А. А. Шелупанов, А. Р. Смолина

ФОРЕНЗИКА

Теория и практика расследования киберпреступлений

Горячая линия–Телеком

УДК 343.983.25:004.056.5
ББК 67.52
DOI 10.25780/0002
Ш44

Р е ц е н з е н т : доктор физ.-мат. наук, профессор *С. С. Бондарчук*

Шелупанов А. А., Смолина А. Р.

Ш44 Форензика. Теория и практика расследования киберпреступлений. – М.: Горячая линия – Телеком, 2020. – 104 с.: ил.

ISBN 978-5-9912-0769-0.

Представлен анализ существующих подходов в современной отечественной практике расследования киберпреступлений. На основе накопленного практического опыта проведения экспертиз преступлений в сфере высоких технологий предложен подход по их унификации.

Для специалистов, научных работников и экспертов, занимающихся вопросами компьютерно-технической экспертизы. Будет полезна преподавателям, аспирантам и студентам, обучающимся по направлениям в области юриспруденции, защиты информации, информационной безопасности.

ББК 22.172

ISBN 978-5-9912-0769-0

ВВЕДЕНИЕ

В настоящее время киберпреступления (преступления, связанные с хищением, разрушением, нарушением целостности компьютерной информацией) занимают лидирующее положение по числу совершенных преступлений и сумме ущерба, принесенного юридическим и физическим лицам. Так, согласно данным информационного ресурса «Ведомости», только за 2014 год правоохранительными органами было зарегистрировано более 11000 компьютерных преступлений в Российской Федерации. По данным Group-IB, ущерб от компьютерных преступлений в РФ увеличивается с каждым годом — в 2015 году ущерб увеличился на 2,649 млрд рублей по сравнению с 2014 годом, а в 2016 году — на 3,811 млрд рублей по сравнению с 2015 годом [1]. В 2017 году ущерб составил более 6 млрд рублей.

Принципиально меняется характер, стиль и методы компьютерных преступлений. С расширением спектра информационных и сетевых услуг, развитием киберфизических систем, интернета вещей возникают и новые виды преступлений. Хорошо организованные преступные группы и сообщества для достижения корыстных целей активно и высокопрофессионально применяют в своей деятельности новые методы, подходы, специальные программно-аппаратные средства и технику. При этом преступные группировки не имеют национальности и принадлежности к какой-либо стране, часто работая в разных странах и имея в своем арсенале не только широкий спектр инструментов для планирования преступления, взлома информационного ресурса и сокрытия (уничтожения) цифровых следов преступлений, но и пользуются при взаимодействии собственными системами скрытой связи. В связи со значительным ростом криминального профессионализма увеличивается и сложность расследования преступлений. Мы не планируем приводить примеры удачно осуществленных кибератак, поскольку в современных СМИ таких фактов превеликое множество.

К сожалению, киберпреступления имеют очень высокую степень латентности (скрытности) — большая часть преступлений остается даже не зарегистрированной. По имеющимся у авторов сведениям, кибератакам подвергаются практически все финансовые структуры и банки. Ряд компьютерных атак завершаются успехом и наносят значительные убытки. Часто коммерческие структуры (финансовые, банковские, кредитные и др.) стремятся не афишировать успешные атаки злоумышленников с целью сохранения бизнеса и нежелательного массового оттока клиентов. Раскрываемость компьютерных преступлений составляет не более 5 % (по данным «Лаборатории Касперского»*). В связи с этим особое значение имеет компьютерно-техническая экспертиза (КТЭ). Ее целью является получение ответа на вызовы и вопросы, требующие специальных познаний в области форензики.

Форензика (forensic science или, сокращенно, forensics — судебная наука) — компьютерная криминалистика, расследование киберпреступлений — совокупность знаний о методах поиска, исследования и закрепления цифровых доказательств по киберпреступлениям. Иными словами, это поиск цифровых доказательств по совершенным киберпреступлениям. Следует отметить, что форензика, находясь на стадии развития, не имеет пока достаточных и развитых теоретических подходов, классификации, методологических основ.

Форензика, производство КТЭ и использование ее результатов являются неотъемлемыми частями комплексной деятельности по обеспечению информационной безопасности, включая выявление, идентификацию и классификацию угроз нарушения информационной безопасности, противодействие угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет, а также формирование политики обеспечения информационной безопасности.

Многие исследователи уделяют внимание только частным подходам: особенностям экспертизы систем на сетевом уровне,

---

* Лаборатории Касперского — компания, работающая в сфере информационной безопасности, и входящая в четверку ведущих мировых производителей программных решений для защиты конечных устройств (Endpoint Protection). В основу рейтинга легли данные о выручке от продаж решений класса Endpoint Security в 2012 году.

созданию корректного образа взломанной системы для ее дальнейшего исследования и др., не затрагивая при этом общих принципов и подходов к проведению расследования компьютерных преступлений.

Весомый вклад в развитие этого направления работ внесли ученые Е.Р. Россинская, А.И. Усов, Н.Н. Федотов, К. Мандиа, К. Проспис [2, 10, 13, 14, 30], сотрудники компании Group-IB [https://www.group-ib.ru], «Лаборатории Касперского» [https://www.kaspersky.ru] и другие. Научной школой профессора А.А. Шелупанова в Томском государственном университете систем управления и радиоэлектроники накоплен значительный опыт по теоретическому обоснованию подходов и методов в области форензики, а также практической деятельности [48–53, 55, 56, 110–123].

В настоящее время темпы развития науки и техники в области компьютерной криминалистики значительно опережают появление экспертного теоретического и методического обеспечения. В результате расследование киберпреступлений, производство экспертиз по ним осложняется тем, что с постоянным развитием информационных технологий появляются новые объекты исследования, которых ранее просто не было. Постоянно изменяются, модифицируются механизмы и методы совершения ранее известных видов преступлений, появляются абсолютно новые виды преступлений. Экспертам КТЭ для дачи полного достоверного научно обоснованного заключения необходимо постоянное повышение квалификации, совершенствование навыков, обновление имеющихся теоретических, практических знаний и использование соответствующей современному состоянию научной и методической литературы. КТЭ обладает существенными особенностями и отличиями от многих видов традиционной экспертизы (например, почерковедческой, дактилоскопической), где для дачи полного достоверного научно обоснованного заключения возможно использование методического обеспечения (экспертных методик) двадцатилетней давности, что неприменимо для КТЭ. Под экспертной методикой принято понимать совокупность методов, используемых при производстве экспертизы.

В основе требований, предъявляемых к экспертным методикам, лежат процессуальные нормы, изложенные в УПК РФ

и Федеральном законе № 73 от 31.05.2001 (ред. 08.03.2015) «О государственной судебно-экспертной деятельности в Российской Федерации».

Так, методы, используемые экспертами при производстве экспертизы, должны удовлетворять перечню требований, выдвигаемому отечественным судопроизводством: законности; обоснованности; достоверности получаемых результатов; безопасности; эффективности; экономичности; этичности и допустимости. Наиболее важным параметром при выборе метода исследования является допустимость. Определяющим фактором при оценке того или иного метода на допустимость является научная обоснованность и удовлетворение метода новейшим достижениям области современных научных технологий [2].

На основе проведенного критического анализа отечественных и зарубежных методических рекомендаций, находящихся в свободном доступе, ранее выполненных исследований по данной тематике установлено, что методическое обеспечение, полностью удовлетворяющее вышеописанным процессуальным нормам, положениям и требованиям, отсутствует.

Потребность в экспертных методиках испытывают не только коммерческие учреждения, но и государственные организации, занимающиеся производством компьютерно-технических, компьютерных экспертиз [3]. В настоящее время из-за отсутствия должных методик, проводя экспертизу, давая заключение, эксперт напрямую зависит от личного опыта. Выбор метода в основном определяется исходя из личных знаний, а не из методических рекомендаций, что, несомненно, порождает большое число экспертных ошибок в заключениях начинающих экспертов. Область производства КТЭ с каждым годом требует все более сложных технических подходов и средств поддержки.

При использовании устаревшей методики возможно увеличение сроков производства экспертизы, ее стоимости, трудозатрат, а также получение недостоверных результатов и заключения, не пригодного в качестве доказательства.

Наличие алгоритмического обеспечения производства КТЭ позволит сократить число экспертных ошибок и сроки производства экспертизы путем разработки с их помощью в дальнейшем системы поддержки.

В соответствии с Доктриной информационной безопасности Российской Федерации (утв. Указом Президента РФ от 5 декабря 2016 г. № 646) одним из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности является «повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям».

В программе «Цифровая экономика», принятой Правительством РФ в 2018 г., большое внимание уделено направлению информационная безопасность: «достижение состояния защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет и устойчивое социально-экономическое развитие Российской Федерации».

В результате КТЭ, проводимой при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности, формируется информация об уязвимости процессов переработки информации в информационных системах. Эти результаты могут быть использованы специалистами по информационной безопасности для совершенствования средств защиты информации и обеспечения информационной безопасности.

Таким образом, необходимы современная методика, алгоритмы производства КТЭ, способствующие обеспечению информационной безопасности объектов различных сфер деятельности (государственной, в том числе политической, оборонной, социально-экономической и культурной сфер и т. д.) от внешних и внутренних угроз хищения/разрушения/модификации информации.

Наличие актуального методического и алгоритмического обеспечения производства КТЭ, применимого при решении широкого круга вопросов, для производства экспертиз в соответствии с текущими требованиями законодательства позволяет су-

щественно повысить общесистемные уровни обеспечения информационных ресурсов, включая критически важные объекты.

Многолетний практический опыт проведения значительного числа КТЭ в интересах различных государственных и коммерческих структур, муниципальных и региональных органов власти позволил авторам провести систематизацию имеющихся в настоящее время подходов и инструментов производства КТЭ и предложить свой подход, позволивший проводить КТЭ высокого качества. В частности, представленные результаты по всем проведенным КТЭ были учтены судами и не получали ни одной рекламации или направление на проведение повторной экспертизы.

1 ИССЛЕДОВАНИЕ СОСТОЯНИЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

В данной главе исследуется текущее состояние компьютерно-технической экспертизы:

- определяются основные понятия судебной экспертизы;
- определяются основные понятия и аспекты компьютерно-технической экспертизы: род экспертизы; цели производства; задачи КТЭ; вопросы; виды КТЭ; роль КТЭ в совершенствовании существующих средств защиты информации и обеспечения информационной безопасности;
- предлагается новое определение термина КТЭ. Данное определение основывается на Приказе Министерства юстиции Российской Федерации (Минюст России) от 27 декабря 2012 г. № 237г. «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России», а также современном уровне развития науки и техники и практическом опыте производства КТЭ, подтверждающее тот факт, что рассмотренные в ходе исследования виды КТЭ при производстве большей части экспертных исследований применяются комплексно (как правило, изучение начинается с технической части, далее — программной, после — исследование данных). Предлагается введение нового определения КТЭ и внесение в связи с этим поправок в соответствующие законодательные акты;
- определяется понятие экспертной методики;
- рассматриваются требования, предъявляемые законодательством к методике (и методам) производства экспертизы;

- проводится анализ существующих методик производства КТЭ.

На основании решенных в данной главе задач определяется перечень задач, которые будут решены в следующих главах.

1.1. Понятие судебной экспертизы

Прежде чем перейти к реализации новых подходов, необходимо дать понятие судебной экспертизы.

Согласно ст. 9 Федеральному закону № 73 «О государственной судебно-экспертной деятельности в Российской Федерации» [4]:

- «*судебная экспертиза* — это процессуальное действие, состоящее из проведения исследований и дачи заключения экспертом по вопросам, разрешение которых требует специальных знаний в области науки, техники, искусства или ремесла и которые поставлены перед экспертом судом, судьей, органом дознания, лицом, производящим дознание, следователем, в целях установления обстоятельств, подлежащих доказыванию по конкретному делу;
- *заключение эксперта* — это письменный документ, отражающий ход и результаты исследований, проведенных экспертом».

Таким образом, судебная экспертиза — это особое процессуальное действие, проводимое в случае возникновения в деле вопросов, требующих специальных познаний в области науки, техники, искусства или ремесла. Понятие судебной экспертизы как средства доказывания присутствует во всех процессах [5–7]. Судебная экспертиза — это отдельный и самостоятельный вид доказательства, имеющий перед законом одинаковую доказательную силу наравне с прочими доказательствами [8].

Предметом экспертизы является информация об экспертных задачах, экспертных методиках, методах решения вопросов, а также информация об объектах и их свойствах.

Предметом исследования в рамках экспертизы является предмет познания. Под предметом познания понимаются сведения об объектах, целях и условиях исследования, полученные в опыте и используемые на практике.

Экспертные задачи делятся на общие, типовые, частные и конкретные. Общие задачи — задачи, решаемые во всех классах экспертиз (диагностические, идентификационные и классификационные задачи) [9–12]. Типовые задачи — задачи, представляющие общую формулировку задач для рода экспертизы. Частные задачи — специфичные задачи для каждой экспертизы. Конкретные задачи — это конкретные вопросы, поставленные перед экспертом.

1.2. Понятие компьютерно-технической экспертизы

КТЭ является самостоятельным родом судебных экспертиз. Она относится к классу инженерно-технических экспертиз [13]. КТЭ проводится в «целях определения статуса объекта как компьютерного средства, выявления и изучения его следовой картины в расследуемом преступлении, получения доступа к информации на носителях данных с последующим всесторонним её исследованием» [13].

Основной задачей КТЭ является ответ на вопросы, требующие специальных познаний в области форензики (компьютерной криминалистики) — знаний о методах поиска, закрепления и исследования цифровых доказательств по преступлениям, связанным с компьютерной информацией (киберпреступлениям) [14].

Согласно Приказу Министерства юстиции Российской Федерации (Минюст России) от 27 декабря 2012 г. № 237г. «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России» в рамках КТЭ происходит исследование информационных компьютерных средств [15]. Такое определение существенно ограничивает круг вопросов, решаемых КТЭ.

В современной научной среде круг вопросов, относящихся к КТЭ, значительно шире. Так, в составе КТЭ выделяют четыре вида экспертиз: аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную (она же экспертиза дан-

ных) и компьютерно-сетевую [16]. Выделение такого числа и именно таких видов экспертиз обусловлено свойствами объектов, предоставляемых на экспертизу, и задач, решаемых в рамках каждой конкретной экспертизы.

Аппаратно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием технической (аппаратной) части компьютерных средств. Как правило, эти вопросы носят диагностический характер.

Программно-компьютерная экспертиза направлена на решение вопросов, связанных с исследованием программного обеспечения. В рамках программно-компьютерной экспертизы исследуются процедуры, алгоритмы, принципы разработки программного обеспечения, а также его использование, текущее состояние, структурные особенности, особенности их эксплуатации.

Выделение *компьютерно-сетевой* экспертизы связано с бурным развитием науки и техники и появлением широкого круга специфичных задач, сопряженных с сетевыми информационными технологиями. Компьютерно-сетевая экспертиза занимается исследованием обстоятельств и фактов, связанных с применением телекоммуникационных и сетевых технологий.

Ключевым видом КТЭ, позволяющим сформировать целостное построение доказательной базы путем решения большей части диагностических и идентификационных вопросов данного рода экспертизы, является информационно-компьютерная экспертиза. *Информационно-компьютерная* экспертиза решает задачи, связанные с поиском, обнаружением, оценкой и анализом информации, содержащейся в компьютерной системе.

В результате КТЭ, проводимой при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности, формируется информация об уязвимости процессов переработки информации в информационных системах. В соответствии с правилами производства экспертизы эксперты КТЭ в своем заключении отвечают на вопросы экспертизы и не дают рекомендаций по совершенствованию существующих средств защиты информации и обеспечения информационной безопасности (если это не является вопросом экспертизы). При этом резуль-

таты КТЭ могут быть использованы специалистами по информационной безопасности для совершенствования существующих средств защиты информации и обеспечения информационной безопасности.

Исследования [15], а также современный уровень развития науки и техники и практический опыт производства КТЭ, подтверждают тот факт, что рассмотренные выше виды КТЭ при производстве большей части экспертных исследований применяются комплексно (как правило, изучение начинается с технической части, далее — программной, после — исследование данных). К сожалению, законодательная практика отстает от практики реального проведения экспертизы. Так было и скорее всего будет всегда. Поэтому авторы предлагают введение нового определения КТЭ и внесение в связи с этим *принципиальных поправок* в соответствующие законодательные акты. Под КТЭ мы предлагаем понимать *самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимых в целях выявления и изучения следовой картины в расследуемом преступлении путем комплексного исследования компьютерных средств: технической (аппаратной) части компьютерных средств; программного обеспечения; объектов сетевых информационных технологий; информации, содержащейся в компьютерной системе.*

В дальнейшем термин КТЭ используется авторами именно в этой трактовке.

