https://doi.org/10.30764/1819-2785-2020-3-89-97

Современные возможности судебной компьютерно-технической экспертизы при расследовании различных видов преступлений

Д.В. Завьялова
ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», Москва 125993, Россия

Аннотация. В статье проанализированы современное состояние судебной компьютерно-технической экспертизы, ее место и потенциал в расследовании различных преступлений с «компьютерным» элементом. Кратко представлены исторический обзор становления судебной компьютерно-технической экспертизы как самостоятельного рода судебных экспертиз и ее теоретические основы.
Проведено обобщение практики лаборатории судебной компьютерно-технической экспертизы ФБУ РФЦСЭ при Минюсте России за 2017–2019 годы. Рассмотрены вопросы, которые чаще всего ставятся перед экспертами при назначении судебных компьютерно-технических экспертиз, процентное соотношение категорий дел, по которым назначаются такие экспертизы, наиболее распространенные объекты, экспертные выводы, их форма и полнота. По итогам обобщения выделены основные запросы следственных органов и судов к экспертным компьютерно-техническим исследованиям, а также типичные ошибки при назначении таких экспертиз.
Автор прогнозирует возможное развитие судебной компьютерно-технической экспертизы и предлагает стратегии и меры по минимизации ошибок и нерационального расходования средств при ее назначении и производстве.

Ключевые слова: *судебная компьютерно-техническая экспертиза, киберпреступления, компьютерные преступления, преступления в сфере компьютерной информации, преступления в сфере информационных технологий, вредоносное программное обеспечение, ошибки при назначении экспертизы*

Для цитирования: Завьялова Д.А. Современные возможности судебной компьютерно-технической экспертизы при расследовании различных видов преступлений // Теория и практика судебной экспертизы. 2020. Т. 15. № 3. С. 89–97. https://doi.org/10.30764/1819-2785-2020-3-89-97

Current Capacities of Digital Forensics for Investigations of Different Types of Crimes

Dar'ya V. Zav'yalova
Kutafin Moscow State Law University, Moscow 125993, Russia

Abstract. The article focuses on the present state of digital forensics and its potential when investigating different types of crimes with a "digital" element. It also presents a brief historical overview of the development of digital forensics as an independent type of forensic examination, its theoretical framework.
The paper presents a summary of the practice of the Laboratory of Digital Forensics of the Russian Federal Centre of Forensic Science of the Russian Ministry of Justice over 2017–2019. In the course of the summary, the author analyses typical questions to experts, the percentage of cases' categories, the most common objects of the expertise, and experts' opinions, their form, and completeness. Following the summary's results, the most frequent investigators' requests for this kind of examination have been highlighted. Also, typical errors at appointing the expertise have been revealed.
The author presents a prognosis for the further development of digital forensics and proposes strategies and measures to minimize the errors at the appointment of the examinations and unsustainable expenditure of resources in appointment and conduct of this type of research.

Keywords: *digital forensics, cybercrimes, computer crimes, IT crimes, malware, errors at appointing an expertise*

For citation: Zav'yalova D.V. Current Capacities of Digital Forensics for Investigations of Different Types of Crimes. *Theory and Practice of Forensic Science*. 2020. Vol. 15. No. 3. P. 89–97. (In Russ.).
https://doi.org/10.30764/1819-2785-2020-3-89-97

Введение

За последние 25 лет информационные технологии внесли значительные изменения во все сферы жизни общества. Однако 2020 год стал, безусловно, поворотным моментом не только в повсеместном распространении информационных технологий, но и в их непосредственном внедрении в бизнес, юридические и социальные процессы.

Не будет преувеличением сказать, что пандемия Covid-19 послужила импульсом, запустившим давно назревавшие технологические и социальные изменения. Если раньше у законодателей, работодателей и рядовых граждан еще оставались вопросы относительно того, какую роль непосредственно в их жизни играют информационные технологии (ИТ), то сейчас их нет. Для всех уже очевидно, что Интернет, ИТ, дистанционные форматы деятельности и прочие последствия «прорастания» Сети и ИТ в нашу жизнь – реальность.

Пандемия коронавируса показала, как быстро могут сложиться новые методы онлайн-деятельности, когда меняется социальный контекст и разрушается привычная рутина [1]. Новая реальность проявляет себя на всех уровнях: от введения электронного документооборота в области трудового права, гражданского оборота, налоговых отношений, следствия и судопроизводства[1] до цифровизации системы госзакупок [2].

В 1987 году Р.С. Белкин определил предмет криминалистики как «специфическую группу объективных закономерностей действительности, методы и средства их познания и использования результатов этого познания в уголовном судопроизводстве» [3]. В связи с радикальными изменениями нашей действительности перед криминалистикой ставится задача выявления и познания ее новых объективных закономерностей, без чего невозможна борьба с новыми видами преступности. Судебно-экспертные исследования, их теоретическое и методологическое обеспечение – неотъемлемая часть этого процесса.

