DOI: 10.30764/1819-2785-2018-13-1-121-124

Актуальные направления судебной экспертизы информационных технологий

Н.А. Хатунцев
Федеральное бюджетное учреждение Российский федеральный центр судебной экспертизы при Министерстве юстиции Российской Федерации, Москва 109028, Российская Федерация

Аннотация. Обсуждены актуальные направления развития судебной компьютерно-технической экспертизы по итогам 20-й ежегодной встречи рабочей группы Европейской сети судебно-экспертных учреждений (ENFSI) по информационным технологиям, прошедшей в ноябре 2017 года в Испании.

Ключевые слова: *судебная компьютерно-техническая экспертиза, информационные технологии, семинар, ENFSI*

Для цитирования: Хатунцев Н.А. Актуальные направления судебной экспертизы информационных технологий // Теория и практика судебной экспертизы. 2018. Том 13. № 1. С. 121-124. DOI: 10.30764/1819-2785-2018-13-1-121-124.

Current Trends in Forensic Information Technology

Nikolai A. Khatuntsev
The Russian Federal Centre of Forensic Science of the Ministry of Justice of the Russian Federation, Moscow 109028, Russian Federation

Abstract. The paper presents current trends in computer forensic science, drawing on the outcomes of the 20th annual meeting of the Forensic Information Technology Working Group (FIT-WG) of the European Network of Forensic Science Institutes (ENFSI) held in November 2017 in Spain.

Keywords: *computer forensic science, information technology, meeting, ENFSI*

For citation: Khatuntsev N.A. Current Trends in Forensic Information Technology. *Theory and Practice of Forensic Science.* 2018. Vol. 13. No 1. P. 121-124. DOI: 10.30764/1819-2785-2018-13-1-121-124.

С 6 по 10 ноября 2017 года в Барселоне (Испания) прошла двадцатая ежегодная конференция рабочей группы ENFSI по информационным технологиям «Информационные технологии в судебной экспертизе, 2017», организованная центральным подразделением компьютерных судебно-экспертных исследований полиции Каталонии (Mossos d'Esquadra) В ее работе приняли участие более 60 представителей 19 стран Европы, Канады, Японии, эксперты международных организаций, таких как Интерпол, Европол, Агентство Европейского союза по обучению правоохранительных органов (CEPOL), Центр прикладных наук и технологий (CAST, UK), а также сотрудники научных подразделений фирм Cellebrite Services, Magnet Forensics и Rusolut – производителей экспертных аналитических программных средств и программно-аппаратных комплексов для исследования объектов информационных технологий.

Встреча была посвящена актуальным проблемам компьютерно-технической экспертизы:

– извлечению данных с твердотельных устройств хранения информации – флеш-чипов типа NAND;

– восстановлению информации с физически поврежденных мобильных устройств и аналитическому исследованию данных с мобильных устройств;

– использованию Apple устройств и особенностям их файловой системы;

– исследованию новых объектов компьютерно-технической экспертизы: бес-

пилотных летательных аппаратов (дронов) и управляющих систем типа «умный дом».

В первый день работы конференции выступил представитель Института судебных экспертиз Нидерландов доктор Ян Петер Зандвжик (Jan Peter van Zandwijk) с докладом о судебном анализе NAND-флеш-чипов памяти.

Методы исследования NAND-флеш-памяти с использованием технологии chip-off применяются, когда невозможно получить доступ к данным, хранящимся в памяти устройства, другими методами. В этом случае микросхема памяти отделяется от устройства и читается напрямую. В выступлении были рассмотрены проблемы надежности при исследовании чипов, а также процедурные и технические решения возможных проблем. Докладчик озвучил идею использования ошибок, возникающих как побочный продукт после автономной обработки дампов памяти NAND-флеш, в качестве дополнительного источника судебной информации. Обнаружено, что данные о битовой ошибке содержат некоторые сведения о времени, когда конкретная часть данных присутствовала в NAND-флеш-памяти, и поэтому эта информация может потенциально использоваться для судебно-экспертных целей в качестве независимого временного канала.

Другой доклад, вызвавший интерес, был представлен Ашером Рубелом (Asher Rubel) и затрагивал исследование дронов. Внимание к беспилотным аппаратам объясняется тем, что они находят применение во многих областях жизни: от развлечений до домашних покупок. Наряду с преимуществами использования дронов, вызывает беспокойство их преступное использование – от контрабанды в тюрьмы до сброса взрывчатых веществ. При противоправном использовании этих устройств перед экспертами стоит в первую очередь задача определения данных и намерений оператора исследуемого дрона, а также решается ряд других вопросов. Докладчик раскрыл некоторые основы систем беспилотных летательных аппаратов и насколько существующие программные инструмен-

ты готовы к исследованиям подобных устройств.