1.3. Понятие экспертной методики

Существует несколько определений понятия «экспертная методика» [17–20]. В общем смысле под экспертной методикой (методикой экспертного исследования) понимается последовательность изучения свойств объекта экспертизы с целью решения экспертной задачи путем упорядоченного применения научно разработанной системы методов экспертного познания.

Экспертная методика может содержать последовательность как категорических, так и альтернативных методов, средств решения задач.

Экспертные методики разделяются на общие, частные и конкретные.

Общая методика описывает технологию экспертного исследования и является общей для всех видов экспертиз.

Частная методика создается под частную ситуацию определенного рода, вида экспертиз.

Конкретная методика — методика, используемая для производства отдельной экспертизы. Как правило, конкретная методика — это частная методика, адаптированная под определенные задачи отдельной экспертизы.

Предлагаемая авторами методика относится к виду частных методик — она содержит практические рекомендации и при этом является применимой для решения широкого круга частных задач КТЭ.

1.4. Требования законодательства к методике и методам производства экспертизы

Требования законодательства к методике и методам производства экспертизы в целом и КТЭ в частности определяются основными процессуальными нормами, определенными УПК РФ в отношении судебной экспертизы, а также Федеральным законом № 73 «О государственной судебно- экспертной деятельности в Российской Федерации».

Российское судопроизводство выдвигает следующий перечень требования к экспертному заключению [3]:

- полнота — указание всех признаков; исследование в отношении всех поставленных вопросов; ответ на все поставленные вопросы; исследование всех объектов, предоставленных на исследование; исследование всех материалов, относящихся к предмету экспертизы; использование необходимых методик, обеспечивающих полноту исследования;
- объективность — применение объективно существующих специальных знаний; объективный подход к исследованию; использование научно обоснованных методик;
- всесторонность — изучение объекта со всех сторон, в том числе экспертная инициатива;
- достоверность — возможность проверки экспертного заключения на относимость (относимость установленного факта к предмету доказывания);

- допустимость (возможность допущения экспертного заключения, как средства доказывания — соблюдение процессуальных требований);
- доказательность — установление доказательного значения как факта.

Приведенный перечень требований к экспертному заключению определяет перечень требований к экспертной методике, с использованием которой оно дается. Экспертная методика должна обеспечивать полноту исследования, быть научно обоснованной, всесторонне исследовать объект и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, эффективной, экономичной, этичной, допустимой.

Законодательство не ограничивает эксперта в выборе методов исследования. Определяющим фактором при оценке того или иного метода на допустимость является научная обоснованность и удовлетворение метода новейшим достижениям области современных научных технологий [3]. В мире информационных технологий, в отличие от многих видов классических экспертиз (например, почерковедческой, дактилоскопической), развитие науки и техники происходит очень быстро, что делает применение методик КТЭ десятилетней давности лишь ограниченно, частично, а порой и вовсе непригодными в связи с появлением новых объектов, новых вопросов, новых способов совершения преступлений. В этой ситуации приобретает большое значение научная специализация, профессиональный уровень и личный опыт эксперта КТЭ.

Допустимость методов КТЭ для эксперта зависит также от их безопасности, характера воздействия на объект исследования, времени получения результатов [3, 21].

Методы КТЭ должны быть эффективны, рентабельны и обеспечивать решение задач исследования в оптимальные сроки с наибольшей продуктивностью. Ценность полученных результатов должна быть соизмерима с затраченными силами.

Объектами КТЭ «являются вещественные доказательства, которые согласно принципу непосредственности, действующему при судебном разбирательстве, необходимо представить в суд неизмененными» [22]. В связи с этим использование неразрушаю-

щих (недеструктивных) методов проведения исследования является предпочтительным. В методическом обеспечении КТЭ может быть использовано следующее разделение методов исследования компьютерных средств и систем в зависимости от степени сохранности объекта [23]:

- методы, никак не влияющие на объект КТЭ и не требующие реализации процедур пробоподготовки;
- методы, не разрушающие объект КТЭ, но изменяющие его состав, структуру или отдельные свойства;
- методы, не разрушающие образец, но требующие для его изготовления разрушения или видоизменения объекта;
- методы, полностью или частично разрушающие объект КТЭ или образец.

Перечень задач и объектов КТЭ довольно разнороден. Этот факт обусловливает большое число экспертных средств и методов. Авторами детально рассмотрен ряд методик производства КТЭ. К сожалению, ни одна из них не удовлетворяет полностью всем требованиям, выдвигаемым отечественном российским судопроизводством.

В качестве примера в следующем подразделе приведено описание преимуществ и недостатков основных существующих экспертных методик.

1.5. Анализ методик производства КТЭ

Ниже представлены результаты анализа ряда методик производства КТЭ. В ходе работы был проведен анализ большего числа методик, технической литературы, научных исследований [2, 3, 10, 14, 16, 23–51], но представлены результаты именно тех методик, которые наиболее часто используются экспертами при производстве КТЭ:

Результаты анализа методики, изложенной в [24]

Методическое обеспечение [24] рекомендовано эспертно-криминалистическим центром МВД России для проведения исследований и экспертиз по программам для ЭВМ на территории Российской Федерации. В результате анализа данного источника информации установлено, что в представленной реализации он не может являться методическим пособием по производству

КТЭ, так как не удовлетворяет требованиям, выдвигаемым отечественным судопроизводством.

Недостатками, ошибками и неточностями (исходя из требований к производству КТЭ и методикам судебной экспертизы [4–7]), являются:

- неточность трактовки понятий «эксперт» и «специалист»;
- не полный перечень прав эксперта и возможных ходатайств эксперта;
- не указано, что согласно ч. 3 ст. 80 УПК специалист дает заключение;
- указаны не все сведения, которые должны содержаться в заключении эксперта, в частности в заключении обязательно должна содержаться информация обо всех заявленных ходатайствах;
- указаны не все сведения, которые должны содержаться в постановлении/определении о назначении экспертизы, в частности в постановлении/определении обязательно должны быть указаны: место и время; лицо назначившее экспертизу; номер дела; какая назначена экспертиза; объекты, предоставленные на экспертизу; права и обязанности эксперта, подписка;
- фраза: «каждый эксперт вправе подписать общее заключение либо ту его часть, которая отражает ход и результаты проведенных им лично исследований» является неверной, так как при производстве комплексной экспертизы общий (совместный) вывод формулируют эксперты, компетентные в оценке полученных результатов и формулировании общих выводов [4]. Если при этом им необходимы данные других экспертов, то они вправе их использовать, указывая на это;
- требование «вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза», к вопросам, выносимым на экспертизу, является ложным. Экспертиза назначается, когда в деле возникают вопросы, требующие специальных знаний. Основная цель экспертизы [4] — помочь разобраться суду, следователю, дознавателю и участникам процесса в сложной ситуации. Если же в экспертной организации нет необходимой материально-техниче-

ской базы или эксперт недостаточно компетентен, то экспертной организацией/экспертом должно быть дано сообщение о невозможности дать заключение [4];

- при указании задач, для решения которых могут потребоваться специальные знания в области компьютерной информации, указано «установление стоимости экземпляров произведений». Данное утверждение является ошибочным, так как при производстве КТЭ не решаются вопросы установления стоимости объектов [52];
- вариант исследования информации с применением блокираторов даже не рассматривается, т. е. безальтернативно предлагается исследование разрушающими методами, как следует из фразы «при отсутствии технической возможности или целесообразности копирования информации»;
- в данном методическом пособии отсутствуют рекомендации по программному обеспечению, которое возможно использовать при решении экспертных задач;

Данное методическое пособие имеет и свои преимущества:

- указаны преимущества и недостатки некоторых методов исследования (исследование клона/копии или непосредственно самого объекта);
- содержатся: перечень типовых следственных ситуаций; задачи, для решения которых могут потребоваться специальные знания в области компьютерной информации, по каждой следственной ситуации (хотя некоторые из задач ошибочно отнесены к задачам КТЭ); наиболее целесообразные виды использования специальных знаний;
- обозначены ошибки, допускаемые экспертами КТЭ;
- указаны «внешние технические признаки контрафактности».

Результаты анализа методики, изложенной в [25]

Методические рекомендации [25] одобрены и рекомендованы к опубликованию Методическим и Редакционно-издательским советами ГУ ЭКЦ МВД России.

Данные методические рекомендации имеют ряд положений, которые остаются актуальными и после более чем десятка лет (задачи КТЭ, классификация видов КТЭ, классификация объектов КТЭ), но в целом требуют дополнения в связи с развитием информационных технологий.

Утарел перечень объектов КТЭ. Так, при описании аппаратных устройств приводится описание такой «новой разработки», как ноутбук. При описании основных видов операционных систем даже не упоминаются операционные системы (ОС) Windows XP/Vista/7/8/10 и более современные версии ОС; перечень основных видов файлов весьма ограничен.

В разделе, содержащем указания по порядку выключения компьютера, не рассматриваются способы выключения в зависимости от операционной системы.

При описании краткого содержания экспертного исследования на стадии исследования жесткого диска (накопителя на жестких магнитных дисках, НЖМД) не указана возможность проведения исследования непосредственно самого жесткого диска без частичного разрушения информации — с использованием блокираторов записи.

Приведенный пример заключения эксперта содержит некоторые недочеты [4]: не указано время производства экспертизы, отсутствует описание примененных методик.

Результаты анализа методики, изложенной в [26]

Учебно-методическое пособие [26] подготовлено авторским коллективом Следственного комитета при МВД России и кафедры криминалистики юридического факультета МГУ им. М.В. Ломоносова. Это учебно-методическое пособие очень сильно устарело и в настоящее время применимо по большей части как литература по истории развития КТЭ, чем руководство к практической работе по КТЭ. Часть рекомендаций применима и в настоящее время, так как содержит указания по общим задачам КТЭ: виды следов преступной деятельности в ЭВМ; общие правила обращения с вычислительной техникой и носителями информации; упаковка объектов; особенности подготовки к проведению обыска; особенности выдвижения следственных версий.

Часть вопросов, отнесенных к вопросам КТЭ, не допустима для КТЭ в той редакции, в которой они указаны: «Кто разработчик данного обеспечения?»; «Имеют ли комплектующие компьютера (печатные платы, магнитные носители, дисководы и пр.) единый источник происхождения?»; «Являются ли данные программные продукты лицензионными (или несанкционированными) копиями стандартных систем или оригинальными разработ-

ками?»; «Какое время проходит с момента введения данных до вывода результатов при работе данной компьютерной программы, базы данных?»; «Исправен ли компьютер и его комплектующие? Каков их износ?...»; «Где и когда изготовлен и собран данный компьютер и его комплектующие? Осуществлялась ли сборка компьютера в заводских условиях или кустарно?». К сожалению, ни один из приведенных примеров в настоящее время практически неприменим.

Результаты анализа методики, изложенной в [14]

Методика [14] не является экспертно-методическим пособием, но содержит ряд научно обоснованных и соответствующих современному уровню развития техники методических указаний по производству КТЭ. Как указано в аннотации: «книга рассказывает о методах раскрытия и расследования компьютерных преступлений, правилах сбора, закрепления и представления доказательств по ним применительно к российскому законодательству. В книге имеются также сведения, относящиеся к гражданским делам, в которых затрагиваются информационные технологии, — таким как дела об авторских правах на программы для ЭВМ и иные произведения в электронной форме, дела о доменных именах, дела об использовании товарных знаков и других средствах индивидуализации в Интернете». Что наиболее важно, всё это не просто описано в общих словах, а даны четкие, лаконичные рекомендации по практическим действиям в конкретной ситуации.

Н.Н. Федотовым отмечено, что «для полного понимания данной книги» необходимо владеть определенным уровнем знаний. Этот момент отличает её от трёх вышеописанных источников, в которых практикуется весьма популяризаторский подход (материал излагается поверхностно, не требует от читателя знания специальности).

С точки зрения авторов данной работы, книга [14] является хорошим вспомогательным инструментом для эксперта КТЭ и при условии некоторых изменений (устранении/сокращении личностной оценки, более развернутом описании рекомендаций) может быть хорошей методикой КТЭ. К сожалению, многие сведения, изложенные в книге, в силу очевидных причин устарели.

Результаты анализа методики, изложенной в [23]

Большая часть информации представляет собой теоретические основы КТЭ без практических рекомендаций: теоретические и организационные основы использования специальных познаний в процессе судопроизводства по делам, сопряженным с применением компьютерных средств; требования к методикам; особенности назначения КТЭ и т. п.

Для решения практических задач КТЭ этот источник просто не применим.

Результаты анализа методики, изложенной в [2]

В книге представлены основы методического обеспечения КТЭ. Она является учебным пособием в данной области, в ней описаны теоретические вопросы КТЭ, большое внимание уделено практическим вопросам производства КТЭ. Указаны рекомендации по действиям эксперта, и дано подробное описание аппаратно-программного экспертного инструментария.

Описанные данные несколько устарели. Так, описанный анализ ОС не содержит рекомендаций по анализу современных и широко распространенных ОС Linux, Windows Vista/7/8/10 и более высоких версий ОС, отсутствуют рекомендации по действиям эксперта при производстве экспертиз по «молодым» видам преступлений в сфере информационных технологий: «фишинг», «нарушение авторских прав в сети», «кардерство» и т. д. Методика в настоящее время лишь частично актуальна и недостаточно полна.

1.6. Результаты анализа методик производства КТЭ

Помимо вышеописанных основных методик производства КТЭ, приведенных выше авторами в качестве примера, было исследовано большое число технической литературы, посвященной вопросам КТЭ, авторские методики производства КТЭ, изложенные в научных работах [2, 3, 10, 14, 16, 23–51].

В результате проведенного анализа был сделан следующий вывод [53]:

- существующие методики производства КТЭ не соответствуют полностью всем требованиям законодательства РФ [4–7];

- многие методики производства КТЭ практикуют популяризаторский подход;
- часть методик содержит смысловые ошибки;
- создание новой методики производства КТЭ является актуальным, необходимым в настоящее время;
- при создании новой методики производства КТЭ необходимо учитывать опыт отечественных и зарубежных авторов.

1.7. Резюме

Понятие судебной экспертизы как средства доказывания присутствует во всех процессах [5–7]. Судебная экспертиза является отдельным и самостоятельным видом доказательства, имеющим перед законом одинаковую доказательную силу наравне с прочими доказательствами [8].

КТЭ является самостоятельным родом судебных экспертиз.

Учитывая [8], а также современный уровень развития науки, техники и практический опыт производства КТЭ, подтверждающий тот факт, что при производстве большей части экспертных исследований осуществляется комплексное исследование (технической части, программной, исследование данных), авторами предлагается введение нового определение КТЭ и внесение в связи с этим поправок в соответствующие законодательные акты.

Под компьютерно-технической экспертизой предлагается понимать *самостоятельный род судебных экспертиз, относящийся к классу инженерно-технических экспертиз, проводимой в целях выявления и изучения следовой картины в расследуемом преступлении путем комплексного исследования компьютерных средств: технической (аппаратной) части компьютерных средств; программного обеспечения; объектов сетевых информационных технологий; информации, содержащейся в компьютерной системе.*

В общем смысле под экспертной методикой (методикой экспертного исследования) понимается последовательность изучения свойств объекта экспертизы с целью решения экспертной задачи путем упорядоченного применения научно разработанной системы методов экспертного познания.

Требования законодательства к методике и методам производства экспертизы в целом и к КТЭ в частности определяются

основными процессуальными нормами, определенными УПК РФ в отношении судебной экспертизы, и Федеральным законом № 73 «О государственной судебно-экспертной деятельности в Российской Федерации».

Экспертная методика должна обеспечивать полноту исследования, быть научно обоснованной, всесторонне исследовать объект и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, эффективной, экономичной, этичной, допустимой.

В результате проведенного анализа существующего экспертно-методического обеспечения нами установлено отсутствие методик, соответствующих всему комплексу требований законодательства РФ, и необходимость в разработке методики производства КТЭ.

Установлена проблема поиска частной методики производства КТЭ и выбора методов в рамках найденной методики, соответствующих потребностям экспертной организации (эффективных по заданному критерию ресурса).

Таким образом, для ускорения, упрощения поиска методики производства КТЭ и обеспечения возможности автоматизации этого процесса необходимо:

- провести классификации методик КТЭ с точки зрения задач исследования, целей исследования (вопросов экспертизы) и объектов исследования;
- в соответствии с проведенной классификацией построить формальную модель методики производства КТЭ;
- на основе формальной модели определить подход, позволяющий получить последовательность методов для каждой из стадии экспертизы, эффективную по заданному критерию (например, временные ресурсы, финансовые ресурсы, человеческие ресурсы и т. д.);
- в рамках сформированного подхода к проведению судебной экспертизы создать методику производства КТЭ с учетом требований возможности дальнейшей автоматизации;
- для всех стадий экспертизы предложенной методики КТЭ разработать алгоритмическое обеспечение, предназначенное для решения наиболее востребованных частных задач КТЭ.