С одной стороны, новые площадки и форматы дистанционного обучения, работы и управления вовлекают огромное количество людей, которые ранее избегали, скажем так, жизнеобеспечивающего ежедневного контакта с информационными технологиями, сводя такое взаимодействие к минимуму, воспринимая ИТ как развлечение или вспомогательный рабочий инструмент. Именно эти люди максимально уязвимы перед киберпреступностью, так как большинство из них обладает низкой технической грамотностью даже на бытовом уровне, и вынужденная вовлеченность в «сетевые» процессы и отношения ставит под удар в первую очередь их финансы и персональные данные. С другой стороны, уровень безопасности самих платформ и сетей может быть довольно низок, что неизбежно привлекает киберпреступников.

По данным за 2018 год, стоимость ущерба от киберпреступлений в развитых странах выросла в среднем на 22,7 % [4]. Согласно данным Главного управления правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации, число киберпреступлений в России в 2019–2020 гг. также выросло[2]. Можно предположить, что одним из последствий углубления и ускорения цифровизации станет рост компьютерной преступности и, как следствие, проведения исследований в рамках судебной компьютерно-технической экспертизы (СКТЭ).

Цель работы

Цель данного исследования – рассмотреть становление, современное состояние, проблемы и перспективы развития СКТЭ, а также дать практические рекомендации для следователей по наиболее эффективному использованию возможностей, предоставляемых СКТЭ, в ходе расследования дел различных категорий.

Кроме того, одной из задач данной работы было обобщение экспертной практики лаборатории судебной компьютерно-технической экспертизы ФБУ РФЦСЭ при Минюсте России (далее – РФЦСЭ) с целью рассмотрения практического применения теоретических положений СКТЭ.

Краткая история возникновения СКТЭ

Судебная компьютерно-техническая экспертиза – самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимых в том числе в целях всестороннего исследования информации, получаемой с электрон-

[1] Обзор: «В ТК РФ хотят закрепить правила электронного обмена кадровыми документами». http://www.consultant.ru/document/cons_doc_LAW_327513/; Обзор: «Правила дистанционной работы могут обновить». http://www.consultant.ru/document/cons_doc_LAW_355063/63125e835439d4ab1fa3e2dc27e7f4048813a02b/ (дата обращения: 22.07.2020).

[2] Генеральная прокуратура Российской Федерации. https://genproc.gov.ru/stat/data/ (дата обращения: 22.07.2020).

ных носителей [5, с. 5]. Потребность в этом роде судебных экспертиз возникла около 20 лет назад в связи с развитием информационных технологий в обществе.

На заре ЭВМ, в конце 50-х – начале 60-х годов, вычислительные машины были очень массивны, дороги и доступны только крупным государственным предприятиям. Однако уже к 70-м ситуация кардинально изменилась. Появление персональных компьютеров, начало использования ЭВМ в бизнесе, а затем и их выпуск на потребительский рынок стали не только прорывом в контексте новых, непревзойденных возможностей для работы, творчества, управления и прочих видов созидательной деятельности, но и основой зарождения киберпреступности.

В 1976 году в Страсбурге состоялась конференция Совета Европы по криминологическим аспектам экономических преступлений, где было выделено несколько категорий компьютерных преступлений, включая мошенничество [6, с. 494].

В 1977 году в США впервые обсуждался законодательный акт, регулирующий компьютерные системы[3], и в нем мошеннические и другие противозаконные действия, совершенные с помощью компьютера, рассматривались как федеральное преступление [6, с. 496]. В тот момент законопроект не был принят, но эта инициатива показала, что проблема киберпреступности вызывала беспокойство на законодательном уровне в некоторых государствах уже тогда. Вполне ожидаемо, что в следующем, 1978, году в штате Флорида был принят первый закон, регулирующий непосредственно компьютерные преступления (Florida Computer Crimes Act of 1978)[4].

К 1980-м годам по всему миру совершалось все больше и больше компьютерных преступлений. В 1979 г. Интерпол признал эту проблему глобальной [6, с. 495]. При раскрытии такого рода преступлений стали широко использовать цифровые доказательства, в основном компьютеры и дискеты. И здесь впервые правоохранители столкнулись с существенной особенностью новых объектов. Помимо вещественных доказательств в виде материальных предметов (компьютеров, дискет и др.), объектами исследования стали и нематериальные объекты, такие как программные продукты и собственно информация в различных проявлениях, а не только ее носители [7].

Необходимость расшифровать материальный носитель, дать возможность представить в деле содержащуюся на нем информацию как допустимое доказательство способствовала развитию судебной компьютерно-технической экспертизы. Важно, что становление нового вида экспертиз носило спонтанный характер.

