УДК 343.98+004.94 doi: 10.37025/1992-4437/2018-30-2-116

В. А. Поліщук
Тернопільський науково-дослідний експертно-криміналістичний центр МВС України
V. A. Polishchuk
Ternopil Scientific Research Forensic Centre, MIA of Ukraine

ОСОБЛИВОСТІ ЕКСПЕРТНОГО ЕКСПЕРИМЕНТУ ПІД ЧАС ПРОВЕДЕННЯ СУДОВИХ КОМП'ЮТЕРНО-ТЕХНІЧНИХ ЕКСПЕРТИЗ

THE FEATURES OF FORENSIC EXPERIMENT DURING COMPUTER-TECHNICAL EXPERTISE

Розроблено алгоритм експертного експерименту, який дає змогу здійснювати більш глибокий і ретельний аналіз результатів дослідження. Висвітлено переваги та недоліки типових методів проведення експертного експерименту. Аргументовано вибір тих чи інших методів, опрацьовано алгоритми їх комплексного використання. Для окремих методів проведення експертного експерименту запропоновано програмні засоби, технічні рішення, зважаючи на завдання, розв'язувані під час судових комп'ютерно-технічних експертиз. Охарактеризовано основні методи проведення експертного експерименту. Сформульовано рекомендації з найоптимальнішого їх застосування та вирішення експертних завдань. Окреслено процесуальні особливості та обмеження, які можуть виникнути в разі проведення експертного експерименту під час виконання судових комп'ютерно-технічних експертиз.

Ключові слова: експеримент; моделювання; віртуалізація; спостереження; накопичувачі інформації; операційні системи.

Разработан алгоритм экспертного эксперимента, позволяющий осуществлять более глубокий и тщательный анализ результатов исследования. Раскрыты преимущества и недостатки типовых методов проведения экспертного эксперимента. Аргументирован выбор тех или иных методов, отработаны алгоритмы их комплексного использования. Для отдельных методов проведения экспертного эксперимента предложены программные средства, технические решения, учитывая задачи, решаемые в ходе судебных компьютерно-технических экспертиз. Охарактеризованы основные методы проведения экспертного эксперимента. Сформулированы рекомендации по наиболее оптимальному их применению и решению экспертных задач. Определены процессуальные особенности и ограничения, которые могут возникнуть при проведении экспертного эксперимента при выполнении судебных компьютерно-технических экспертиз.

Ключевые слова: эксперимент; моделирование; виртуализация; наблюдение; накопители информации; операционные системы.

The algorithm of an expert experiment is developed, which gives an opportunity to perform more detailed and substantial analysis of the research results. The advantages and disadvantages of typical methods of an expert experiment conduction are highlighted. The author gives

reasons for the choice of one or another method, develops algorithms for their complex use. For some methods of conducting an expert experiment the author suggests software tools and technical solutions, taking into account the tasks solved during forensic computer-technical expertise. The main methods of conducting an expert experiment are described in the article. Recommendations on the most optimal use of them and solving of expert tasks are given. The procedural peculiarities and limitations that may arise in the course of conducting an expert experiment during forensic computer-technical expertise are outlined.

Key words: experiment; modelling; virtualization; observation; data storage; operating system.

Об'єктами судових експертиз як результат інформатизації суспільства дедалі частіше стають цифрова техніка та інформація, а коло питань і завдань, вирішуваних експертами, постійно розширюється.

Інформація і комп'ютерна техніка являє собою об'єкт дослідження комп'ютерно-технічної експертизи – доволі молодого виду судової експертизи, що стрімко розвивається. Її основними завданнями є виявлення та аналіз інформаційних слідів злочинної діяльності, які часто мають прихований вигляд. Методи і засоби, якими послуговуються судові експерти під час досліджень, різні, що зумовлено колом питань, вирішуваних експертизою, наявною методичною і технічною базою. Доволі часто поставлені завдання можна розв'язати лише експертним експериментом.

Методологічні основи комп'ютерно-технічної експертизи започаткували у своїх працях О. Р. Россинська та О. І. Усов [1–3]. Але питання експертного експерименту в межах цього виду судових експертиз науковці практично не розглядали, не деталізували особливості його застосування.