2 КЛАССИФИКАЦИЯ МЕТОДИК И ПОСТРОЕНИЕ МОДЕЛИ МЕТОДИКИ ПРОИЗВОДСТВА КТЭ

В настоящее время имеется проблема поиска методики производства КТЭ и выбора методов в рамках найденной методики, соответствующих потребностям экспертной организации (с учетом ограничений по срокам производства, финансовым ресурсам и т. д.). Это обусловлено, прежде всего, бурным развитием информационных технологий — появлением новых объектов и вопросов КТЭ и устареванием существующих методик и методов.

Для ускорения и упрощения поиска методики производства КТЭ, а также для обеспечения возможности автоматизации этого процесса проведем классификацию методик производства КТЭ и построим модель методики производства КТЭ. Далее в рамках выбранной методики определим методы производства КТЭ, наиболее подходящие экспертной организации с точки зрения заданного ей критерия (сроки производства, финансовые ограничения, человеческие ресурсы и т. д.). Попробуем формализовать критерии классификации методик КТЭ, разработки модели методики производства КТЭ, определим подход для выбора методов производства КТЭ и определения сроков производства комплексной экспертизы.

2.1. Базовые критерии классификации методик КТЭ

Содержание экспертных методик КТЭ определяется задачами, целями и объектами рассматриваемого рода судебных экспертиз.

Описание методов и алгоритмов классификации зачастую основывается на представлении исходной информации о классифицируемых объектах в виде графов [54–62]. Далее в работе будет

использован подход к классификации и буквенная нотация, предложенные в [54] и использованные в [56].

Для классификации методик КТЭ предлагается использование теории графов, в частности ориентированный граф $A(B, C)$, в котором:

- $B = \{b_0, b_{1,1}, b_{1,2} \ldots, b_{i,j}, b_e\}$ — множество вершин графа A;
- C — множество ориентированных рёбер графа A;
- начало классификации — вершина b_0;
- конец классификации — вершина b_e;
- i — число критериев классификации методик;
- j — число признаков конкретного критерия.

В настоящее время число критериев классификации методик производства экспертизы $i = 3$, а число признаков для КТЭ удовлетворяет требованию $3 \leqslant j \leqslant 4$ в зависимости от каждого конкретного критерия.

Предлагаемый подход к классификации методик КТЭ с использованием теории графов может быть использован независимо от состава и числа критериев классификации методик и признаков критериев классификации методик. Более того, данный подход может быть использован для классификации методик других родов и видов экспертиз, т. е. этот подход является унифицированным.

Для классификации методик КТЭ используются простые пути на графе. Задача эксперта КТЭ по выбору необходимой методики производства КТЭ сводится к поиску пути на графе, т. е. определение путей между вершинами b_0 и b_e и будет процессом определения методики производства КТЭ.

Множеством простых путей между вершинами b_0 и b_e определяется множество методик производства КТЭ (М). Существующие в настоящее время критерии классификации методик КТЭ и признаки критериев представлены в табл. 2.1.

В рамках предложенного подхода, для возможности автоматизации и унификации, авторами предлагается построить граф, где базовые критерии для классификации методик КТЭ формируют множество $B = \{b_0, b_{1,1}, b_{1,2} \ldots, b_{i,j}, b_e\}$ вершин графа A (рис. 2.1).

Согласно рис. 2.1 свойства методик критериев i (объекты КТЭ) не имеют зависимостей от значений критериев 2, а кри-

Таблица 2.1

Критерии классификации методик КТЭ [2]

Критерий	Признак критерия
1. Категория задач	1.1. Диагностические — направлены на определение свойств и состояний объекта, определение факта его изменения, определение причины этих изменений и ее связи с рассматриваемым делом (например, причины возникновения ошибок в работе программного обеспечения или неисправности ноутбука) [2] 1.2. Классификационные — направлены на установление характеристик (свойств) неизвестного/известного объекта с целью отнесения его к общепринятому классу (например, отнесение графического редактора к классу векторных или растровых) [2] 1.3. Идентификационные — направлены на установление тождества объекта самому себе, индивидуально-конкретного тождества (например, идентификация программного обеспечения по предоставленному образцу лицензионного программного обеспечения) [2]
2. Цели (вопросы КТЭ)	2.1. Относящиеся к аппаратным средствам [2] 2.2. Относящиеся к программным средствам [2] 2.3. Относящиеся к данным (информации) [2] 2.4. Относящиеся к вычислительной сети и ее элементам [2]
3. Объекты КТЭ	3.1. Аппаратные средства [2] 3.2. Программные средства [2] 3.3. Данные (информация) [2] 3.4. Вычислительная сеть и ее компоненты [2]

терии 2 не имеют зависимостей от значений критериев 1. То есть методики, относящиеся к любой из трех категорий задач (диагностические, классификационные, идентификационные), могут предназначаться для решения вопросов любой из четырех групп, объектами которых могут являться объекты любой из четырех групп.

Результатом классификации методик КТЭ будет определение методики КТЭ (типа методики КТЭ). Обозначим через m_{ij} тип методики КТЭ. Тогда типы методик КТЭ m_{ij} определяются множеством M — простых путей графа А из вершины b_0 в вершину b_e, где:

- i — порядковый номер типа методики в предложенной классификации типов методик, $1 \leqslant i \leqslant 12$;
- j — тип объекта (см. табл. 2.1).

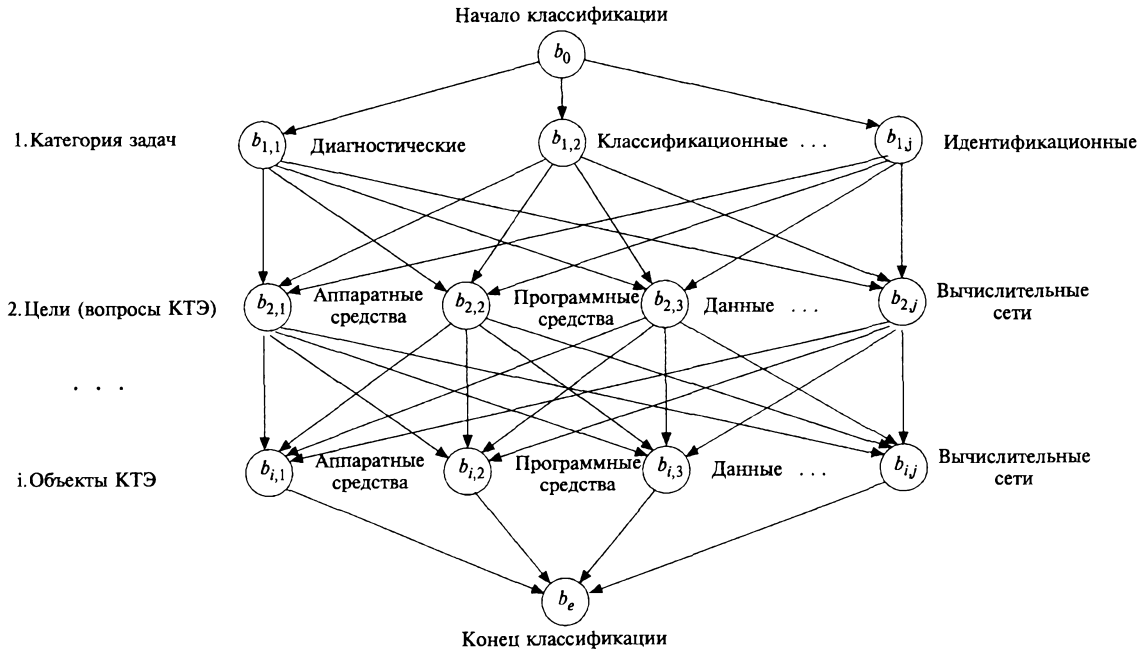


Рис. 2.1. Граф классификации методик производства КТЭ

Для предлагаемого набора методик в рамках классификации выделено 12 основных типов методик КТЭ, каждому из которых соответствует 4 типа методик. Общее число типов экспертных методик КТЭ — 48. Выделенные основные 12 типов методик представлены в табл. 2.2.

Таблица 2.2

Множество M типов методик КТЭ

Тип методики КТЭ	Значение
$m_1 = \langle b_{1,1}, b_{2,1}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение диагностических задач с целью ответа на вопросы, относящиеся к аппаратным средствам
$m_2 = \langle b_{1,1}, b_{2,2}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение диагностических задач с целью ответа на вопросы, относящиеся к программным средствам
$m_3 = \langle b_{1,1}, b_{2,3}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение диагностических задач с целью ответа на вопросы, относящиеся к данным (компьютерной информации)
$m_4 = \langle b_{1,1}, b_{2,4}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение диагностических задач с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам
$m_5 = \langle b_{1,2}, b_{2,1}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение классификационных задач с целью ответа на вопросы, относящиеся к аппаратным средствам
$m_6 = \langle b_{1,2}, b_{2,2}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение классификационных задач с целью ответа на вопросы, относящиеся к программным средствам
$m_7 = \langle b_{1,2}, b_{2,3}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение классификационных задач с целью ответа на вопросы, относящиеся к данным (компьютерной информации)
$m_8 = \langle b_{1,2}, b_{2,4}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение классификационных задач с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам
$m_9 = \langle b_{1,3}, b_{2,1}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение идентификационных задач с целью ответа на вопросы, относящиеся к аппаратным средствам

Окончание табл. 2.2

Тип методики КТЭ	Значение
$m_{10} = \langle b_{1,3}, b_{2,2}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к программным средствам
$m_{11} = \langle b_{1,3}, b_{2,3}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации)
$m_{12} = \langle b_{1,3}, b_{2,4}, b_{3,j} \rangle$, $j \in \{1,2,3,4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам

Таким образом, можно выявить общие свойства методик производства КТЭ и сформировать базовые критерии и признаки их классификации. Процесс классификации по базовым критериям описан в виде ориентированного графа с описанием множеств его вершин и дуг. Критерии классификации разделены на три уровня, определяющих свойства методик КТЭ. Полученные 48 типов методик представлены в виде множества. Предложенный подход к классификации экспертных методик является унифицированным и может быть применен для классификации экспертных методик любых видов и родов экспертиз.

Полный перечень вопросов КТЭ, сформированный на основании предложенной классификации методик КТЭ, представлен в Приложении.

2.2. Содержание модели методики производства КТЭ

Технология экспертного исследования описывается общей методикой производства экспертиз и является общей для всех видов.

Согласно общей методике производства экспертиз, экспертное исследование состоит из следующих стадий [23].

Подготовительная — основной целью этой стадии является уяснение экспертом экспертной задачи, для чего рассматриваются поставленные вопросы, формируется общее представление о

состоянии и признаках исследуемых объектов (в результате представленных объектов), происходит ознакомление с постановлением и материалами дела (имеющими отношение к экспертизе). На данной стадии выдвигаются рабочие гипотезы, определяются необходимые методы, приемы и средства исследования, а также алгоритм их применения, составляется план работы. В случае необходимости запрашиваются дополнительные материалы, изучается специальная и справочная литература. В завершении стадии экспертом даются предварительные выводы.

Аналитическая — на этой стадии выполняется тщательное исследование объектов. На аналитической стадии экспертом используются рабочие инструментальные методы и технические средства. Ход проведения исследования, используемые методы фиксируются. В завершении стадии экспертом даются предварительные выводы. Сделанные на аналитической стадии выводы дополняются на последующих стадиях исследования.

Эксперимент (наличие этой стадии зависит от каждой конкретной ситуации). Эксперимент проводится экспертом в целях выявления механизма взаимодействия объектов экспертного исследования и (или) механизма следообразования, его отдельных параметров. В ходе эксперимента эксперт изучает интересующие его процессы и условия. Наличие/отсутствие этой стадии определяется задачами и целями экспертного исследования. Результаты эксперимента оформляются в виде предварительных выводов по данной стадии.

Синтезирующая — заключается в синтезе информации на основе проведенного анализа.

Результативная — на этой стадии происходит подведение итогов, оцениваются результаты проведенных исследований.

Формирование выводов — на этой стадии оформляются выводы по экспертизе.

На основе проведенных стадий экспертного исследования формируется экспертное заключение, состоящее из трех обязательных частей [4–7]:

- вводная — описание и результаты подготовительной стадии;
- исследовательская — описание и результаты анализирующей части эксперимента, синтезирующей и результативной частей;

- выводы — формирование выводов (стадия «*формирование выводов*»).

Методика производства КТЭ, как и методика любого другого рода экспертизы, базируется на совокупности методов производства экспертизы.

Частная методика содержит как методы, применимые во всех видах экспертиз (в основном методы, используемые на подготовительной стадии), так и частные методы, применимые только в определённых типах вида экспертизы (в основном методы, используемые на аналитической, синтезирующей стадии или при эксперименте).

В общем смысле под экспертной методикой (методикой экспертного исследования) понимается последовательность изучения свойств объекта экспертизы с целью решения экспертной задачи путем упорядоченного применения научно разработанной системы методов экспертного познания.

При производстве экспертизы применяются методы из четырех категорий:

- всеобщие методы познания — материалистическая диалектика;
- общенаучные методы — к ним относятся наблюдение, измерение, описание, эксперимент, моделирование;
- частные методы — инструментальные методы, применимые для определённого рода экспертизы;
- специальные методы — частные методы, адаптированные под производство конкретной экспертизы.

Некоторые методы, примененные на одной стадии, могут быть использованы и на другой стадии (например, наглядно-образный метод представления информации используется для фиксации результатов на всех стадиях исследования), т. е. существуют методы общие для нескольких стадий экспертного исследования.

Методы делятся на простые (описывают способ выполнения одного действия) и комплексные (описывают способ выполнения нескольких действий).

Предлагается унифицировать методику производства КТЭ. Для этого представим элементы методики КТЭ в виде множеств:

$D = \{d_1, d_2, \ldots, d_l\}$ — множество методов подготовительной стадии исследования, где l — число методов подготовительной стадии исследования;

$V = \{v_1, v_2, \ldots, v_w\}$ — множество методов аналитической стадии исследования, где w — число методов аналитической стадии исследования;

$G = \{g_1, g_2, \ldots, g_u\}$ — множество методов стадии эксперимента, где u — число методов стадии эксперимента;

$E = \{e_1, e_2, \ldots, e_q\}$ — множество методов синтезирующей стадии исследования, где q — число методов синтезирующей стадии исследования;

$F = \{f_1, f_2, \ldots, f_p\}$ — множество методов результативной стадии исследования, где p — число методов результативной стадии исследования;

$H = \{h_1, h_2, \ldots, h_t\}$ — множество методов стадии формирования выводов, где t — число методов стадии формирования выводов.

Методы стадий исследования могут быть простыми или комплексными, их тип и содержание зависит от того, к какому классу отнесена методика.

Элемент множества $S = \{s_1, s_2, \ldots, s_n\}$ — методов унифицированной методики производства КТЭ — представляет собой кортеж, состоящий из шести элементов:

$$s_n \in S = (d_l, v_w, g_u, e_q, f_p, h_t),$$

где $d_l \in D$, $v_w \in V$, $g_u \in G, e_q \in E, f_p \in F, h_t \in H$.

Множество методов, используемых при производстве КТЭ, является подмножеством декартового произведения множеств методов стадий экспертного исследования:

$$S \subset D \times V \times G \times E \times F \times H.$$

Тогда моделью методики производства КТЭ будет являться упорядоченное множество взаимосвязанных методов КТЭ S, лежащих на одном пути графа A.

Если S содержит помимо всеобщих методов познания и общенаучных методов познания частные методы, то на основании множества S определяется частная методика производства КТЭ.

Рис. 2.2. IDEF0-диаграмма процесса определения методики производства КТЭ

Если S содержит помимо всеобщих методов познания, общенаучных методов познания и частных методов специальные методы, то на основании множества S определяется конкретная методика производства КТЭ.

Эта модель методики производства КТЭ может быть использована для разработки общих, частных и конкретных методик, относящихся к любому типу методик КТЭ, согласно классификации, предложенной в предыдущем подразделе. Этот процесс может быть автоматизирован. Представим процедуру определения методики с помощью структурного подхода. В качестве методологии функционального моделирования и графической нотации используем IDEF0. Для построения диаграммы здесь и далее использовался веб-ресурс **https://www.draw.io/**. Контекстная диаграмма процедуры определения методики производства КТЭ представлена на рис. 2.2.