Нередко новая специальность появляется как результат дифференциации или интеграции знания. Но в данном случае стихийное развитие информационных технологий привело к тому, что практика определила теорию, и ее требования заставили действовать *ad hoc*, без проведения серьезных научных изысканий, что стало общемировой тенденцией [6, с. 497; 7]. Несмотря на это, качество судебных экспертиз даже на ранних этапах в российских экспертных подразделениях оказалось довольно высоким.

Изначально для проведения подобного рода исследований приглашались специалисты по экспертизе электронных приборов. Однако ресурсы (материальные, кадровые, методические) были ограничены и не удовлетворяли потребности практики. В скором времени на базе различных ведомств стали создаваться специализированные экспертные подразделения.

Впервые о необходимости создания и государственной поддержки экспертных учреждений для производства компьютерных экспертиз в России было заявлено в рамках Плана мероприятий по реализации Коммюнике и Плана действий министров юстиции и внутренних дел стран «восьмерки» от 10 декабря 1997 г.[5] После этого остро встал вопрос о разработке научной и законодательной базы нового рода экспертиз. В связи с этим 22 октября 1999 г. Правительство РФ издало распоряжение об усилении борьбы с преступлениями в сфере высоких технологий и реализации международных договоренностей и обязательств Российской Федерации[6], которое содержа-

[3] Bill S.1766 – Federal Computer Systems Protection Act. https://www.congress.gov/bill/95th-congress/senate-bill/1766 (дата обращения: 22.07.2020).

[4] https://fall.law.fsu.edu/collection/FlSumGenLeg/FlSumGenLeg1978.pdf (дата обращения: 22.07.2020).

[5] Усов А.И. Концептуальные основы судебной компьютерно-технической экспертизы: автореф. дис. … док. юрид. наук. Москва, 2002. 41 с.

[6] Распоряжение Правительства Российской Федерации от 22.10.1999 № 1701-р «О мерах по усилению борьбы с преступлениями в сфере высоких технологий». http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=211873#01513461363903884 (дата обращения: 22.07.2020).

ло прямое предписание МВД России, ФСБ, Министерству юстиции изучить вопрос о состоянии судебных экспертиз и исследований в сфере информационных технологий и выработать соответствующие предложения[5]. В результате на базе ЭКЦ МВД России был создан отдел компьютерных экспертиз и технологий и научно-исследовательская лаборатория, где разрабатывали перспективные направления развития этого рода экспертиз и их методические основы [8].

В апреле 2003 года в РФЦСЭ была учреждена специализированная лаборатория судебной компьютерно-технической экспертизы и информационных технологий. В том же году в перечне родов (видов) экспертиз, выполняемых в государственных судебно-экспертных учреждениях Минюста России, появилась данная экспертиза и соответствующая экспертная специальность 21.1 – «Исследование информационных компьютерных средств»[7].

Таким образом, к началу XXI века в главных экспертных центрах страны стала формироваться практическая и научная база для дальнейшей разработки компьютерно-технической экспертизы, но даже относительно ее названия согласие не было достигнуто сразу. Так, можно было встретить следующие названия: судебная компьютерно-техническая экспертиза, компьютерная экспертиза, информационно-аналитическая техническая экспертиза, экспертиза электронно-вычислительной техники и ее комплектующих [8]. Такой разброс в названиях создал не только технические трудности и путаницу, но и обусловил разные подходы к формулированию задач экспертизы, ее предмета, объектов. Это в свою очередь привело к проблеме признания допустимости выводов некоторых экспертиз в качестве доказательств в суде.

Отметим, что терминологическая несогласованность в области СКТЭ, децентрализация ведомств и стандартов, связанных с этой экспертизой, потребность в их гармонизации и унификации характерны не только для нашей страны, но являются общемировыми проблемами [9].

В 1996 году в своей монографии Е.Р. Россинская отметила формирование нового рода судебных экспертиз – компьютерно-технических [10]. Это название вошло в перечень Министерства юстиции и сегодня общепринято, хотя в системе МВД сохраняется название «компьютерная экспертиза».

Основные теоретические положения СКТЭ

Родовой предмет СКТЭ – факты и обстоятельства, устанавливаемые на основе исследования закономерностей разработки и эксплуатации компьютерных средств, обеспечивающих реализацию информационных процессов, которые зафиксированы в материалах уголовного или гражданского дела, дела об административном правонарушении. *Видовая классификация СКТЭ* основана на компонентах, обеспечивающих функционирование любого компьютерного средства (аппаратном (техническом), программном, информационном) [10].