Водночас, засвідчує практика, судові експерти застосовують різні підходи до експертного експерименту в межах комп'ютерно-технічних експертиз, бракує й єдиного алгоритму його проведення.

Метою статті є систематизація підходів до застосування експертного експерименту під час судових комп'ютерно-технічних експертиз, розроблення рекомендацій щодо вибору оптимального алгоритму його використання.

Експеримент – метод, заснований на досліді, що поставлений у певних умовах із метою перевірки гіпотези, відтворення певних явищ або подій, встановлення зв'язку з іншими явищами тощо. Метою експерименту є також з'ясування сутності досліджуваного об'єкта, можливості настання події за певних умов, визначення впливу будь-яких відхилень у нормальній діяльності на стан об'єкта тощо [4].

Експеримент порівняно з іншими методами дослідження дозволяє досліджувати об'єкти в так званому чистому вигляді, а також в умовах, наближених до реальних, що сприяє більш глибокому проникненню в їх сутність. Важлива перевага експерименту – його повторюваність. Основна відмінність від методу спостереження – те, що експеримент дає змогу активно впливати на стан досліджуваного об'єкта, спрямовуючи дослідження в необхідне русло. Активна фаза експерименту потребує від експерта ретельного планування, чіткого розуміння загальних та окремих завдань, способів фіксації результатів.

Застосовують метод експертного експерименту під час судових комп'ютерно-технічних експертиз і насамперед тоді, коли необхідно:

з'ясувати працездатність засобів комп'ютерної техніки (як загальну, так і поелементну);

встановити окремі технічні характеристики і параметри цифрових пристроїв (швидкість оброблення та передання даних, роздільна здатність цифрових камер, фактичний обсяг пам'яті носія тощо);

з'ясувати працездатність програмного забезпечення (умови забезпечення його працездатності);

визначити особливості функціонування програмного забезпечення (наявність чи відсутність певних функцій, алгоритм роботи, наявність елементів захисту інформації тощо);

вирішити ситуаційні завдання (можливість здійснення певних операцій з інформацією, програмними засобами і технікою за певних умов);

провести ідентифікаційні дослідження належності інформації (даних і файлів) до наданих цифрових пристроїв (створення експериментальних зразків у процесі дослідження);

дослідити «шкідливе» програмне забезпечення.

Наведений перелік не вичерпний і може бути доповнений.

Результат експертного експерименту значною мірою залежить від вибору методів та алгоритму його проведення. З огляду на те, що зазвичай використання одного методу недостатньо, доцільно застосовувати кілька методів із подальшим зіставленням отриманих результатів. При цьому, щоб забезпечити збереження стану досліджуваного об'єкта, у процесі дослідження вплив на нього зводять до мінімуму, тобто насамперед застосовують методи і засоби, які не змінюють досліджуваний об'єкт.

Проте вирішення низки завдань неможливе без внесення певних змін до наданого на експертизу об'єкта. Дозвіл на це має надати ініціатор дослідження після отримання інформації про особливості такого дослідження та можливі наслідки його проведення (як приклад, дослідження мобільного телефона на базі Android шляхом отримання root-прав може призвести до повної втрати інформації без можливості її відновлення).

Найпоширенішим методом проведення експертного експерименту під час дослідження комп'ютерної техніки є клонування носія інформації, що передбачає внесення в процесі експерименту змін у копію носія, при цьому основний об'єкт не змінюється. Попри те, що застосування цього методу дає змогу вирішити широке коло завдань, він має низку обмежень.

Так, окремі об'єкти не дозволяють підміняти носій даних (смартфони, ноутбуки із вбудованими накопичувачами тощо). Також в експерта може не бути носія з необхідним інтерфейсом чи обсягом. У цьому разі перед ініціатором дослідження порушують клопотання про надання накопичувача потрібного формату для створення копії.