Как указано на рис. 2.2, входными данными при определении методики производства КТЭ являются постановление/определение о назначении экспертизы, объекты экспертизы и данные о предмете экспертизы. Под данными о предмете экспертизы понимается в соответствии с процессуальными кодексами: информация об исследуемых данным видом экспертизы объектах, их свойствах, экспертных задачах и методиках. При автоматизации процесса определения методики данные о предмете экспертизы могут быть перенесены в базу данных разрабатываемой системы. Так как в рамках работы не предусмотрена разработка программного обеспечения (ПО) для автоматизации рассматриваемого

процесса, то выполняется он экспертом вручную, после автоматизации основным механизмом также будет ПО определения методики. По итогам данной процедуры принимается решение о составе и последовательности выполнения методики.

2.3. Применение методов КТЭ

Высокоуровневый алгоритм производства КТЭ аналогичен алгоритму производства прочих видов экспертиз [4, 27]. В его основе лежит применение на каждой стадии экспертизы методов, необходимых для ее (стадии) выполнения.

Высокоуровневый алгоритм производства КТЭ, представляющий собой последовательность стадий экспертизы, приведен на рис. 2.3.

Алгоритм построен на основе [16].

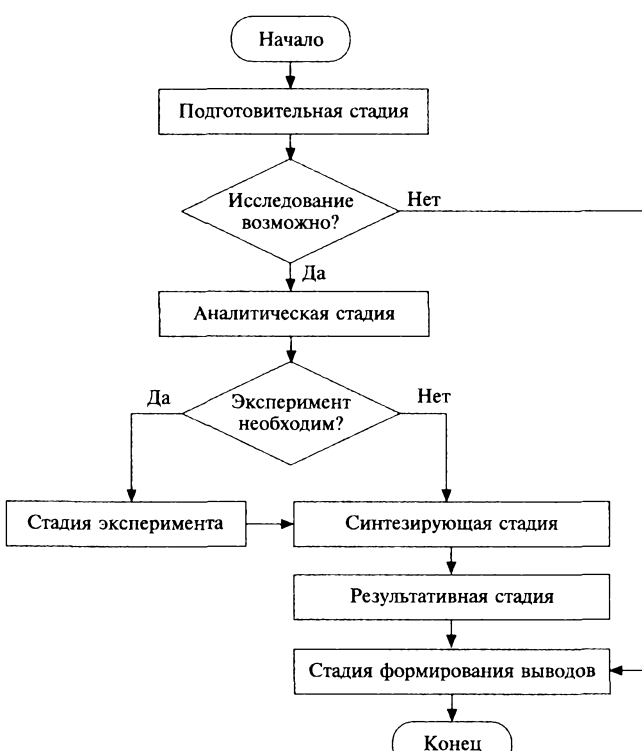


Рис. 2.3. Высокоуровневый алгоритм производства КТЭ

Методы, применяемые на каждой из стадий КТЭ, должны соответствовать выбранной методике производства КТЭ (подход к классификации и выбору методики представлен в разделе 2.1 и на рис. 2.2). Вместе с тем во многих методиках КТЭ одновременно описываются несколько методов, предоставляющих возможность провести всестороннее и полное исследование и направленных на решение одних и тех же задач. В этом случае (при наличии в экспертном учреждении технологической возможности проведения исследования любым из допустимых методов) для определения метода исследования предлагается выбирать метод с учетом наличия ресурсов в экспертной организации (финансовых, временных, человеческих и т. д.). Так, поиск методов предлагается выполнить, обратившись к теории графов, и решить данную задачу как типовую задачу теории графов — задачу о поиске кратчайшего пути [63].

Для поиска методов КТЭ воспользуемся ориентированным графом RR (R, RE), где:

- $R = \{r_0, r_{1,1}, r_{1,2} \ldots, r_{i,j}, r_e\}$ — множество вершин графа RR;
- RE — множество ребер d_{ij} графа RR. Каждому ребру RE сопоставлен вес k_{ij};
- вершина r_0 — начало производства КТЭ;
- вершина r_e — завершение производства КТЭ;
- i — число альтернативных методов на определенной стадии производства КТЭ, $i \geqslant 1$;
- j — число стадий производства КТЭ, $j \geqslant 1$;
- k_{ij} — вес ребра, обозначает длину ребра — неотрицательное число, характеризующее затраты ресурса (число затрачиваемого времени, либо необходимое число экспертов, либо финансовые затраты), по которому проводится определение методов.

Веса ребер определяются опытными экспертами экспертной организации исходя из конкретной технико-экономической характеристики экспертного учреждения и пересматриваются при ее изменении. Расставленные веса используются далее при производстве экспертиз экспертами, в том числе экспертами невысокой квалификации.

Частный случай графа поиска методов КТЭ в рамках выбранной методики представлен на рис. 2.4.

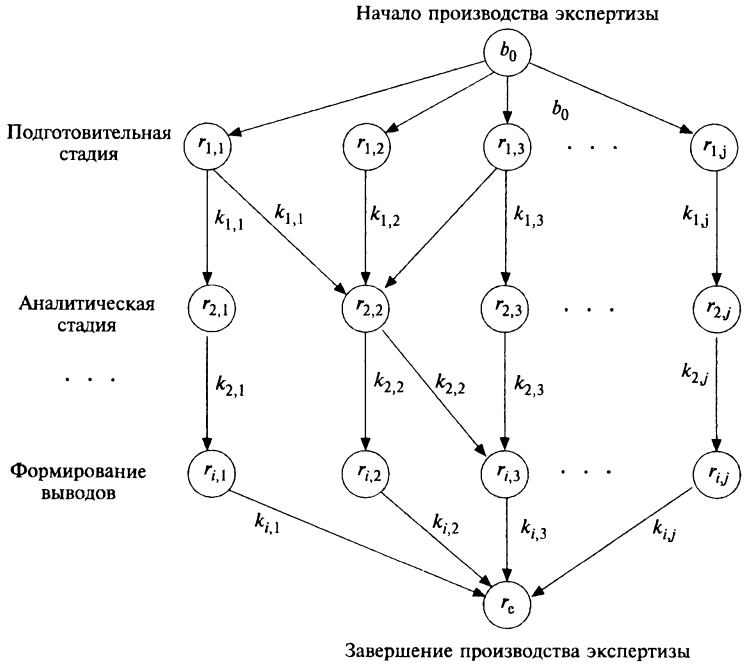


Рис. 2.4. Частный случай графа поиска методов производства КТЭ

Данная задача имеет следующие особенности:

- для определения последовательности методов используется ориентированный граф;
- наличие большого числа вершин в графе;
- отсутствие в графе ребер с отрицательным весом;
- путями минимальной длины должны быть соединены с первой вершиной все вершины, содержащиеся в схеме (методике);
- конечная схема методов не может содержать цикла;
- конечная схема методов может не содержать все вершины графа;
- необходимо знать как длину кратчайшего пути, так и список вершин, через которые проходит он;
- на вес ребра могут влиять несколько несвязанных параметров, например затраты на производство экспертизы и сроки производства экспертизы.

Рис. 2.5. IDEF0-диаграмма процесса формирования частной методики, эффективной по заданному ресурсному критерию

Так как задача имеет ряд особенностей, важным становится выбор алгоритма ее решения, учитывающего их. Учитывая особенности задачи, алгоритм поиска кратчайшего пути должен иметь определенные свойства. Сравнение алгоритмов для решения задач с такими особенностями выполнено в работе Р.А. Черных [64]. Основываясь на результатах данного сравнения, для решения задачи был выбран алгоритм Дейкстры [65].

Решаемая задача удовлетворяет ограничениям применимости алгоритма Дейкстры — в графе отсутствуют ребра с отрицательным весом.

Алгоритм Дейкстры основан на следующем тезисе: если кратчайший путь проходит через вершину r_{ij}, то длина части пути от r_0 до r_{ij} должна быть минимально возможной.

Контекстная IDEF0-диаграмма процесса формирования частной методики, эффективной по заданному ресурсному критерию, представлена на рис. 2.5. Входными данными является решение о составе и последовательности методов методики, полученное выше (см. рис. 2.2). Так как здесь не предусмотрена разработка ПО для автоматизации рассматриваемого процесса, то этот процесс выполняется экспертом вручную, но после автоматизации основным механизмом также будет ПО определения методики. По итогам данной процедуры принимается решение о составе и последовательности методов частной методики.

Такой подход определения последовательности методов производства компьютерно-технической экспертизы, основанный на теории графов, весьма прагматичен. По существу это классификация и выбор методики производства КТЭ исходя из предмета

экспертизы и последующее формирование частной методики, эффективной по заданному ресурсному критерию. Формирование частной методики решается как типовая задача теории графов — задача о поиске кратчайшего пути по алгоритму Дейкстры.

Возможна ситуация, когда будет определяться несколько вершин, которые можно отнести к текущей. Это говорит о существовании нескольких методов производства КТЭ, подходящих с точки зрения оценки их по выбранному критерию. В этом случае можно выбрать любой из них или дополнить анализ методов с позиции поиска кратчайшего пути по другим критериям.

2.4. Оценка трудозатрат при производстве комплексной экспертизы

Одной из задач, решаемых при назначении экспертизы, является определение трудозатрат. От правильности решения данной задачи зависит не только планирование производственного графика проведения экспертиз в экспертном учреждении, но и определение стоимости производства экспертизы, определение возможности производства экспертизы в установленные процессуальными нормами сроки, а следовательно, и деловая репутация экспертного учреждения.

Как правило, оценка трудозатрат не вызывает сложностей при производстве КТЭ одним экспертом. В случае, когда КТЭ выполняется в составе комплексной экспертизы, где исследования экспертов разных специальностей проводятся не параллельно, а зависят друг от друга, задача значительно усложняется и увеличивается вероятность допущения ошибок в оценке.

Для решения задачи оценки трудозатрат при производстве КТЭ в составе комплексной экспертизы можно предложить использование методологии PERT (Project Evaluation and Review Technique) [67–69].

Для наглядности представим оценку трудозатрат с помощью метода критического пути [70, 71], опирающегося на построение сетевой диаграммы PERT. Нужно учитывать, что в зависимости от объектов, задач и вопросов комплексной экспертизы вид сетевой диаграммы изменяется. На рис. 2.6 представлена сетевая диаграмма оценки трудозатрат для частного случая — производства комплексной экспертизы, вопросами которой являются:

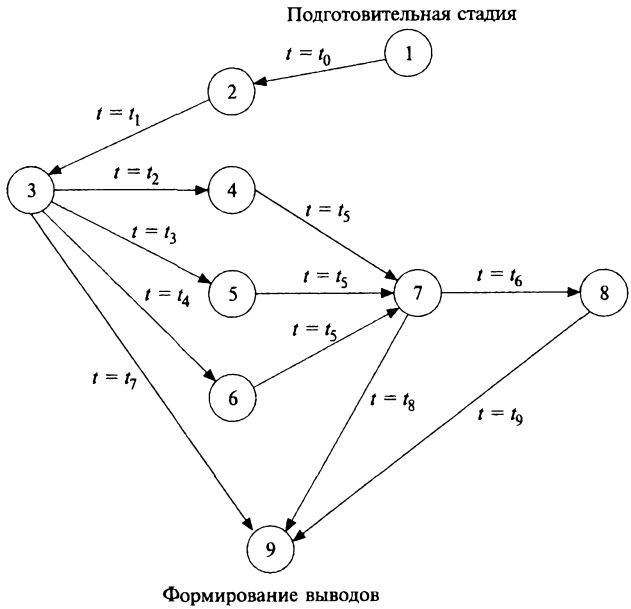


Рис. 2.6. Частный случай сетевой диаграммы PERT (производство комплексной экспертизы)

- установление наличия в сети интернет по адресу x в открытом доступе сайта *xxx;*
- в случае положительного ответа на первый вопрос, установление наличия на сайте фото- или видеоматериалов, имеющих признаки порнографии;
- в случае положительного ответа на второй вопрос установление размещения сайта (географического расположения).

На сетевой диаграмме приняты следующие обозначения:

- подписка об уголовной ответственности (подготовительная стадия);
- результаты подготовительной стадии: t_0 — время проведения подготовительной стадии всеми экспертами комплексной экспертизы;
- предварительные выводы по первому вопросу: t_1 — время проведение исследования экспертом КТЭ по первому вопросу экспертизы;
- предварительные выводы по второму вопросу эксперта видео-, фототехнической экспертизы: t_2 — время проведения

исследования по второму вопросу экспертом видео-, фототехнической экспертизы;

- предварительные выводы по второму вопросу эксперта искусствоведческой экспертизы: t_3 — время проведения исследования по второму вопросу экспертом искусствоведческой экспертизы;
- предварительные выводы по второму вопросу эксперта-психолога: t_4 — время проведения исследования по второму вопросу экспертом-психологом;
- общие выводы по второму вопросу: t_5 — время формирования общих выводов по второму вопросу;
- предварительные выводы по третьему вопросу: t_6 — время проведение исследования экспертом КТЭ по третьему вопросу экспертизы;
- вывод: t_7 — время формирования общих выводов по экспертизе; t_8 — время формирования общих выводов по экспертизе; t_9— время формирования общих выводов по экспертизе.

2.5. Резюме

Таким образом, процесс классификации по основным критериям представлен в виде ориентированного графа с описанием множеств его вершин и ребер. Критерии классификации разделены на три уровня, определяющих свойства методик КТЭ. Были определены 12 обобщенных типовых методик производства КТЭ.

В соответствии с разработанной классификацией методик КТЭ и на основании методических документов [2, 3, 10, 14, 16, 23–51] представлен полный перечень возможных основных вопросов КТЭ.

Модель методики производства КТЭ построена на алгоритмическом применении методов КТЭ множества S, представляющего собой подмножество декартового произведения множеств методов для всех стадий экспертного исследования. Она применима для разработки общих, частных и конкретных методик, относящихся к любому типу методик КТЭ, в том числе и по предложенной классификации методик.

Описан общий алгоритм производства КТЭ — последовательность стадий производства экспертизы.

Решена задача выбора методов производства КТЭ, эффективных по заданному критерию (финансовые, временные, человеческие ресурсы или иные) как задача о поиске кратчайшего пути на графе.

Для решения задачи оценки трудозатрат при производстве КТЭ в составе комплексной экспертизы предлагается использовать методологии PERT.

3 УНИФИЦИРОВАННАЯ МЕТОДИКА ПРОИЗВОДСТВА КОМПЬЮТЕРНО-ТЕХНИЧЕСКИХ ЭКСПЕРТИЗ

Обратимся теперь к методическому и алгоритмическому обеспечению производства КТЭ.

Методика производства КТЭ оказывается весьма унифицированной, так как применима для решения широкого круга частных задач, среди которых есть и диагностические, и классификационные, и идентификационные задачи. Таким образом согласно классификации обобщенная методика включает в себя следующие типы методик производства КТЭ, направленных на решение:

- диагностических задач с целью ответа на вопросы, относящиеся к программным средствам;
- диагностических задач с целью ответа на вопросы, относящиеся к данным (компьютерной информации);
- диагностических задач с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам;
- классификационных задач с целью ответа на вопросы, относящиеся к программным средствам;
- классификационных задач с целью ответа на вопросы, относящиеся к данным (компьютерной информации);
- классификационных задач с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам;
- идентификационных задач с целью ответа на вопросы, относящиеся к аппаратным средствам;
- идентификационных задач с целью ответа на вопросы, относящиеся к программным средствам;
- идентификационных задач с целью ответа на вопросы, относящиеся к данным (компьютерной информации);
- идентификационных задач с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам.

Разработанная методика является унифицированной и пригодной для ответа на любые вопросы КТЭ в случае ее использования в качестве общей методики производства КТЭ.

В случае использования разработанной методики в качестве частной она является унифицированной, но имеющей ряд ограничений, связанных с описанием в методике определенных частных методов, применимых для определенного круга объектов. Основное ограничение связано с применимостью методов методики для определенных ОС (Windows).

Разработанное методическое обеспечение производства КТЭ ориентировано на экспертов КТЭ частных и государственных экспертных учреждений. Оно содержит: рекомендации по выполнению стадий производства КТЭ и применению частных инструментальных методов; требования по оформлению экспертного заключения; описание структуры заключения эксперта о результатах производства КТЭ.

Методическое обеспечение предполагает использование пошаговых алгоритмов стадий производства КТЭ, разработанных на основе анализа графовых моделей производства КТЭ. Они представлены в виде IDEF0-диаграмм для каждой стадии производства КТЭ:

- подготовительной стадии;
- аналитической стадии;
- эксперимента;
- синтезирующей стадии;
- результирующая стадии;
- стадии формирования выводов.

Предложенный подход создания пошаговых алгоритмов позволяет формализовать производство КТЭ и планировать ресурсы, необходимые для каждой из ее стадий.

3.1. Подготовительная стадия

Основной целью подготовительной стадии является уяснение экспертом экспертной задачи [10].

В ходе подготовительной стадии экспертом КТЭ выполняются следующие действия [4–7]:

1. Дается подписка о предупреждении об уголовной ответственности за дачу заведомо ложного заключения по ст. 307 Уголовного кодекса Российской Федерации (УК РФ) [46] или об административной ответственности по ст. 17.9 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) [47], а в необходимых случаях по ст. 310 УК РФ — за разглашение данных предварительного расследования.