При этом отметим, что в ФБУ РФЦСЭ при Минюсте России пока еще не сталкивались с исследованием дронов, но такого рода задачи могут возникнуть в любой момент. Наряду с исследованием беспилотников, необходимо уделять внимание исследованию и других современных технических средств. Так, исследование GPS-навигаторов или GPS-трекеров, в которых сохраняются данные о перемещениях людей и механизмов, могут иметь важное криминалистическое значение в доказывании и определении местоположения пользователя в конкретный момент времени. Подобные исследования уже проводились, и в дальнейшем предполагается увеличение количества экспертиз, в которых объектами исследования будут не стандартные компьютерные средства, а иные объекты – носители цифровой информации.

Можно предположить дальнейшее развитие компьютерно-технической экспертизы и все большее ее смещение в экспертизу цифровой информации. Последняя будет проводиться с целью фиксации информации, представленной в цифровом виде на носителях данных, установленных в объекте. При этом объектом может стать не только системный блок персонального компьютера, но и иные содержащие данные механизмы – дроны, GPS-навигаторы, устройства «умного дома».

В продолжение темы, затрагивающей исследования устройств, содержащих цифровую информацию, выступил Джонни Бенгтссон (Johnny Bengtsson) из Шведского национального центра судебной экспертизы с докладом об исследовании «умного дома». Системы домашней автоматизации – «интеллектуальные домашние системы» или «интернет дома» – прежде устанавливали энтузиасты, которые с особым интересом наблюдали за домашним мониторингом и автоматизацией. Использование подобных систем позволяет управлять освещением, устанавливать различные приводы для перекрытия кранов, контролировать доступ в помещение, следить за потреблением электричества и воды, а также осуществлять климат-контроль.

Интеграция дополнительных аудиовизуальных компонентов может превратить хорошо сконфигурированную домашнюю систему автоматизации в высококомпетентную надежнейшую систему обнаружения вторжений. Типичная система домашней автоматизации основана по крайней мере на одном центральном аппаратном контроллере или концентраторе с программным обеспечением для локальной или удаленной конфигурации системы администрирования, автоматизации, мониторинга и управления проводными или беспроводными периферийными датчиками и приводами. Автоматизация осуществляется путем создания сцен – это программный способ выражения правил условного поведения, основанных на данных датчиков, состоянии исполнительного механизма или произошедших событиях.

Общие принципы судебной компьютерно-технической экспертизы также применимы к системам домашней автоматизации, где полученные данные могут состоять из выделенных, нераспределенных или перезаписанных данных контроллера, а для некоторых систем – дополнительных данных, хранящихся, например, в облачном хранилище. Тем не менее, есть основания считать, что судебная экспертиза средств домашней автоматизации является самостоятельной цифровой судебной дисциплиной. Ее задачи – разработка общей методологии и соответствующих инструментов анализа и интерпретации системных данных домашней автоматизации независимо от марки производителей таких систем. При этом необходимо, чтобы следователи, осматривающие место преступления, эффективно находили датчики и приводы, а также проверяли их функциональные свойства. Эксперты же должны проводить исследование данных, хранящихся в системах, исследовать точность и качество показаний, временных интервалов включения или выключения, идентификаторов устройств и так далее. Наибольшее правдоподобие при эмуляции работы датчиков может иметь решающее значение для определения механизма работы систем домашней автоматизации и тем самым помочь в расследования преступления.

В рамках конференции обсуждалась также новая версия общих методических рекомендаций по производству компьютерно-технической экспертизы – Best practice manual for the forensic examination of digital technology. Были рассмотрены вопросы теоретического, методического, инструментального и технического обе-

спечения компьютерно-технической экспертизы, подготовки и повышения квалификации экспертов, проблемы внедрения современных информационных технологий в экспертную практику, вопросы сертификации экспертов и аккредитации судебно-экспертных учреждений на соответствие требованиям ISO 17025/МЭК 17025.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Хатунцев Николай Александрович – заместитель директора ФБУ РФЦСЭ при Минюсте России по информатизации; e-mail: n.khatuntsev@ sudexpert.ru.

ABOUT THE AUTHOR

Khatuntsev Nikolai Aleksandrovich – Deputy Director for IT Development of the Russian Federal Centre of Forensic Sciecne of the Russian Ministry of Justice; e-mail: n.khatuntsev@ sudexpert.ru.