Якщо клонувати носій даних неможливо, застосовують метод віртуалізації – створюють віртуальну копію досліджуваної системи з використанням цифрової копії (образу) накопичувача об'єкта дослідження. Для роботи з віртуальними машинами послуговуються низкою спеціалізованих програмних засобів: Microsoft Hyper-V, VMware Workstation, VirtualBox, Virtual PC, Genymotion Android Emulator тощо [5]. Обирають програмне забезпечення, зважаючи на досліджувану систему і завдання, поставлені перед експертом. Трапляється, що постає необхідність використання кількох систем віртуалізації, хоча застосування цього методу також має низку обмежень: метод є більш складним і потребує трудомістких підготовчих операцій. Зокрема, конфігурувати віртуальну копію системи для забезпечення її ко-

ректної роботи доволі складно (водночас не потребує додаткового налаштування використання копії носія даних).

Але провести дослідження зазначеним методом не завжди можливо. Електронні системи можуть містити прив'язку до апаратних засобів досліджуваної техніки і на віртуальних машинах не функціонувати або працювати некоректно. Крім того, якщо на дослідження надано окремий носій даних і вирішення поставлених завдань потребує дослідження динамічної системи, також послуговуються методом віртуалізації.

Під час експертного експерименту використовують і такий підвид віртуалізації, як так звана пісочниця – спеціально виокремлене середовище для безпечного виконання комп'ютерних програм [6]. На відміну від віртуальних машин ці системи призначені для дослідження окремих програм із максимальним аналізом їх активності. Метод використовують для дослідження «шкідливого» програмного забезпечення, комп'ютерних вірусів тощо. Найпоширенішими «пісочницями» є програми Sandboxie, Evalaze, Enigma Virtual Box, Cameyo, Spoon.net.

Якщо метод клонування чи віртуалізації застосувати неможливо або використання зазначених методів не забезпечило необхідного результату, досліджують безпосередньо наданий об'єкт. Таким способом послуговуються і в разі, коли неможливо зробити копію накопичувача пристрою, програмне забезпечення містить прив'язку до апаратних засобів, пристрій містить захищені накопичувачі даних тощо. Проте, як зазначалося, цей метод має бути узгоджений з ініціатором дослідження з огляду на потребу внесення змін до досліджуваного об'єкта. При цьому вплив на об'єкт дослідження має максимально мінімізуватися.

Тож, убачається доцільним запропонувати такий загальний алгоритм експертного експерименту:

з'ясування потреби в проведенні експертного експерименту, спираючись на поставлені перед експертом завдання і відомі методи проведення дослідження;

окреслення цілей експерименту, зважаючи на завдання, поставлені перед експертом, наявні апаратно-програмні засоби та особливості об'єкта дослідження;

визначення умов проведення експерименту, з'ясування наявності обмежень і потреби виконання додаткових заходів (надання додаткових матеріалів, дозволу на використання методів, що приводять до зміни об'єкта, тощо);

обґрунтування вибору методів і засобів проведення експерименту, програмно-апаратних комплексів, використовуваних у процесі дослідження, методів фіксації результатів;

складання покрокового алгоритму проведення експерименту;

спостереження, фіксація виявлених під час експерименту даних, зв'язків, тенденцій поведінки досліджуваного об'єкта;

аналітичне оброблення результатів експерименту, формування попередніх висновків;

визначення достатності отриманих результатів, наявності розбіжностей з іншими вихідними даними, з'ясування необхідності повторного чи додаткового експерименту (з тими самими чи зміненими вихідними даними);

формування висновків на основі отриманих результатів.

Експерт у своєму висновку має докладно зафіксувати умови проведення експертного експерименту, використані апаратні та програмні засоби, а також отримані результати.

Важливого значення набуває форма використання результатів експертного експерименту під час судової експертизи, які мають отримати експертну оцінку і логічно пов'язуватися зі змістом експертних висновків.