2. Изучается постановление/определение, рассматриваются поставленные вопросы.

3. Осуществляется изучение материалов дела.

4. Выполняется осмотр и описание объектов, предоставленных на экспертизу. При осмотре эксперт изучает общие признаки исследуемых объектов. Осмотр рекомендуется сопровождать фотосъемкой объектов при их поступлении в экспертное учреждение — в упаковке и без упаковки, с целью фиксации внешних признаков исследуемых объектов.

5. После внешнего осмотра объектов осуществляется предварительный анализ информационного содержимого объектов с целью определения пригодности и достаточности объектов для ответа на вопросы экспертизы и определении методов исследования. Для этого объекты подключаются к тестовому компьютеру эксперта.

Перед подключением носителей информации к тестовому компьютеру должна быть обеспечена неизменность и сохранность информации. Так, при подключении исследуемых НЖМД к тестовому компьютеру для предотвращения утечки важной информации с подключаемого НЖМД должно быть осуществлено блокирование возможности сохранения данных на носителях, подключаемых к портам USB тестового компьютера. Блокирование возможности сохранения данных рекомендуется осуществлять аппаратными блокираторами, допускается блокирование возможности сохранения данных программными средствами (средствами экспертной ОС, специализированным ПО).

Для установления пригодности носителей информации для дальнейшего проведения исследования рекомендуется использование специализированного ПО. С этой целью для НЖМД возможно проведение тестирования на наличие сбойных кластеров (участков на поверхности диска, имеющих механическое либо

другое повреждение), например, с использованием программы HDDScan.

Программа автоматически тестирует все сектора диска и проверяет скорость считывания данных. Если отклик составляет <5 мс, то сектор считается абсолютно рабочим. Сектора с откликами <20 мс, <50 мс, <150 мс считаются рабочими, но для доступа к ним требуется соответствующее время. Сектора с откликом <500 мс — очень плохие сектора. Пометкой «B» отмечаются сбойные сектора, доступ к которым невозможен.

6. Составляется рабочий план проведения исследования. Для этого проводится:

- пересмотр нормативных документов и законодательных актов (если требуется);
- определение возможности проведения экспертизы на основании:
- постановка цели, определении конечного результата проведения исследования;
- определение методов исследования;
- анализ применимости технической базы (программного обеспечения, оборудования) экспертного учреждения для решения конкретных поставленных задач;
- определение соответствия квалификации эксперта по сложности вопросов, решаемых в рамках конкретной экспертизы;
- анализ наличия среди ранее проведенных экспертиз аналогичных. В случае наличия — использование плана ранее проведенных экспертиз в качестве шаблона. При отсутствии — составление индивидуального плана проведения экспертизы;
- при необходимости использования на каком-либо из этапов разрушающих или частично разрушающих методов исследования — подача соответствующего ходатайства лицу, назначавшему экспертизу;
- в случае отклонения ходатайства — пересмотр методов проведения экспертизы. При невозможности проведения экспертизы без использования разрушающих или частично разрушающих методов — информирование заказчика о невозможности проведения исследования.

7. На тестовом компьютере эксперта осуществляется подготовка *рабочих зон*. Под рабочими зонами будем понимать дирек-

тории на тестовом компьютере эксперта, содержащие всю исследуемую информацию и информацию, имеющую доказательное значение в рамках дела. Подготовка рабочих зон осуществляется следующим образом:

- выполняется клонирование/копирование данных с предоставленных на экспертизу носителей информации на рабочую станцию эксперта (тестовый компьютер). При проведении анализа данных, содержащихся непосредственно на самом носителе без их предварительного копирования на рабочую станцию эксперта, данный этап отсутствует;
- на рабочей станции эксперта создается директория, в которой будут размещены файлы, содержащие информацию, необходимую для ответа на поставленные вопросы;
- на рабочей станции эксперта создается директория, в которой размещается информация, полученная с объектов, предоставленных на экспертизу, необходимая для проведения экспертизы, но в своем полном объеме не являющаяся доказательствами по делу. Таким образом, в данной директории могут быть размещены: полные образы носителей информации, все log-файлы, reg-файлы, история интернет-активности, index-файлы и т. д.

Такая организация рабочих зон весьма удобна при работе с большим числом информации, но не является обязательной.

При выборе экспертом между исследованием клонов/копий/образов и исследованием информации непосредственно на носителе, нужно руководствоваться тем, что в соответствии со стандартами криминалистики эксперты проводят исследование или анализ копий цифровых объектов — так исключается изменение или нарушение целостности данных оригинала.

Исследование непосредственно самого носителя возможно в случае, если такой вид исследования физически не может внести изменения в информацию (например, из-за особенностей носителя — DVD-R) или невозможно получение копии, пригодной для проведения исследования (в этом случае необходимо разрешение лица, назначавшего экспертизу, на применение частично разрушающих методов).

Копия исходных цифровых данных для исследования обычно называется *образом* [72]. Для того чтобы этот образ являл-

ся юридическим эквивалентом оригинала, он должен представлять собой абсолютную копию исходных данных. Следовательно, каждый бит оригинала должны быть скопирован на образ. Существуют различные методы клонирования носителей информации. Выбор того или иного метода обуславливается конкретной ситуацией. Описание некоторых методов приведено ниже.

Клонирование с диска на диск [73]. Этот способ клонирования (drive-to-drive) происходит полностью в ОС, а исследуемый накопитель и накопитель для сохранения образа подключены к одной и той же системной плате. Достоинством этого метода является его простота — требуется только загрузочный диск (например, Acronis или EnCase) и накопитель для сохранения образа. Многие эксперты, которые начали заниматься компьютерно-технической экспертизой много лет назад, когда этот метод клонирования считался стандартным, до сих пор предпочитают пользоваться им.

Клонирование с диска на диск — относительно быстрый способ дублирования данных. Ограничение скорости обычно связано с медленными компонентами в подсистеме ATA, будь то контроллер, кабель, конфигурация или скорость диска. Более быстрой конфигурацией обычно является «главный-главный» (master-to-master) на разных каналах (первичный и вторичный), более медленной — «главный-подчинённый» (master-to-slave) на одном и том же канале. Если вы берёте свой кабель для накопителя, на котором будет храниться образ, убедитесь, что это 80-проводной кабель IDE, чем короче, тем лучше. Максимальная длина для таких кабелей — 18 дюймов, чем длиннее кабель, тем больше вероятность ошибки передачи данных при клонировании.

Клонирование данных по сети [73]. Это еще один способ клонирования, который содержит в себе преимущества загрузки в ОС. Применение данного метода может помочь в следующих ситуациях.

Клонирование невидимых данных в области HPA или DCO. Столкнувшись с HPA или DCO, можно поместить этот накопитель в безопасный лабораторный компьютер и загрузить EnCase для DOS, при этом подключиться к своему рабочему компьютеру и запустить EnCase в среде Windows. Так же клонирование по сети пригодится для загрузки с исследуемого компью-

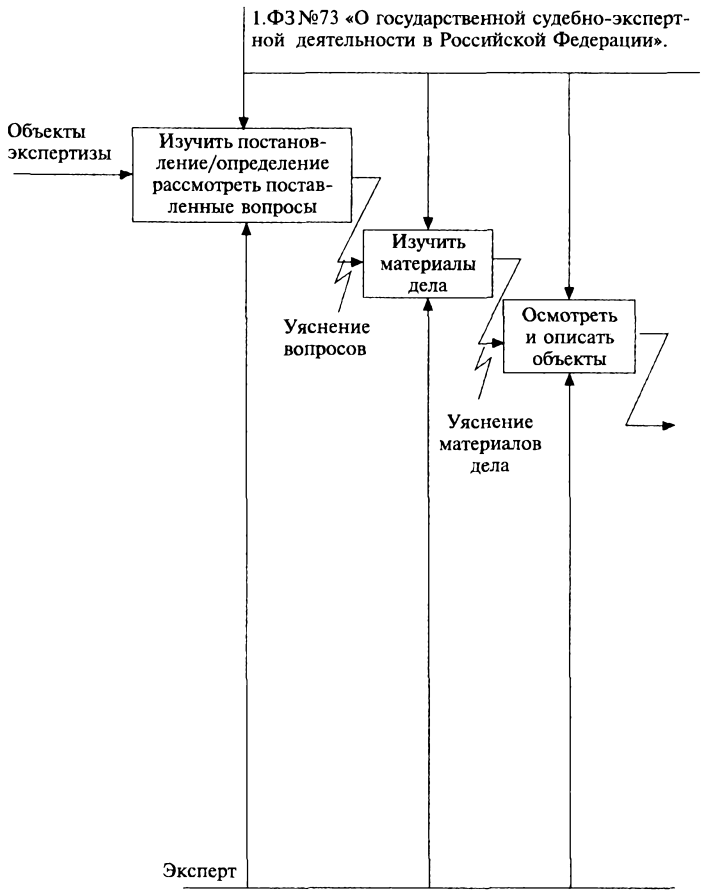
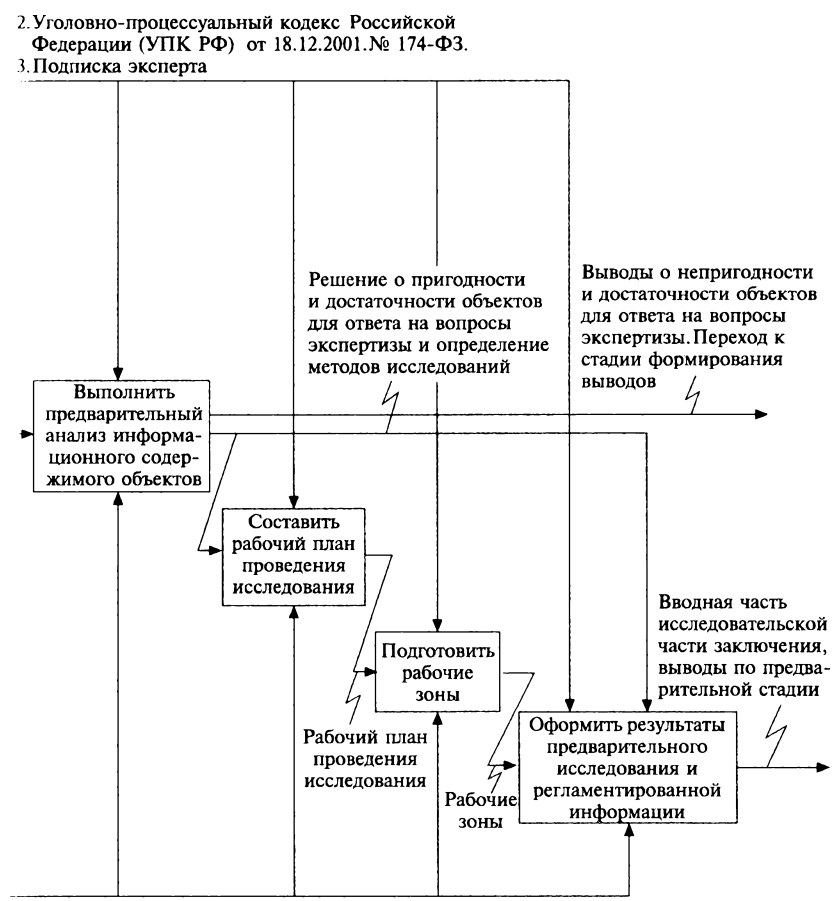


Рис. 3.1. IDEF0-диаграмма производства

тера, когда не совпадает версия унаследованной BIOS (обычно на исследуемом компьютера) и новой BIOS (обычно на компьютере эксперта) или при работе с конфигурациями RAID. Применяя загрузку в DOS, можно использовать конфигурацию аппаратного RAID для монтирования его как физического накопителя/устройства. EnCase распознаёт этот RAID-массив как монтированный физический накопитель и позволяет выполнить его клонирование и предварительный просмотр (просмотреть логическую структуру) посредством подключения к EnCase в Windows через сетевой кабель.

Дублирование данных с НЖМД лэптопа. Иногда извле-



подготовительной стадии КТЭ

чение жёсткого диска из лэптопа является сложной задачей из-за физического доступа или других проблем, таких как патентованная защищённая схема, с помощью которой накопитель подключён к системной плате. Если вы можете получить доступ к BIOS и контролировать процесс загрузки, то клонирование по сети — очень удобная опция при значительной степени внимания и осторожности.

Быстрое клонирование данных. Способ клонирования по сети очень удобен для скрытых операций, когда необходимо быстро создать образ целевого накопителя, пока его владелец отсутствует.

8. Результаты предварительного исследования и регламентированная информация об эксперте, экспертном учреждении, экспертизе отражаются в вводной и частично исследовательской частях заключения.

На подготовительной стадии в вводной части заключения указывается [4–7]:

- место и время производства экспертизы;
- основания производства;
- информация об экспертном учреждении, эксперте;
- отметка о предупреждении эксперта об уголовной ответственности;
- вопросы, поставленные на экспертизу;
- отметка о редакции вопроса (в случае редакции формулировки вопроса экспертом);
- информация об объектах, поступивших на исследование;
- предоставленные материалы дела, относящиеся к вопросам экспертизы;
- лица, присутствовавшие при производстве экспертизы (может быть указано/дополнено на последующих стадиях экспертизы);
- информация о заявленных ходатайствах, результаты их разрешения (может быть указано/дополнено на последующих стадиях экспертизы);
- отметка о производстве повторной или дополнительной экспертизы;
- использованная литература (может быть указано/дополнено на последующих стадиях экспертизы).

На подготовительной стадии в исследовательской части заключения указывается [4–7]:

- информация о результатах внешнего осмотра объектов;
- информация о результатах исследования информационного пространства носителей информации и их пригодности для проведения исследования;
- информация о выбранных методах исследования носителей информации.

На рис. 3.1 представлена IDEF0-диаграмма производства подготовительной стадии КТЭ.

3.2. Аналитическая стадия

На этой стадии выполняется тщательное исследование объектов. Исследование выполняется с использование аппаратно-программных средств — экспертного инструментария.

Аналитическая стадия состоит из двух этапов исследования: предварительного, направленного на получение общей информации об исследуемых объектах, и основного, на котором происходит детальный анализ с целью получения информации, имеющей значение для ответа на вопросы постановления/определения.

В рамках *предварительного этапа* исследования обобщается информация об объеме данных, их структуре, настройках, проводится экспресс-анализ данных, файлов, формируется представление об их виде. Так, для НЖМД на предварительном этапе будут выполнены следующие действия (для прочих объектов исследование выполняется по аналогии).

1. Подсчет хеш-сумм [74] (MD5, SHA) образца и копии.

2. Проверка физического размера диска и сравнение его с размером всех областей дискового пространства (в том числе DCA/HPA) [75].

3. Определение и сравнение размеров логических разделов с размером диска для определения информации об удаленных разделах или о неиспользуемом дисковом пространстве.

4. Получение информации о настройках временных зон для каждого диска и применение правильной зоны, если это возможно.

5. Переименование разделов НЖМД так, как это необходимо («C», «D» и т. д.).

6. Сбор системной информации:

- определение типа ОС, SP [76], даты установки ОС; перечня установленных и запускаемых приложений; имени пользователя и имени компьютера и т. п.;
- получение информации о профиле пользователя (имя, SID [77], дата создания и последнего входа в систему).

7. Экспресс-анализ данных:

- анализ сигнатуры файлов, просмотр переименованных файлов;
- определение зашифрованных файлов;

- определение и монтирование файлов-образов, контейнеров, архивов — VHD, VMDK, ZIP, RAR, Email-контейнеры, Reg-файлы и т. д.

8. Проведение анализа включенных работающих сервисов.

9. Проведение сканирования:

- поиск и анализ вирусов;
- поиск и анализ артефактов программ для стеганографии.

10. Поиск по ключевым словам:

- составление списка ключевых слов;
- формирование поискового запроса с использованием синтаксиса выбранного поискового инструментария;
- проведение целевого поиска (в определенных директориях) всего пространства (включая нераспределенные области и удаленные разделы);
- составление отчета по результатам поиска;
- фильтрация данных (на основании метаданных — дата, время, расширение и т. д.).

В рамках *основного этапа* исследования выполняются следующие действия.