В СКТЭ выделяют *аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную, компьютерно-сетевую* экспертизы. Кроме того, выделяют судебную *телематическую экспертизу*, предметом которой являются фактические данные, устанавливаемые на основе применения специальных знаний при исследовании средств телекоммуникаций и подвижной связи как материальных носителей информации о факте или событии, имеющем отношение к расследуемому делу [11, с. 389].

Каждый из представленных видов экспертизы позволяет решить комплекс идентификационных и диагностических задач. Однако современная практика показывает, что при производстве большинства экспертиз все обозначенные выше виды СКТЭ применяются комплексно и чаще всего последовательно [12, с. 484]. Это видно и по структуре экспертных заключений по конкретным делам, которые включают и внешний осмотр аппаратной части компьютерного оборудования, и программное и информационное исследование, и исследование следов работы и «пребывания» в сети конкретного устройства. Поэтому в настоящее время в постановлениях о производстве судебной экспертизы указывают, как правило, не видовое наименование, а родовое: следственные органы и суды назначают судебную компьютерно-техническую экспертизу.

Обобщение экспертной практики

Поскольку на современном этапе развития общества компьютерный элемент может быть практически у любого преступления, осведомленность о возможностях СКТЭ, а также активное сотрудничество с

[7] Приказ Минюста России от 14.05.2003 № 114 «Об утверждении Перечня родов (видов) экспертиз, выполняемых в государственных судебно-экспертных учреждениях Министерства юстиции Российской Федерации…».

экспертом обязательны для следователя и обуславливают успешность его работы.

Из отзывов правоохранительных органов следует, что выводы судебных экспертов-компьютерщиков имеют высокую значимость для дела как оперативно-розыскную, так и доказательственную. Они позволяют:

– расшифровать закодированную информацию;

– обнаружить информацию, считавшуюся отсутствующей, утерянной или уничтоженной;

– восстановить механизм преступного события по информационным следам [13, с. 220];

– установить *modus operandi* преступника [1];

– установить общий источник происхождения данных и документов (в составе комплексного исследования) и ответить на многие другие вопросы, что способствует быстрому и эффективному построению и проверке следственных версий.

Стоит отметить важную особенность СКТЭ – возможность рассмотреть колоссальное количество доказательственной информации. Так, в ходе расследования дела об изнасиловании и убийстве 18-летней Кимберли Проктор (Kimberly Proctor) в городке Лэнгфорд в Британской Колумбии (Канада) полиция собрала и исследовала в рамках компьютерно-технической экспертизы эквивалент 1,4 миллиарда бумажных страниц доказательств, включая переписку преступников в «Фейсбуке», программах мгновенного обмена сообщениями, СМС, чатах онлайн-игр [6, с. 492]. Раскрытие этого дела было бы невозможным без современных возможностей СКТЭ.

Нами было проведено обобщение практики производства компьютерно-технических экспертиз по уголовным делам в РФЦСЭ, при этом рассмотрено более 300 экспертных наблюдательных производств за 2017–2019 годы на предмет:

– квалификации уголовного дела, по которому была назначена экспертиза;

– объектов экспертизы;

– вопросов, поставленных перед экспертом;

– методов и средств исследования;

– формы выводов эксперта, их соответствия поставленным вопросам и полноты.

По итогам обобщения можно сделать следующие выводы.

СКТЭ назначается практически по всем категориям уголовных дел (рис.), но больше всего – по делам о преступлениях в сфере экономики. На втором месте – преступления против личности, затем – против государственной власти. Наименьшее количество экспертиз было назначено по делам о преступлениях против общественной безопасности и общественного порядка, делам о преступлениях в сфере компьютерной информации и делам против конституционных прав и свобод граждан (как правило, это нарушение авторских прав).

Может показаться парадоксальным, что по делам о преступлениях в сфере компьютерной информации за последние 3 года было проведено так мало экспертиз, однако ничего удивительного в этом нет. Дело в том, что тенденция снижения общего количества расследований дел о таких преступлениях в процентном соотношении на-