Крім того, під час експертного експерименту в процесі судової комп'ютерно-технічної експертизи потрібно чітко усвідомлювати межі компетенції судового експерта. Згідно з ч. 4 ст. 69 Кримінального процесуального кодексу України (далі – КПК України) експерт не має права з власної ініціативи збирати матеріали для проведення експертизи, зокрема коли виникає необхідність отримати додаткові дані із зовнішніх джерел, використовуваних як матеріал для дослідження [7]. Прикладом може слугувати дослідження програмного забезпечення, застосовуваного для організації азартних ігор. Щоб встановити алгоритм роботи таких програм, необхідно зареєструвати користувача на інтернет-сайті і надати програмі доступ до віддаленого сервера з використанням отриманих реєстраційних даних. Такі дії, проведені експертом самостійно, суперечитимуть зазначеній вище нормі КПК України. За потреби отримати додаткові дані для дослідження експерт має порушити клопотання перед ініціатором експертизи. Необхідні дані мають бути отримані в процесі слідчих дій і процесуально оформлюватися.

Висновки. Застосування експертного експерименту під час судових комп'ютерно-технічних експертиз, зважаючи на особливості його проведення, є важливим і ефективним інструментом, який дозволяє вирішити широке коло експертних завдань.

З огляду на постійний розвиток інформаційних технологій особливості судової комп'ютерно-технічної експертизи потребують подальших досліджень та узагальнень експертної практики.

References

1. Rossinskaya E. R. Sudebnaya kompyuterno-tehnicheskaya ekspertiza / E. R. Rossinskaya, A. I. Usov. M.: Pravo i zakon, 2001. 416 s.

2. Usov A. I. Metody i sredstva resheniya zadach kompyuterno-tehnicheskoj ekspertizy: ucheb. posobie / A. I. Usov. M.: GU EKC MVD Rossii, 2002. 368 s.

3. Usov A. I. Sudebno-ekspertnoe issledovanie kompyuternyh sredstv i sistem. Osnovy metodicheskogo obespecheniya: ucheb. posobie / A. I. Usov; pod red. E. R. Rossinskoj. M.: Ekzamen; Pravo i zakon, 2003. 368 s.

4. Metody issledovaniya v SKTE / Usov A. I., Edzhubov L. G., Hatuncev N. A., Karpuhina E. S. *Teoriya i praktika sudebnoj ekspertizy.* 2008. Vyp. 3 (11). S. 31–47.

5. *Obzor* virtualnyh mashin. Luchshaya virtualnaya mashina. URL: http://www.spy-soft.net/luchshaya-virtualnaya-mashina (data obrasheniya: 18.07.2018).

6. *Obzor* programm dlya raboty s virtualnymi pesochnicami. URL: https://www.ixbt.com/soft/sandboxes.shtml (data obrasheniya: 18.07.2018).

7. *Kryminalnyi* protsesualnyi kodeks Ukrainy: zakon vid 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (data zvernennia: 12.07.2018).

Список використаних джерел

1. *Россинская Е. Р.* Судебная компьютерно-техническая экспертиза / Е. Р. Россинская, А. И. Усов. М.: Право и закон, 2001. 416 с.

2. *Усов А. И.* Методы и средства решения задач компьютерно-технической экспертизы: учеб. пособие / А. И. Усов. М.: ГУ ЭКЦ МВД России, 2002. 368 с.

3. *Усов А. И.* Судебно-экспертное исследование компьютерных средств и систем. Основы методического обеспечения: учеб. пособие / А. И. Усов; под ред. Е. Р. Россинской. М.: Экзамен; Право и закон, 2003. 368 с.

4. *Методы* исследования в СКТЭ / Усов А. И., Эджубов Л. Г., Хатунцев Н. А., Карпухина Е. С. *Теория и практика судебной экспертизы.* 2008. Вып. 3 (11). С. 31–47.

5. *Обзор* виртуальных машин. Лучшая виртуальная машина. URL: http://www.spy-soft.net/luchshaya-virtualnaya-mashina (дата обращения: 18.07.2018).

6. *Обзор* программ для работы с виртуальными песочницами. URL: https://www.ixbt.com/soft/sandboxes.shtml (дата обращения: 18.07.2018).

7. *Кримінальний* процесуальний кодекс України: закон від 13.04.2012 № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 12.07.2018).

Стаття надійшла до редакції 03.08.2018