1. Анализ данных. Анализ файлов с использованием специализированного ПО, в качестве которого может быть использован следующий экспертный инструментарий:

- анализ памяти [78–80];
- работа с паролями [81–84];
- ключи Shellbags реестра [85];
- Интернет-активность [86];
- LNK-файлы [87];
- Event Logs-файлы (файлы формата .evt и .evtx) [88, 89];
- анализ MFT [90, 91];
- анализ файлов Index.dat: *Index.dat Analyzer* — ПО, предназначенное для поиска и анализа файлов Index.dat;
- анализ e-mail сообщений [92, 93];
- монтирование файлов-образов: ПО для монтирования файлов-образов определяется типом файла-образа (расширением). Так, в зависимости от типа файла могут быть использованы следующие программы: FTK Imager, ImDisk Live, View OSFMount, Virtual Box, Acronis и т. д.;
- анализ артефактов программ стеганографии [94, 95];

- подсчет хеш-сумм [96];
- работа с реестром ОС: *Registry Recon* [97]. *Windows Registry Recovery* — программа, предназначенная для анализа и редактирования реестра. Имеется возможность работы с реестром активной и пассивной ОС;
- восстановление данных [98–100];
- выявление ПО с признаками контрафактности. *Defacto* — ПО, предназначенное для определения признаков использования ПО с нарушением исключительных прав: скомпрометированный серийный номер, наличие следов взлома технических средств защиты авторских прав (ТСЗАП) и т. д.

2. Анализ основных областей. Анализ основных областей выполняется для поиска артефактов и/или другой интересующей информации. Примером основных областей являются:

- рабочий стол;
- директория пользователя;
- директория «Документы»;
- директория «Загрузки»;
- директория «Недавние места»;
- временные директории браузеров;
- директория System32.

3. Анализ системного реестра. Анализ системного реестра может помочь в получении многочисленной важной информации как о самой системе и о приложениях, так и об активности пользователя. Например:

- версия ОС (ветка SOFTWARE);
- информация о последнем входе в систему (ветка SAM);
- имя пользователя и SID (ветка SAM);
- время последнего завершения работы (ветка SYSTEM);
- временная зона (ветка SYSTEM);
- носители, подключаемые пользователем (ветка SYSTEM);
- установленное программное обеспечение (ветка SOFTWARE).

4. Анализ артефактов ОС. В ОС имеется ряд артефактов, которые могут содержать важную информацию для ответа на вопросы экспертизы. К таким артефактам, например, относятся:

- резервные копии;
- файлы Event Logs (.evt, .evtx);

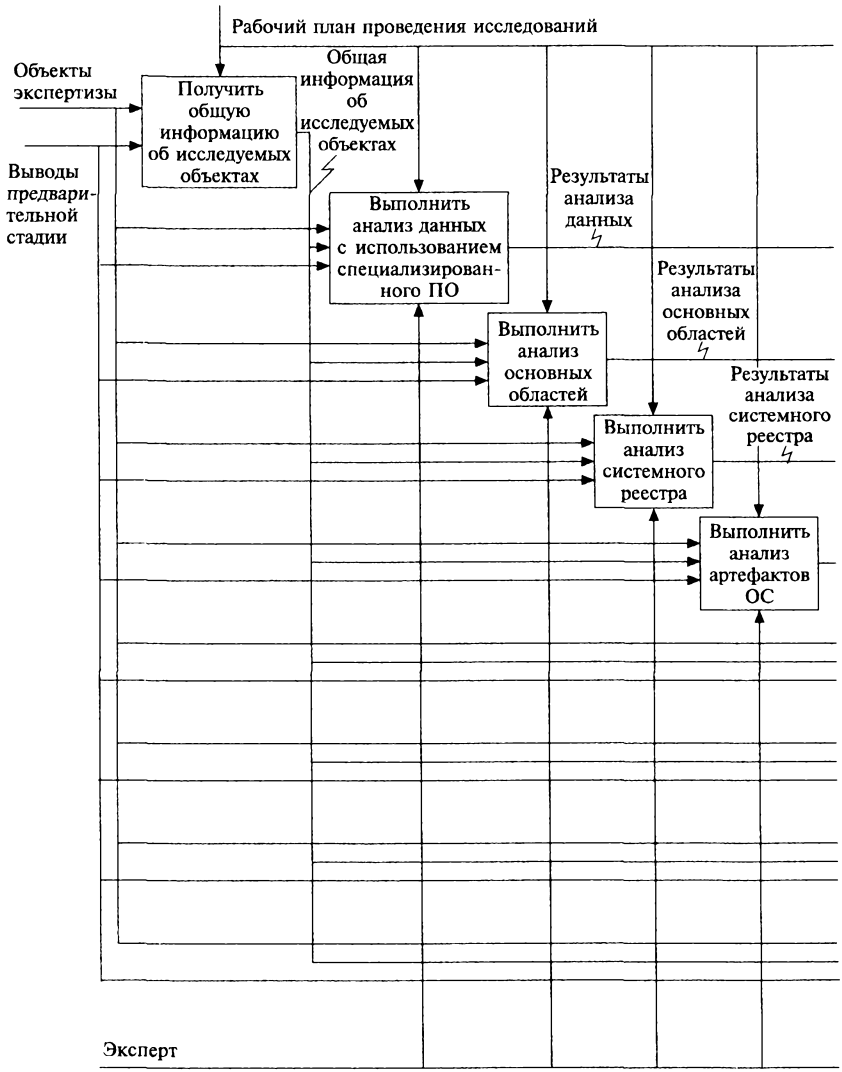
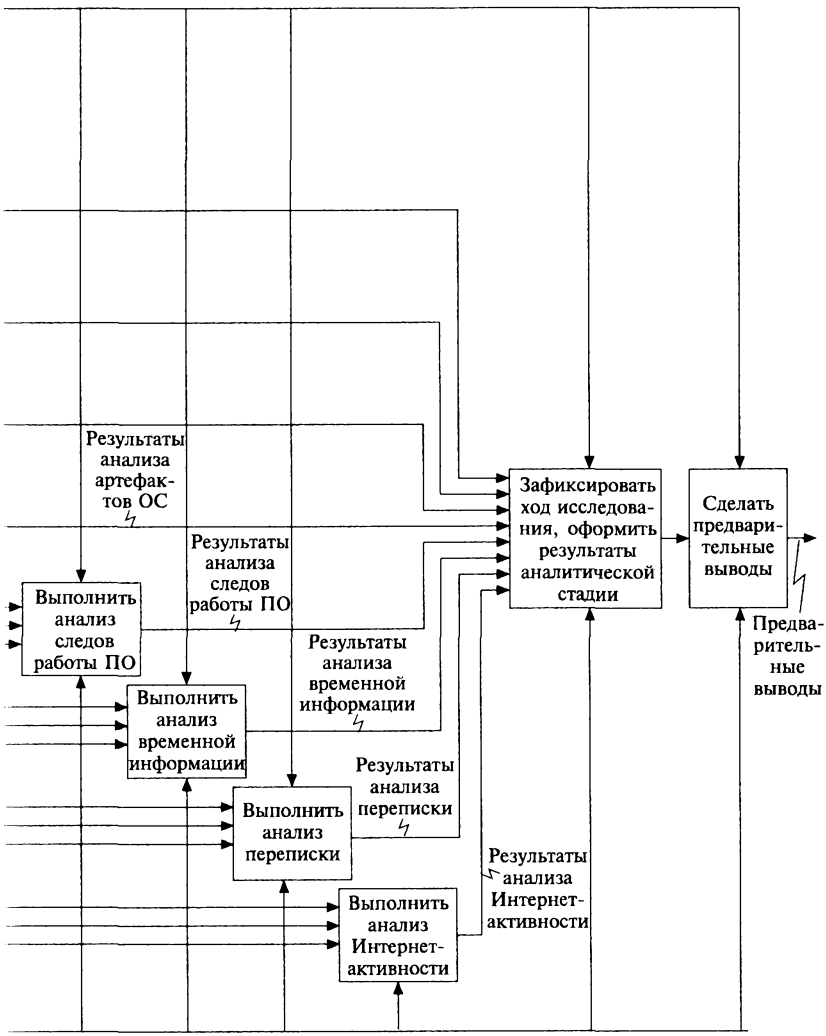


Рис. 3.2. IDEF0-диаграмма производства

- Shell bags;
- Jump Lists;
- LNK-файлы;
- Prefetch;
- PageFile.

5. Анализ следов работы программного обеспечения. Определение наличия программного обеспечения (например, Wiping



аналитической стадии КТЭ

tools, P2P, Sticky Notes, программное обеспечение для взлома и т. д.), анализ журналов (логов), настроек, реестра и т. д.

6. Если есть возможность, то необходимо провести анализ временной информации, содержащейся в памяти.

7. Анализ переписки (e-mail, соц. сети). Для анализа информации о переписке пользователя необходимо выполнить:

- поиск установленных почтовых клиентов, архивов сообщений почтовых клиентов. Для анализа информации, содержащейся в них, используется либо почтовый клиент, либо специализированное программное обеспечение, предназначенное для просмотра файлов соответствующего типа;
- поиск установленных программ обмена мгновенными сообщениями (QIP, ICQ и т. д.), архивов сообщений;
- для анализа информации о переписке в социальных сетях (ВК, Facebook, Twitter и т. д.) производится анализ интернет-активности пользователя.

8. Анализ интернет-активности. Для анализа интернет-активности пользователя необходимо определить установленные браузеры и провести для них анализ артефактов, таких как:

- файлы истории посещения (index.dat, sqlite и т. д.);
- временные директории;
- куки (cookies);
- кеш страниц;
- избранное, закладки;
- панели инструментов;
- WebSlices;
- плагины;
- системный реестр;
- удаленная информация.

Безусловно, указанный перечень не является исчерпывающим и может быть расширен при требуемой заказчиком КТЭ детализации исследования.

Ход проведение исследования, а также используемые методы фиксируются. В завершении стадии экспертом даются предварительные выводы. Сделанные на аналитической стадии выводы уточняются на последующих стадиях исследования.

На рис. 3.2 представлена IDEF0-диаграмма производства аналитической стадии КТЭ.

Информация об уязвимости процессов переработки информации в информационных системах (важная при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности) формируется именно на аналитической ста-

дии. В соответствии с правилами производства экспертизы эксперты КТЭ в своем заключении отвечают на вопросы экспертизы и не дают рекомендаций по совершенствованию существующих средств защиты информации и обеспечения информационной безопасности. Если же сами рекомендации по совершенствованию существующих средств защиты информации и обеспечения информационной безопасности являются вопросом экспертизы, то данные рекомендации даются в результате ее обобщения на синтезирующей стадии.

Информация, полученная на аналитической стадии, излагается в тексте заключения КТЭ и может быть использована специалистами по информационной безопасности для совершенствования существующих подходов, средств защиты информации для обеспечения информационной безопасности.

3.3. Эксперимент

Наличие стадии эксперимента зависит от каждой конкретной ситуации, его форма базируется на задачах и целях экспертного исследования. Место и состав эксперимента определяются экспертом. Эксперимент может быть проведен как в экспертном учреждении, так и вне его. Эксперимент включает в себя следующие этапы:

- планирование эксперимента;
- подготовка эксперимента;
- проведение эксперимента;
- подведение итогов эксперимента.

Эксперимент проводится экспертом в целях выявления механизма взаимодействия объектов экспертного исследования и (или) механизма следообразования его отдельных параметров. В ходе эксперимента эксперт изучает интересующие его процессы и условия.

В исследовательской части заключения эксперт должен подробно описать условия проведения эксперимента и его результаты. Результаты эксперимента оформляются в виде предварительных выводов по данной стадии.

На рис. 3.3 представлена IDEF0-диаграмма производства стадии эксперимента.

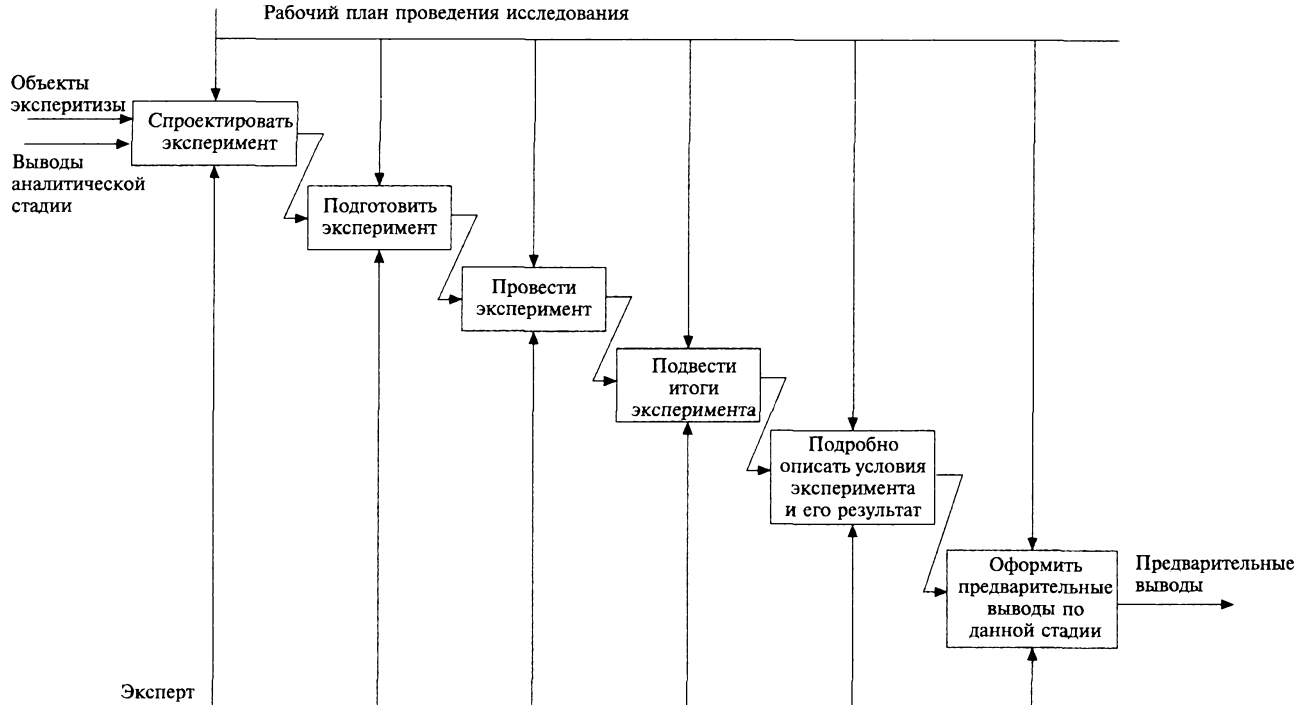


Рис. 3.3. IDEF0-диаграмма производства стадии эксперимента КТЭ

3.4. Синтезирующая стадия

Данная часть исследования представляет собой обобщение информации, полученной на предыдущих стадиях экспертизы, интерпретацию артефактов. В зависимости от *конкретных* задач, решение которых необходимо для ответа на поставленные вопросы, рассматриваются определенные артефакты. Ниже приведен перечень основных *частных* задач (диагностических, идентификационных, классификационных) и артефактов, рассматриваемых для их решения в ОС семейства Windows на примере Win7. Для прочих ОС семейства Windows артефакты будут отличаться их расположением (адресом директорий и названием файлом), а для некоторых задач и составом. Подробная информация о составе и расположении артефактов содержится на официальном сайте компании-разработчика ОС.

Задача определения информации о загрузке файла. Артефакты:

- *Open/Save MRU* — этот ключ фиксирует информацию об открытых или сохраненных файлах для многих приложений. Расположение (в случае стандартной конфигурации): **Win7** NTUSER.DAT\Software\Microsoft\ Windows\CurrentVersion\ Explorer\ComDlg32\OpenSavePIDlMRU;
- *Email* — почтовые сообщения Outlook. Расположение: **Win7** %userprofile%\AppData\Local\Microsoft\Outlook;
- *история Skype* — история активности Skype содержит историю сессий чата и пересылки файлов. Сохраняется она по умолчанию в папке установки. Расположение: **Win7** C: \Users\AppData\Roaming\Skype;
- *Index.dat/places.sqlite* — данные файлы содержат информацию об активности пользователя: о посещенных им сайтах, об открываемых файлах, о файлах, к которым было обращение;
- *downloads.sqlite* — это артефакт браузера Firefox, содержащий историю о загрузках файлов и посещенных сайтах. Расположение: **Win7** %userprofile%\AppData\Roaming\Mozilla\ Firefox\Profiles\.default\downloads.sqlite.