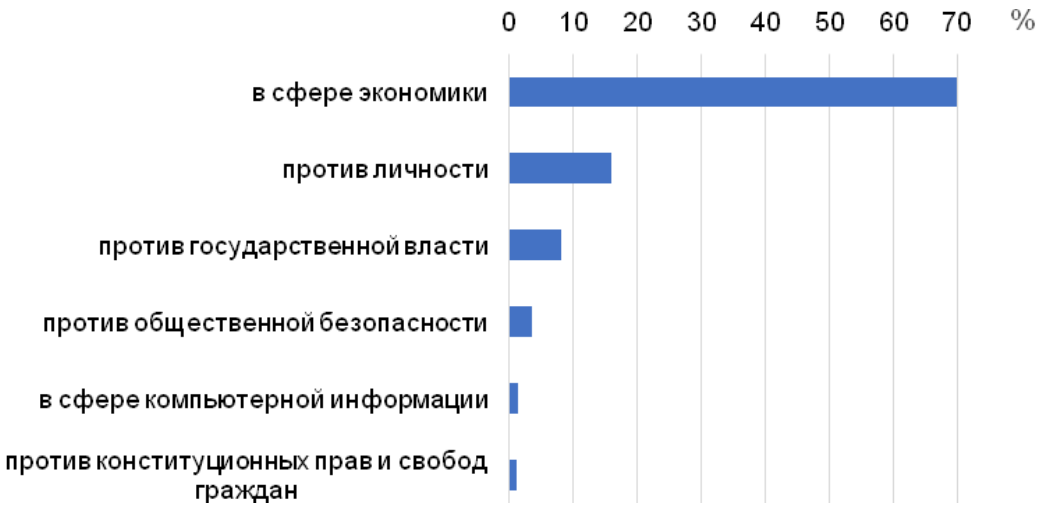

Рис. Процентное соотношение видов преступлений, по которым назначалась СКТЭ в 2017–2019 гг. в РФЦСЭ

Fig. *The percentage of crime types for which a digital forensic research was appointed to the Russian Federal Centre of Forensic Science over 2017–2019*

метилась уже давно. Так, по данным, приведенным в обзорной монографии по анализу киберпреступности, видно, что в 2010 году было зарегистрировано 8 669 преступлений в сфере компьютерной информации, из них раскрыто 4 832, а в 2014 году эти показатели составили 3 056 и 753 соответственно [14, с. 72–74]. Высокая латентность данной категории преступлений сохраняется до сих пор. По данным Генеральной прокуратуры РФ за 2018 год, только четверть от общего числа зарегистрированных компьютерных преступлений была раскрыта[8]. Таким образом, крайне низкое число экспертиз в области компьютерной информации за последние три года можно объяснить тем, что сравнительно небольшое количество дел о таких преступлениях становилось объектом грамотного и досконального расследования.

В то же время в 2019 году Генеральная прокуратура отметила тенденцию роста количества выявленных преступлений (+ 68,5 %), совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, по сравнению с предыдущим годом. Показатели предварительного следствия по закрытым делам этой категории на конец 2019 года также выросли (+ 50,4 %)[9]. В 2020 году эта тенденция сохраняется. Только за период январь – май 2020 года количество рассматриваемых преступлений возросло более чем на 85 %. Если годом ранее такими деяниями было каждое десятое регистрируемое преступление, то сегодня это уже каждое пятое. Больше половины из них (56,6 %) совершается с использованием сети Интернет (прирост по сравнению с предыдущим годом + 74,1 %, что составило 102,2 тыс. преступлений), свыше 40 % – при помощи средств мобильной связи (+ 99,7 %, 76,6 тыс.). Три четверти таких преступлений совершается путем кражи или мошенничества (+ 96,2 %, 143 тыс.), почти каждое десятое связано с незаконным производством, сбытом или пересылкой наркотиков (+ 73,9 %, 17,1 тыс.)[10]. Такие показатели еще раз указывают на то, что востребованность исследований в рамках СКТЭ в ближайшее время будет только расти, и, вероятно, довольно резко.

Среди объектов судебной компьютерно-технической экспертизы первое место занимают мобильные телефоны, затем – ноутбуки и их жесткие диски, флеш-карты и планшеты. Реже – отдельные жесткие диски, серверы, системные блоки, АРМ[11], видеорегистраторы и другие устройства и носители информации.

С развитием информационных технологий для следователей начинают представлять интерес новые объекты, и велика вероятность, что вскоре по этим объектам потребуются отдельные методические разработки в рамках СКТЭ. В настоящий момент наибольший интерес представляют объекты IoT – Интернета вещей (разного рода «умная» техника промышленного и бытового применения) [15, с. 179], облачные сервисы хранения информации, 3D-принтеры и некоторые другие технологии производства и обработки информации (искусственный интеллект, машинное обучение, Big Data).

Развитие нанотехнологий и технологий географических информационных систем, сращивание нейротехнологий с микроэлектроникой, активное внедрение принципиально новых технологий свидетельствуют о важности совершенствования уже существующих и формирования новых направлений судебной компьютерно-технической экспертизы [8, с. 48].

СКТЭ назначаются в основном с целью поиска и исследования на объектах пользовательской информации, относящейся к делу. При этом в одном постановлении перед экспертом, как правило, ставится сразу ряд вопросов. К наиболее распространенным из них относятся следующие.

– Имеются ли на объекте пользовательские файлы (графические, текстовые, видео, аудио), в том числе среди удаленных? Возможно ли их восстановление? Были ли они как-то изменены?[12]

[8] ТАСС: Генпрокуратура сообщила почти о двукратном росте числа киберпреступлений в РФ в 2018 году. 29.10.2018. https://tass.ru/proisshestviya/5733551 (дата обращения: 22.07.2020).

