensic examination; martial law; digital forensics; mobile laboratories; cyber incidents; artificial intelligence.*

Як особливий правовий режим воєнний стан в Україні запроваджено з 2022 року, після початку повномасштабного вторгнення російської федерації, що стало істотним викликом для всього українського населення — від простих громадян до представників державної влади, зокрема для суб'єктів судово-експертної діяльності — науково-дослідних установ судових експертиз Міністерства юстиції України.

Складні й загрозливі умови праці співробітників установ судових експертиз є наслідком збройної агресії рф проти України. Постійні повітряні

атаки, бомбардування, обстріли цивільних об'єктів та об'єктів критичної інфраструктури, масовані кібератаки й різноманітні інциденти у цифровій сфері створюють значні труднощі для оперативного реагування на загрози, якісне та своєчасне проведення судових експертиз, опрацювання значних обсягів інформації.

З огляду на викладене вище та зважаючи на міжнародний досвід країн-партнерок у галузі ціфровізації та інновацій [1], особливого значення в оперуванні цифровими даними (виявлення, збір, ідентифікація, збереження, відновлення пошкоджених або втрачених даних тощо), зокрема, щодо військових злочинів, набувають інструменти діджиталізації — цифрові технології та штучний інтелект (далі — *ШІ*).

Застосування згаданих інструментів також є дуже важливим для оперативного відновлення державних інформаційно-телекомунікаційних систем, програмно-апаратних сервісів і комплексів у разі їх пошкодження країною-агресоркою.

Аналіз даних у цифровому вигляді із застосуванням криміналістичного спеціалізованого програмного забезпечення на основі ШІ із застосуванням дистанційних методів поводження з доказами дає змогу ефективно проводити судові експертизи або окремі процесуальні дії в межах експертиз навіть у складних умовах воєнного стану з урахуванням виявлених дослідниками певних переваг і недоліків відповідних баз даних та алгоритмів роботи ШІ [2].

У таких умовах фізичний доступ судових експертів до об'єктів дослідження, які перебувають у зонах ведення бойових дій, є обмеженим, самі об'єкти можуть бути пошкодженими (транспортні засоби, озброєння та військова техніка, комп'ютерні й автоматизовані системи тощо), що негативно позначається на часових показниках і взагалі можливості проведення експертних досліджень та необхідних процесуальних дій.

Для розв'язання цієї проблеми доцільним є застосування дистанційних методів збору доказів (фотографування, копіювання електронних файлів даних, відеофіксування з використанням безпілотних літальних апаратів (дронів) тощо).

Слід звернути увагу, що під час вогневого ураження рф інфраструктури України часто відбувається фізичне пошкодження або повне знищення об'єктів, що підлягають дослідженню в межах експертизи. Це значно обмежує або (в окремих випадках) унеможливлює проведення експертних досліджень, визначених відповідними методиками, проведення повного дослідження у межах судової експертизи із застосуванням традиційних методів. Така ситуація потребує розроблення та застосування нових підходів до поводження із даними, зокрема високотехнологічних цифрових технологій на основі ШІ [3].

Наприклад, пошкодження комп'ютерної техніки, серверів, інших електронних пристроїв потребуватиме відновлення втрачених

даних із залишкових елементів або резервних / хмарних сховищ. У таких випадках експерти застосовують методи цифрової криміналістики для відновлення інформації з пошкоджених носіїв або аналізу даних, зібраних до знищення обладнання. Такі дії можуть містити відновлення файлів із частково пошкоджених носіїв даних, аналіз залишків цифрових слідів (облікових записів і даних авторизації у хмарних / мережевих ресурсах та сервісах) або навіть фрагментів даних (окремих складових елементної бази електронних устаткувань), що залишилися після фізичного пошкодження [2, 4].

Україна також стикається зі значним зростанням кіберінцидентів, включно з атаками на критичну інфраструктуру, державні установи, військові системи та приватний сектор. Уже давно кібератаки стали складовою сучасної війни, ворог уражає слабкі місця ІТ-інфраструктури, блокує окремі інформаційні системи, викрадає важливі дані, руйнує критичні державні сервіси шляхом застосування шкідливого програмного забезпечення.

Цифрова криміналістика кіберінцидентів є невід'ємною складовою сучасної судово-експертної діяльності, що висуває високі вимоги до професійних знань, навичок і забезпеченості експертів сучасним обладнанням (мобільні автоматизовані робочі місця / лабораторії на базі спеціалізованого програмного забезпечення, спеціалізованих апаратних і програмних засобів на основі ШІ) для швидкого й ефективного реагування на можливі ІТ-загрози на всіх етапах: від моменту виявлення, блокування, фіксування, збирання цифрових доказів із пошкоджених систем, аналізування виявленого шкідливого коду — до визначення джерела походження кібератаки й ідентифікації її виконавців.

Важливо зауважити, що проведення експертиз сучасних ІТ-інцидентів потребує дослідження значного обсягу даних у цифровому вигляді та, відповідно, значних витрат часу на проведення інструментальних досліджень об'єктів експертизи [3, 4].

У проведенні судових експертиз системи на основі ШІ не замінять судового експерта, але на етапах пошуку та первинного інструментального аналізу цифрових доказів значно прискорять процес опрацювання значних обсягів даних, дадуть змогу оперативно реагувати на загрози.

Підбиваючи підсумки викладеного вище, убачаємо, що проведення судових експертиз в інформаційно-телекомунікаційній сфері в умовах війни потребує впровадження більш широкої діджиталізації, удосконалення наявних і розроблення нових методів та методик (стандартних операційних процедур) дослідження, застосування новітніх технологій на основі ШІ та мобільних автономних експертних модулів / лабораторій, підвищення професійної підготовки експертів з урахуванням досвіду країн-партнерок у відповідній предметній сфері.

Перелік джерел посилання

1. Матуєлене С., Шевчук В., Балтрунене Б. Штучний інтелект в діяльності органів правопорядку та юстиції: вітчизняний та європейський досвід. *Теорія та практика судової експертизи і криміналістики*. 2022. Вип. 4 (29). С. 12—46. DOI: 10.32353/khrife.4.2022.02 (дата звернення: 05.10.2024).
2. Нестор Н. В. Штучний інтелект у судовій експертизі: загроза чи перспектива? *Криміналістика і судова експертиза*. 2024. Вип. 69. С. 85—88. DOI: 10.33994/kndise.2024.69.07 (дата звернення: 05.10.2024).
3. Плахотнік О. В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4. DOI: 10.17721/2413-5372.2019.4/45-57 (дата звернення: 05.10.2024).
4. Документування воєнних злочинів: як система БПД долучається до збору доказів порушення прав людини / Вільшанська громада : офіц. сайт. 15.06.2022. URL: https://vilshsr.gov.ua/news/1655288046/ (дата звернення: 05.10.2024).