Задача определения информации об открытии/создании файла. Артефакты:

- *Open/Save MRU* (см. описание выше);

- *Last Visited MRU* — ключ реестра OpenSaveMRU, содержащий информацию об открытии файлов определенными приложениями. С его помощью можно определить информацию о том, какой файл был открыт приложением последним. Расположение: **Win7** NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\ComDlg32\LastVisitedPidlMRU;
- *последние документы* — информация о последних открытых файлах и папках, отображаемая в меню *Пуск*, содержится в ключе системного реестра RecentDocs. Расположение: NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs;
- *MS Office MRU* — в системном реестре содержится информация о последних документах, открытых с использованием приложений Microsoft Office. Располагается в ключе NTUSER.DAT\Software\Microsoft\Office\version, где 14.0 для Office 2010; 12.0 для Office 2007; 11.0 для Office 2003; 10.0 для Office XP;
- *LNK-файлы* — файлы-ярлыки. Эти файлы генерируются в ОС для последних открытых файлов. Расположение (могут быть обнаружены и в других директориях):
  Win7: C:\Users\AppData\Roaming\Microsoft\ Windows\Recent\;
  Win7 C:\Users\AppData\Roaming\Microsoft\ Office\Recent\;
- *Index.dat* (см. описание выше);
- *JumpLists* — информация о задачах, файлах отображаемая в панели задач Windows 7 (Jump List), расположенная по адресу C:\Users\\AppData\Roaming\ Microsoft\Windows\Recent\AutomaticDestinations;
- *Shellbags* — ключи реестра, содержащие информацию о директориях. Информация в данных ключах сохраняется даже после удаления директории или отключения подключенного носителя. Расположение:
  Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\Bags
  Win7 USRCLASS.DAT\Local Settings\Software\Microsoft\Windows\Shell\BagMRU

Win7 NTUSER.DAT\Software\Microsoft\Windows\Shell\Bag MRU

Win7 NTUSER.DAT\Software\Microsoft \ Windows \ Shell \ Bags;

- *Prefetch*-файлы (.pf) могут быть использованы для определения информации о последних используемых файлах и устройствах, они располагаются в директории C:\Windows\ Prefetch.

Задача определения информации о файлах (задача поиска файлов), в том числе удаленных. Артефакты:

- **Win7** *Search WordWheelQuery* — артефакт, содержащий информацию о поисковых запросах, вводимых в меню *Пуск* в ОС Windows 7. Расположение: **Win7** NTUSER.DAT Hive NTUSER.DAT \ Software \ Microsoft \Windows\CurrentVersion \Explorer\WordWheelQuery;
- *Thumbs.db* — артефакт, являющийся скрытым файлом. Содержит информацию об изображениях, имеющихся и имевшихся в директории, т. е. даже после их удаления из нее. Артефакт располагается в любой директории, где были просмотрены изображения в режиме эскизов, многие камеры создают этот файл автоматически;
- **Win7** *Thumbnails* — в ОС Vista/Win7 файлы thumbs.db отсутствуют, информация сохраняется отдельно для каждого пользователя, в директории : \Users\\AppData\Local\Microsoft\Windows\Explorer;
- *корзина* — Анализ корзины важен, так как зачастую значимые удаленные файлы были удалены именно через эту директорию. Расположение:
- **Win7**: Системная директория корзины C:\$Recycle.bin;
- *артефакты браузеров* — эта группа артефактов будет рассмотрена ниже при описании артефактов задачи определения интернет-активности пользователя;
- *Last visited MRU* — см. описание выше.

Задача определения использования/подключения USB-устройств. Артефакты:

- системный реестр: NTUSER.DAT ветка: NTUSER // Software / Microsoft / Windows / CurrentVersion / Explorer/Mount Points2/;

- *ключи реестра* — ключи системного реестра, содержащие информацию о ранее подключаемых USB-устройствах. Расположены по адресу SYSTEM \ CurrentControlSet \ Enum \ USBSTOR и SYSTEM\CurrentControlSet\Enum\USB;
- *First/Last Time* (недавно и давно подключаемые) — артефакты, содержащие информацию о подключении конкретных USB-устройств, их серийного номера, даты подключения. Расположение: *журнал Plug and Play* (недавно подключаемые): **Win7** C:\Windows\inf\setupapi.dev.log;
- *идентификация пользователя* — если стоит задача определения пользователя, которым было подключено USB-устройство, то необходимо проанализировать:
  - GUID пользователей в ключе реестра SYSTEM\Mounted Devices;
  - ключ реестра NTUSER.DAT \ Software \ Microsoft\Windows\CurrentVersion\Explorer\MountPoints2;
- *имя раздела* — информация об имени, присвоенном носителю при подключении, может быть определена при анализе артефактов системного реестра, расположенных в нем по адресу: **Win7**: SOFTWARE\Microsoft\Windows Portable Devices\Devices и SYSTEM\MountedDevices;
- *LNK Files* — см. описание выше;
- *Event Logs* — информация об установке Plug and Play драйверов логируется (журналируется) в системном журнале Windows. Важно отметить, что сохраняется информация о подключении не только для USB-устройств.

Задача определения информации о запуске программ. Артефакты:

- *User Assist* — артефакт запуска графических приложений, содержащийся в системном реестре по адресу: NTUSER.DAT\Software\Microsoft\Windows\Currentversion\Explorer\UserAssist\{GUID}\Count;
- *LastVisited MRU* — см. описание выше;
- *Run MRU (Start->Run)* — артефакт, образующийся в результате запуска кем-либо команд *открыть, запустить*. Он расположен в системном реестре по адресу NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RunMRU;

- *Prefetch* — см. описание выше;
- *Jump Lists* — см. описание выше;
- *Event Logs* — артефакты о запуске программ, содержащиеся в системном журнале Windows.

Задача определения физического нахождения (локализации) пользователя. Артефакты:

- *Time Zone* (временная зона) — артефакт, расположенный в системном реестре, и содержащий информацию о временной зоне. Расположение: SYSTEM\CurrentControlSet\Control\TimeZoneInformation;
- *Vista/W7 Network History* — артефакт, содержащий информацию о сетевых подключениях компьютера, типе сети (проводная, беспроводная) и т. д. Расположение: SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged; SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed; SOFTWARE\Microsoft\Windows NT\CurrentVersion\Network List\Nla\Cache;
- *Cookies* — артефакт, анализируемый для получения информации о посещенных пользователем сайтах. Для разных браузеров располагаются в разных директориях;
- *Search Terms* (поисковые запросы в браузерах) — артефакт, содержащий информацию о дате и времени посещения сайтов, числе посещений, поисковых запросах. Он расположен для разных браузеров в разных директориях;
- *IP-адрес* — информация об IP-адресе, которая, например, может быть получена из системного реестра, используется для определения нахождения пользователя.

Задача определения информации об учетной записи. Артефакты:

- *информация о смене пароля* — артефакты, содержащие информацию о последней смене пароля пользователем, расположены в C:\windows\system32\config\SAM и системном реестре по адресу SAM\ Domains\Account\Users;
- *успешная/неуспешная авторизация* — артефакты, содержащие информацию об успешных авторизациях и ее попытках (неуспешных авторизациях), расположены в системном журнале по адресу: **Win7** %system root%\System32\winevt\logs\Security.evtx;

- *системный журнал* — подробная информация об учетной записи, запуске ОС, приложений, установке приложений, сетевых соединениях содержится в системном журнале ОС;
- *RDP-соединения* — артефакт, содержащий информацию о соединениях по протоколу RDP (в том числе информацию об IP-адресе устройства, подключившегося по RDP) и расположенный по адресу: **Win7** %system root%\System32\winevt\logs\Security.evtx;
- *авторизация пользователя* — артефакты, содержащие информацию об авторизации пользователя в ОС, расположены по адресу C:\windows\system32\config\SAM и в системном реестре: SAM\Domains\Account\Users.

Задача определения интернет-активности пользователя [49]. Браузер *Internet Explorer (IE)* предоставляется вместе с ОС Microsoft Windows как составная часть инсталляционного пакета ОС. Артефактами IE являются:

- файлы *index.dat*. Данные файлы содержат записи о доступе к url, включая поисковые запросы, доступ к Веб-почте. Данный артефакт часто считается основным источником судебной информации при анализе IE браузера;
- «избранное» IE. «Избранное» — закладки в Internet Explorer, оставленные пользователем при движении в сети. «Избранное» пользователя можно найти (в Windows XP) в директории \Documents and Settings\user\Favorites. Помимо содержимого «Избранного» эксперт может найти ценную информацию в файле MAC times. Данный файл иллюстрирует время создания файла, время последнего доступа к файлу, время внесения последних изменений;
- *Cookies IE*. Cookies Internet Explorer находятся по пути Users \ %username% \ AppData\Roaming\Microsoft\Windows\Cookies (в ОС Vista и Windows 7). IE представляет cookies пользователя виде текстовых файлов — они могут быть просмотрены непосредственно;
- *Cache IE* (кэш). Кэш браузера — это файлы, которые остаются в системе в результате активности пользователя в сети Internet. В Windows Vista и Windows 7: Users\ %username%\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5.

Браузер Mozilla's Firefox — это второй по популярности браузер в мире после Internet Explorer:

- Firefox 3 сохраняет данные истории в файлы базы данных SQLite 3, которые достаточно просто просматриваются с помощью инструментов с открытым исходным кодом. *Formhistory.sqlite*: содержит данные, вводимые пользователем. Эти данные включают в себя: имена, адреса, адреса электронной почты, номера телефонов, Веб-почту, поисковые запросы. *Downloads.sqlite*: содержит данные о загружаемых файлах. *Cookies.sqlite*: содержит данные о cookies. *Places.sqlite*: содержит данные Internet history (данные Интернет-активности пользователя);
- Cache (кэш). В различных операционных системах кэш Firefox сохраняется в разных местах: ОС Windows Vista/7 — \Users\%username%\AppData\Roaming\Mozilla\Firefox\Profiles; ОС Linux – /home/$username/.mozilla/firefox/Profiles;
- Сохраненные данные сессии. При некорректном завершении работы с браузером (например, отключение электричества) создается файл *sessionstore.js* в директории профиля пользователя. Данный файл содержит информацию, необходимую браузеру для восстановления сессии. Для более комфортного анализа информации данного файла предпочтительнее использование не текстового программного редактора, а просмотрщика. В качестве просмотрщика может быть использовано программное обеспечение с открытым исходным кодом, например *JSON Viewer*;
- расширения. Firefox поддерживает установку расширений, которые могут улучшить или изменить работу с браузером. Данные расширения содержатся в файле *extensions.rdf*, в каталоге пользователя. Иногда эти данные также полезны при производстве экспертизы.

Chrome — это браузер, разработанный Google и являющийся программным обеспечением с открытым исходным кодом. Об артефактах в Chrome:

- как в Firefox, так и в Chrome для хранения данных пользователя используются базы данных SQLite. В различных ОС база данных хранятся в различных местах: в Windows Vista/7 — \Users\%username%\AppData\Local\Google\Chro-

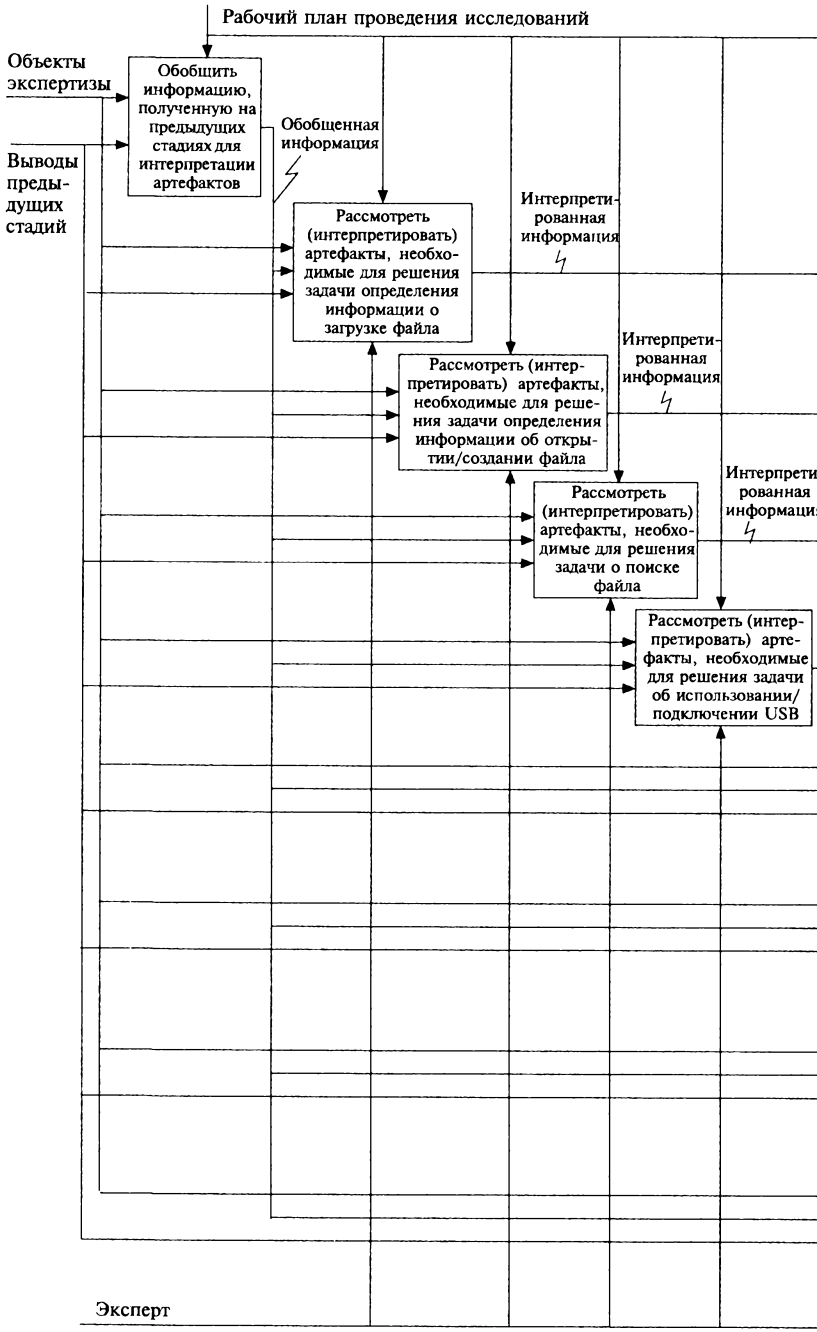
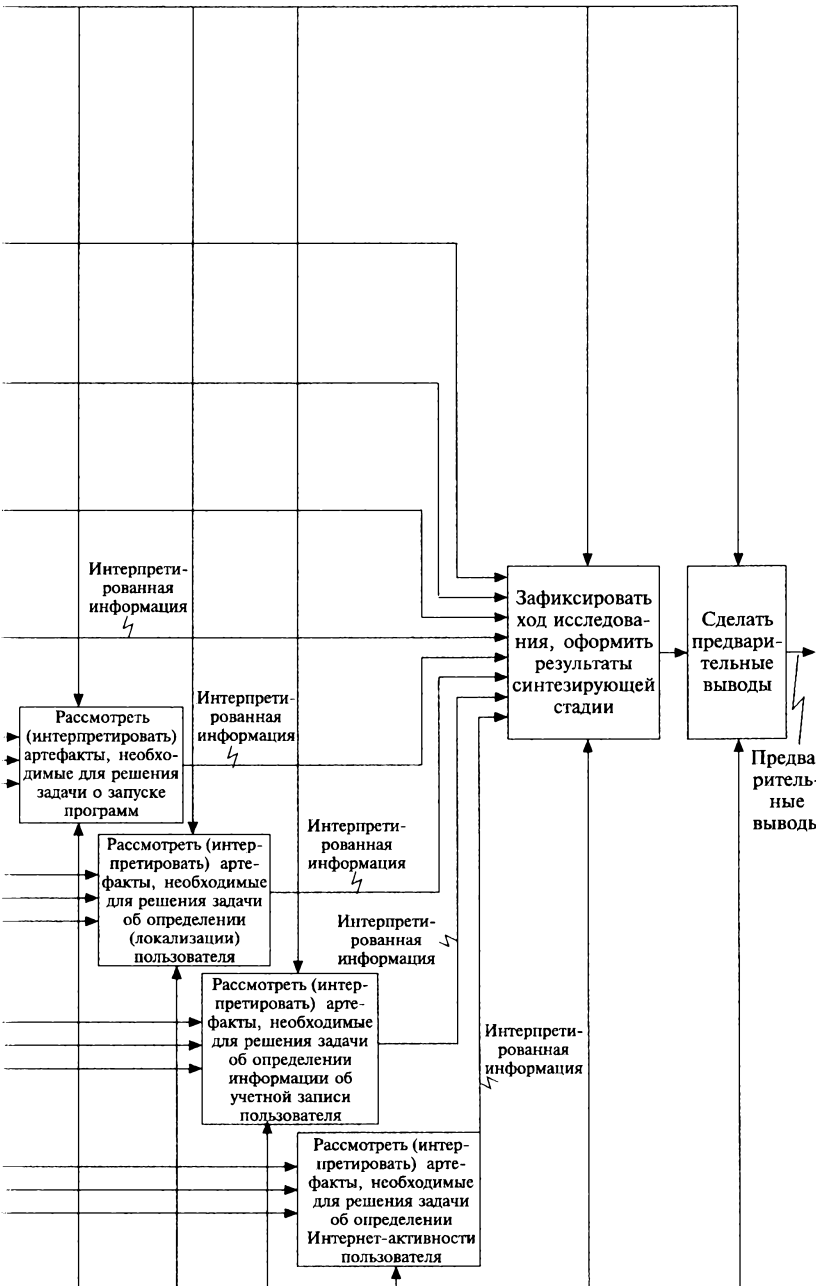


Рис. 3.4. IDEF0-диаграмма производства



синтезирующей стадии КТЭ

me\Default; в Linux — /home/$username/.config/google-chrome/Default;

- Cookies — это база данных SQLite, используемая для ведения истории cookies. Информация, содержащаяся в этой базе данных, содержит информацию о времени создания файла cookie, времени последнего доступа к нему и хост-файлу cookie;
- History — это база данных SQLite, содержащая наиболее интересную информацию об активности пользователя, поделенную на таблицы. Наибольший интерес представляют таблицы: downloads, urls, visits;
- Login Data — это база данных SQLite, содержащая информацию о сохраненных учетных данных. В ОС Linux здесь может содержаться информация о паролях;
- Web Data — это база данных SQLite, содержащая информацию, сохраненную пользователям для осуществления возможности автозаполнения. Эта информация может включать информацию об именах, адресах, номерах кредитных карт и т. д.;
- Thumbnails — это база данных SQLite, содержащая миниатюры изображений посещенных сайтов;
- Bookmarks — это файл, содержащийся в директории профиля пользователя и содержащий закладки пользователя в браузере. Этот файл содержит объекты JSON и может быть просмотрен с помощью любого JSON-просмотрщика или просто текстовым редактором;
- Local State — этот файл используется для восстановления работы в Chrome после некорректного завершения работы. Файл содержит объекты JSON;
- *Cache* (кэш) в Chrome представлен виде index-файла, четырех пронумерованных файлов данных (от data_0 до data_3) и множества файлов, начинающихся с «f» и оканчивающихся на комбинацию из шести шестнадцатеричных цифр.