[9] Генеральная прокуратура РФ. Главное управление правовой статистики и информационных технологий. Состояние преступности в России за январь – декабрь 2019 года. Москва. 2019. С. 8. https://genproc.gov.ru/upload/iblock/034/sbornik_12_2019.pdf (дата обращения: 22.07.2020).

[10] Генеральная прокуратура РФ. Главное управление правовой статистики и информационных технологий. Состояние преступности в России за январь – май 2020 года. Сборник на основании формы федерального статистического наблюдения № 4-ЕГС. Москва. 2020. С. 6. http://crimestat.ru/analytics (дата обращения: 22.07.2020).

[11] Автоматизированные рабочие места.

[12] Эти вопросы ставились перед судебными экспертами примерно в 60 % проанализированных исследований.

– Имеются ли на объекте файлы, содержащие ключевые слова «…»? Или файлы, содержащие значимую для дела информацию определенного характера (например, изображения обнаженных людей в делах о распространении порнографии или бухгалтерскую документацию в делах о мошенничестве)?[13]

– Всевозможные варианты запросов по выходу устройства в Интернет или работе в Сети: совершался ли выход в Интернет? На какие сайты совершался выход с устройства? В какое время совершался выход? Откуда совершался выход (включая запросы об IP-адресах)? Имеется ли история браузера? Производилось ли скачивание или передача файлов?[13]

Среди других вопросов, которые ставятся перед экспертами лаборатории СКТЭ в РФЦСЭ, можно выделить:

– Работоспособен ли объект, представленный на экспертизу?

– Имеется ли на объекте определенное программное обеспечение (ПО) (например, программы удаленного доступа, ПО для ведения бухгалтерского учета, вредоносное ПО и др.)?

– Возможно ли использовать объект с определенной целью? (для выхода в Интернет, пользования определенными информационными системами или базами данных, например 1С)?

– Какие пользовательские данные содержатся на объекте (учетные записи, логины, пароли и пр.)?

Всего около 2 % экспертиз назначались для выяснения соответствия ПО техническому заданию, закону.

По результатам обобщения экспертной практики можно отметить эффективность и высокий уровень проведенных компьютерно-технических экспертиз. Большинство выводов в заключениях экспертов даны в категорической форме. Вывод в форме НПВ (не представляется возможным ответить на поставленный вопрос) встречается только в 15 % случаев и, как правило, не связан с возможностями экспертизы. Невозможность ответить на поставленные перед экспертом вопросы была обусловлена одной из следующих причин:

а) непригодностью / неработоспособностью / критичным дефектом объекта;

б) отсутствием пароля от объекта, без которого невозможно его информационное исследование или такое исследование становится нецелесообразным в силу того, что необходимо затратить необоснованное количество ресурсов на подбор пароля;

в) поставленные вопросы не входили в компетенцию эксперта.

Проведенное обобщение экспертной практики производства СКТЭ позволило выявить типичные ошибки, допускаемые при ее назначении, а также предложить рекомендации по их минимизации.

Компьютерно-техническая экспертиза – очень трудоемкий процесс. Ее производство занимает много времени, человеческих и технических ресурсов. Среднее время ожидания исполнения экспертизы для следователя или суда составляет около полугода. Поэтому при назначении такой экспертизы следователь должен быть максимально «экономным». Это относится к количеству и качеству объектов, их подготовленности к проведению экспертизы, к формулированию или выбору вопросов. Например, при назначении экспертизы следователям необходимо иметь первичное представление об устройстве и назначении различных объектов (телефона, ноутбука, роутера и пр.), что такое IP, MAC-номер, у каких объектов они есть и зачем и т. д. То есть следователь или лицо, назначающее экспертизу, должны обладать базовым уровнем технической грамотности, чтобы исключить некорректные и лишние вопросы при назначении экспертиз, предоставление непригодных объектов.

В случае разной природы объектов (например, телефон и компьютер) или их большого количества есть смысл назначать по каждому объекту (или по их небольшой однородной группе) отдельную экспертизу. Это значительно сокращает время исполнения, поскольку тогда можно задействовать разных экспертов, в том числе с разной специализацией. И такая тенденция наметилась с начала 2018 года: большое количество объектов в одних и тех же уголовных делах направляются на разные экспертизы (до 10 и более экспертиз различных объектов по одним и тем же уголовным делам).

Что касается наиболее популярных объектов (например, ноутбуков, телефонов, планшетов), то здесь необходимо разработать простые стандартные алгоритмы работы с ними, которые должны быть доведены до сведения следователей. Это поможет скорректировать обращение с потенциальными объектами СКТЭ, например можно ли

[13] Подобные вопросы содержались примерно в 40 % исследований.

их включать, что делать, если здание было обесточено, как лучше организовать проведение следственного действия с учетом особенностей конкретной инфраструктуры и др.

Некоторые ошибки при подготовке объектов и назначении экспертизы могут не только повлиять на ее результаты, но и сделать исследование вовсе невозможным или значительно увеличить его сроки. Так, достаточно редко в постановлении о назначении экспертизы в отношении мобильного телефона (смартфона) указывается разрешение на внесение изменений в данные объекта. Без него эксперт даже не может включить телефон, поскольку это ведет к изменению его данных. Самостоятельное же внесение изменений в свойства объекта запрещено эксперту положениями ст. 25 Федерального закона от 31 мая 2001 г. № 73-ФЗ «О государственной судебно-экспертной деятельности в Российской Федерации»[14]. В итоге эксперт вынужден ходатайствовать перед следователем о даче соответствующего разрешения, что ведет к затягиванию сроков экспертного исследования в условиях дефицита времени предварительного следствия.

Общее же правило работы с объектами – не включать, не производить никаких манипуляций непосредственно с объектом, не исследовать его самому.

Наконец, определение задания и формулировка вопросов – чрезвычайно важный этап назначения экспертизы. Вопрос – основной ориентир для эксперта, от которого зависит, например, выбор методики исследования. Поэтому не следует включать дополнительные вопросы «на всякий случай» или перечислять все вопросы по списку из справочника, так как это увеличивает время производства экспертизы и ведет к нерациональному расходованию ресурсов.

Залог успешного проведения экспертизы в разумные сроки – взаимодействие следователя и эксперта на каждом этапе работы: от формулирования вопросов для назначения экспертизы до разъяснения выводов эксперта. Именно поэтому так важен контакт и сотрудничество между представителями различных ведомств на всех уровнях.

Заключение

Подводя итоги, необходимо еще раз отметить, что компьютерно-техническая экспертиза обладает огромным потенциалом в разрешении самых разных уголовных дел и ее значение в ближайшем будущем будет только расти.

Исследование практики лаборатории СКТЭ РФЦСЭ показало, что в настоящее время там проводится колоссальная и эффективная работа. Однако в связи с изменяющимися социальными и техническими условиями в скором времени можно ожидать роста нагрузки на экспертов-специалистов по СКТЭ, а также недостаточности методической поддержки в силу появления значительного массива новых объектов. Эти вопросы и каждый из объектов нуждаются в отдельных подробных и предметных исследованиях.

[14] http://www.consultant.ru/document/cons_doc_LAW_31871/ (дата обращения: 27.06.2020).

СПИСОК ЛИТЕРАТУРЫ

1. Ribaux O., Souvignet T.R. “Hello Are You Available?” Dealing with Online Frauds and the Role of Forensic Science // Forensic Science International: Digital Investigation. 2020. Vol. 33. P. 1–11. https://doi.org/10.1016/j.fsidi.2020.300978
2. Камнева К. Пандемия подстегнула цифровизацию российской системы госзакупок // Российская газета. 21.07.2020. https://rg.ru/2020/07/21/pandemiia-podstegnula-cifrovizaciiu-rossijskoj-sistemy-goszakupok.html
3. Белкин Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частная теории. М.: Юрид. лит., 1987. 272 с.
4. Broadhead S. The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments // Computer Law & Security Review. 2018. Vol. 34. P. 1180–1196.

REFERENCES

1. Ribaux O., Souvignet T.R. “Hello Are You Available?” Dealing with Online Frauds and the Role of Forensic Science. *Forensic Science International: Digital Investigation*. 2020. Vol. 33. P. 1–11 https://doi.org/10.1016/j.fsidi.2020.300978
2. Kamneva K. The Pandemic Has Spurred the Digitization of Russia’s Public Procurement System. *Russian Newspaper*. 21.07.2020. (In Russ.). https://rg.ru/2020/07/21/pandemiia-podstegnula-cifrovizaciiu-rossijskoj-sistemy-goszakupok.html
3. Belkin R.S. *Criminalistics: Problems, Trends, Perspectives. General and Special Theories.* Moscow: Yuridicheskaya literatura, 1987. 272 p. (In Russ.)
4. Broadhead S. The Contemporary Cybercrime Ecosystem: A Multi-Disciplinary Overview of the State of Affairs and Developments. *Computer Law & Security Review*. 2018. Vol. 34. P. 1180–1196.

5. Зубаха В.С., Усов А.И., Саенко Г.В., Волков Г.А., Белый С.А., Семикаленова А.И. Общие положения по назначению и производству компьютерно-технической экспертизы. Метод. рекомендации. М.: ЭКЦ МВД России, 2001. 72 с.

6. Holt T.J., Bossler A.M., Seigfried-Spellar K.C. Cybercrime and Digital Forensics. 2nd ed. London: Routledge, 2017. 754 p. https://doi.org/10.4324/9781315296975
7. Усов А.И. Судебная компьютерно-техническая экспертиза: становление, развитие, методическое обеспечение // Теория и практика судебной экспертизы. 2008. № 3 (11). С. 10–22.
8. Дёмин К.Е. О проблемах судебной компьютерно-технической экспертизы и путях их решения // Вестник Московского университета МВД России. 2017. № 2. С. 46–48.
9. Horsman G. Opinion: Does the Field of Digital Forensics Have a Consistency Problem? // Forensic Science International: Digital Investigation. 2020. Vol. 33. P. 1–5. https://doi.org/10.1016/j.fsidi.2020.300970
10. Россинская Е.Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе. М.: Право и Закон, 1996. 224 с.
11. Россинская Е.Р., Галяшина Е.И. Настольная книга судьи. Судебная экспертиза. М.: Проспект, 2019. 464 с.
12. Россинская Е.Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе. М.: Норма: ИНФРА-М, 2011. 576 с.
13. Смирнова С.А. Вызовы времени и экспертные технологии правоприменения. Мультимодальное издание «Судебная экспертиза: перезагрузка». Ч. 1. М.: Эком, 2012. 656 с.
14. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ. Монография / Под ред. И.Г. Смирновой. М.: Юрлитинформ, 2016. 312 с.
15. Gilchrist A. Industry 4.0. New York: Apress, 2016. 250 p. https://doi.org/10.1007/978-1-4842-2047-4

СВЕДЕНИЯ ОБ АВТОРЕ

Завьялова Дарья Владимировна – аспирант кафедры криминалистики Московского государственного юридического университета им. О.Е. Кутафина (МГЮА); e-mail: dariazav@mail.ru

Статья поступила: 25.06.2020
После доработки: 30.07.2020
Принята к печати: 10.08.2020

5. Zubakha V.S., Usov A.I., Saenko G.V., Volkov G.A., Belyi S.A., Semikalenova A.I. *General Terms on the Appointment and Conduct of a Forensic Digital Investigation. Methodological Recommendations*. Moscow: State Forensic Centre of the Ministry of Internal Affairs of Russia, 2001. 72 p. (In Russ.)
6. Holt T.J., Bossler A.M., Seigfried-Spellar K.C. *Cybercrime and Digital Forensics.* 2nd ed. London: Routledge, 2017. 754 p. https://doi.org/10.4324/9781315296975
7. Usov A.I. Forensic Digital Investigation: Formation, Development, Methodological Support. *Theory and Practice of Forensic Science*. 2008. No. 3 (11). P. 10–22. (In Russ.)

8. Demin K.E. About the Problems of the Judicial Computer Forensic and Technical Expertise and Their Solutions. *Vestnik Moskovskogo Universiteta MVD Rossii*. 2017. No. 2. P. 46–48. (In Russ.)
9. Horsman G. Opinion: Does the Field of Digital Forensics Have a Consistency Problem? *Forensic Science International: Digital Investigation.* 2020. Vol. 33. P. 1–5. https://doi.org/10.1016/j.fsidi.2020.300970
10. Rossinskaya E.R. *Forensic Examination in Criminal, Civil and Arbitration Procedure*. Moscow: Pravo i Zakon, 1996. 224 p. (In Russ.)
11. Rossinskaya E.R., Galyashina E.I. *A Judge's Handbook. Forensic Expertise*. Moscow: Prospekt, 2019. 464 p. (In Russ.)
12. Rossinskaya E.R. *Forensic Examination in Criminal, Civil and Arbitration Procedure*. Moscow: Norma: Infra-M, 2011. 576 p. (In Russ.)
13. Smirnova S.A. *Challenges of the Time and Expert Technologies of Law Enforcement. Multimodal Issue "Forensic Expertise: Reboot". Part I*. Moscow: Ekom, 2012. 656 p. (In Russ.)

14. Smirnova I.G. (ed). *Cybercrime: Criminological, Penal, Procedural and Forensic Analysis. Monograph*. Moscow: Yurlitinform, 2016. 312 p. (In Russ.)

15. Gilchrist A. *Industry 4.0.* New York: Apress, 2016. 250 p. https://doi.org/10.1007/978-1-4842-2047-4

ABOUT THE AUTHOR

Zav'yalova Dar'ya Vladimirovna – postgraduate student of the Criminalistics Department Kutafin Moscow State Law University (MSAL); e-mail: dariazav@mail.ru

Received: June 25, 2020
Revised: July 30, 2020
Accepted: August 10, 2020