На рис. 3.4 представлена IDEF0-диаграмма производства синтезирующей стадии КТЭ.

3.5. Результирующая стадия

Результирующая стадия — это стадия, на которой происходит подведение итогов, оцениваются результаты проведенных исследований. На данной стадии выполняется окончательное оформление исследовательской (и если требуется вводной) части заключения.

На рис. 3.5 представлена IDEF0-диаграмма производства результативной стадии КТЭ.

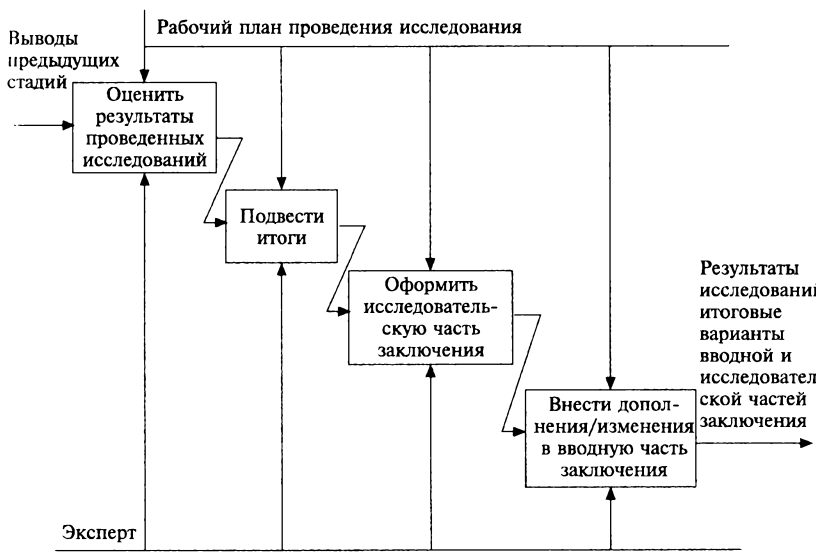


Рис. 3.5. IDEF0-диаграмма производства результативной стадии КТЭ

3.6. Формирование выводов

Формирование выводов — на этой стадии оформляются выводы по экспертизе. Результаты этой стадии оформляются в разделе заключения «Выводы». В Выводах должны быть обязательно отражены все вопросы экспертизы и ответы на них.

Вывод по каждому вопросу должен быть развернутым, желательно указание ссылок на пункты, страницы исследовательской части, исходя из которых сделаны выводы.

На рис. 3.6 представлена IDEF0-диаграмма производства стадии формирования выводов КТЭ.

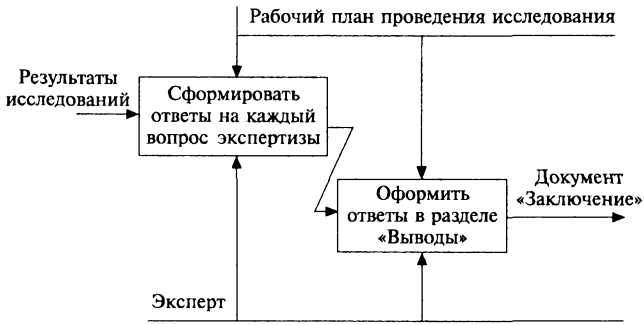


Рис. 3.6. IDEF0-диаграмма производства стадии формирования выводов КТЭ

3.7. Заключение эксперта

Согласно требованиям законодательства, в заключении эксперта обязательно указываются [3–7]:

- дата, время и место производства судебной экспертизы;
- на основании чего производится судебная экспертиза;
- информация о должностном лице, назначившем судебную экспертизу;
- информация об экспертном учреждении и эксперте (ФИО эксперта, специальность, образование, занимаемая должность, стаж работы, ученая степень и (или) ученое звание);
- информация о предупреждении эксперта об ответственности за дачу заведомо ложного заключения;
- вопросы, поставленные на разрешение экспертизы;
- объекты исследований и материалы, представленные для производства судебной экспертизы;
- данные о лицах, которые присутствовали при производстве экспертизы;
- состав и результаты исследований с перечнем использованных методик;
- выводы по вопросам, поставленным перед экспертом, и их обоснование.

В случае необходимости экспертом подаются ходатайства (ходатайства могут быть заявлены на любой стадии исследования):

- об ознакомлении с материалами дела, имеющими отношение к предмету экспертизы;

- о предоставлении дополнительных материалов, имеющих отношение к экспертизе;
- о привлечении другого эксперта;
- об участии в процессуальных действиях;
- о применении разрушающих/частично разрушающих методов.

Информация о поданных ходатайствах и их разрешении отображается в заключении.

Эксперт вправе отказаться от дачи заключения в случае выявления на любой стадии исследования следующих обстоятельств:

- эксперт не обладает достаточной компетентностью для решения поставленных задач;
- в экспертном учреждении отсутствует материально-техническая база, необходимая для проведения исследования;
- недостаточно данных после заявленных ходатайств;
- нет данных науки для решения поставленных вопросов.

В случае отказа от дачи заключения экспертом оформляется сообщение о невозможности проведения исследования

3.8. Оценка эффективности разработанной методики производства экспертизы

Говоря об эффективности методики, будем понимать возможность эксперта с ее помощью выполнять работу (производить КТЭ) и достигать необходимого или желаемого результата с наименьшей затратой времени и других ресурсов.

Как было сказано ранее (см. п. 1.4), требования законодательства к методике и методам производства экспертизы в целом и к КТЭ в частности определяются основными процессуальными нормами, определенными УПК РФ в отношении судебной экспертизы и Федеральным законом № 73 «О государственной судебно-экспертной деятельности в Российской Федерации». Экспертная методика должна обеспечивать полноту исследования, быть научно обоснованной, всесторонне исследовать объект и обеспечивать достоверность экспертного заключения, отвечать требованиям законности, быть безопасной, этичной, допустимой, эффективной, экономичной [3, 21]. Все требования можно условно разделить на две группы:

- требования, влияющие на допустимость экспертного заключения как средства доказывания;
- требования, влияющие на конечную стоимость производства экспертизы, ее время и требуемую квалификацию экспертов.

Будут ли назначены по проведенной экспертизе повторные и дополнительные экспертизы, влияет первая группа требований (к ней относятся весь перечень требований кроме требования к экономичности). Вторая группа требований влияет на стоимость и сроки производства экспертизы (это требования к эффективности и экономичности). Таким образом, требование к эффективности включает в себя одновременно и качественные требования (допустимость производства экспертизы) и численные (стоимость и сроки производства экспертизы).

Такой подход используются при производстве экспертиз по гражданским, арбитражным и уголовным делам. Общепринятой практикой является применение при производстве одной экспертизы одновременно нескольких методик. Такой комплексный подход предполагает использование экспертом преимуществ различных методик для каждой конкретной экспертизы. По некоторым из экспертиз при этом назначаются повторные и дополнительные экспертизы, так как большое значение в таком подходе играет опыт эксперта. При этом сам подход являются допустимым судом для производства КТЭ.

Наиболее опытные эксперты используют комплексный подход, добиваясь большей эффективности. Потому сравнение разработанной методики будем производить с ним.

Приведем некоторые примеры проведенных экспертиз. Результаты сравнительного анализа представлены в табл. 3.1 и на рис. 3.7.

Таким образом, наш подход по сравнению с комплексным подходом позволяет добиться выигрыша, гарантируя получение даже экспертом низкой квалификации экспертного заключения, соответствующего требованиям законодательства по следующей группе критериев:

- время разработки частной методики КТЭ (относительно общепринятой методики) — меньше на 20...40 %;
- сроки производства экспертизы (относительно общепринятой методики) — меньше на 10...25 %;

Таблица 3.1

Сравнительная оценка эффективности методики

Методика	Допустимость (интегральный критерий качества — процент результатов, принятых судами)	Время разработки частной методики КТЭ (относительно общепринятой методики)	Сроки производства экспертизы (относительно общепринятой методики)	Стоимость производства (относительно общепринятой методики)
Комплексный подход на основе использования наиболее распространенных методик (п. 1.5)	В пределах нормы судов РФ	100 %	100 %	100 %
Разработанная методика	В пределах нормы судов РФ (на текущей выборке — 100 %)	60...80 % в зависимости от особенностей КТЭ	75...90 % в зависимости от особенностей экспертизы и квалификации эксперта	70...90 % в зависимости от особенностей экспертизы (за счет снижения времени проведения и требований к квалификации эксперта)

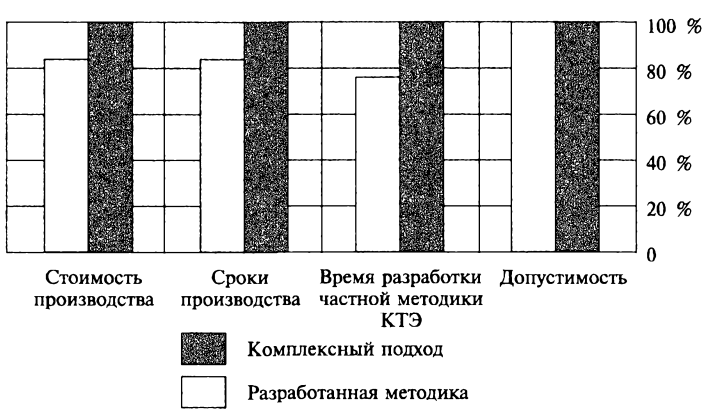


Рис. 3.7. Сравнительная диаграмма комплексного подхода и разработанной методики (использованы средние значения)

- стоимость производства (относительно общепринятой методики) — меньше на 10...30 %.

Заключения экспертов не получили ни одного отклонения в суде при оценке их на допустимость.

По экспертным заключениям в рамках гражданского, арбитражного и уголовного судопроизводств, выполненных в соответствии с разработанной методикой, не было назначено повторных или дополнительных экспертиз.

3.9. Резюме

Предлагаемый подход и методическое обеспечение производства КТЭ ориентированы на экспертов КТЭ частных и государственных экспертных учреждений. В них содержатся рекомендации по выполнению стадий производства КТЭ и применению частных инструментальных методов; требования по оформлению экспертного заключения; описание структуры заключения эксперта о результатах производства КТЭ.

Методическое обеспечение предполагает использование пошаговых алгоритмов стадий производства КТЭ, разработанных на основе анализа графовых моделей производства КТЭ. Пошаговые алгоритмы представлены в виде IDEF0-диаграмм для каждой стадии производства КТЭ.

Разработанная методика по сравнению с комплексным подходом позволяет добиться выигрыша по следующей группе критериев, гарантируя получение даже экспертом низкой квалификации экспертного заключения, соответствующего требованиям законодательства:

- время разработки частной методики КТЭ (относительно общепринятой методики) — меньше на 20...40 %;
- сроки производства экспертизы (относительно общепринятой методики) — меньше на 10...25 %;
- стоимость производства (относительно общепринятой методики) — меньше на 10...30 %.

Предложенное методическое и алгоритмическое обеспечение может быть использовано для автоматизации, а значит, упрощения процесса разработки частных методик производства КТЭ путем создания системы поддержки формирования частных методик производства КТЭ.

4 ПРАКТИЧЕСКОЕ ПРИМЕНЕНИЕ РАЗРАБОТАННОЙ МЕТОДИКИ ПРОИЗВОДСТВА КТЭ

Как было ранее представлено, в составе КТЭ выделяют четыре вида экспертиз — аппаратно-компьютерную, программно-компьютерную, информационно-компьютерную (она же экспертиза данных) и компьютерно-сетевую [16]. Выделение такого числа и именно таких видов обусловлено свойствами объектов, предоставляемых на экспертизу, и вопросами, решаемыми в рамках каждой конкретной экспертизы.

Рассмотрим применение методики в производственном процессе экспертного учреждения (для всех 4 видов экспертиз).

4.1. Аппаратно-компьютерная экспертиза (пример экспертизы № 1)

Руководствуясь ст. 79, 216, 224 ГПК РФ мировым судьей назначено проведение компьютерно-технической экспертизы по гражданскому делу о взыскании убытков, морального вреда и судебных расходов.

Эксперту в связи с назначением проведения экспертизы в соответствии со ст. 85 ГПК РФ разъяснены права и обязанности эксперта. Об ответственности за дачу заведомо ложного заключения в соответствии со ст. 307 УК РФ эксперт был предупрежден.

На разрешение экспертизы поставлены следующие вопросы:

1. В каком техническом состоянии на момент исследования находится сотовый телефон Samsung GT-C3010 IMEI <*номер*>?

2. Имеются ли в данном телефоне неисправности, если да, то какие?

3. Могут ли указанные неисправности быть следствием неправильной эксплуатации телефона либо производственного (конструктивного) брака?

4. Имеются ли в телефоне следы неавторизованного ремонта, следы залития какой-либо жидкостью?

5. Какова давность их возникновения?

6. Является ли существенной неисправностью заявленный истицей дефект: телефон не заряжается?

На экспертизу поступили следующие объекты:

- копия определения о назначении компьютерно-технической экспертизы;
- мобильный телефон Samsung GT-C 3010 в упаковке (не опечатанный);
- материалы гражданского дела.

Был разработан следующий план производства экспертизы.

1. Методом органолептического осмотра устанавливались:

- товарные характеристики изделия (модель, конструкция, цвет, применяемые материалы);
- пороки (дефекты), их расположение, степень выраженности;
- причина возникновения пороков (дефектов) и их характер (производственный, эксплуатационный).

2. Аналитическая обработка результатов исследования.

3. Формулирование окончательных выводов.

Исследование проводилось с использованием следующего оборудования:

- детальная и обзорная фотосъемка проводилась при естественном и искусственном освещении методом обычной и макросъемки цифровым фотоаппаратом DMC-LZ8EE9K фирмы Panasonic с применением встроенной фотовспышки;
- для замеров напряжения аккумуляторной батареи специалистом был использован цифровой мультиметр FLUKE, модель 177 (мультиметр поверен в ТЦСМ);
- оптическая лупа с увеличением 5х;
- контрольные SIM карты (MTS, Beeline);
- оригинальный блок питания торговой марки Samsung.

В результате были получены следующие выводы:

1. В каком техническом состоянии на момент исследования находится сотовый телефон Samsung GT-C3010 IMEI <*номер*>?

Представленный на исследование сотовый телефон находится в технически неисправном состоянии.

2. Имеются ли в данном телефоне неисправности, если да, то какие?

В представленном на исследование телефоне имеется неисправность (дефект) аккумуляторной батареи, входящей в его комплектацию.

3. Могут ли указанные неисправности быть следствием неправильной эксплуатации телефона либо производственного (конструктивного) брака?

Выявленная экспертом неисправность аккумуляторной батареи вызвана окончанием срока ее службы. Признаков производственного (конструктивного) брака, как и признаков ненадлежащего эксплуатационного воздействия у представленной на исследование аккумуляторной батареи, не установлено.

4. Имеются ли в телефоне следы неавторизованного ремонта, следы залития какой-либо жидкостью?

В результате исследования установлено наличие налета белого цвета на компаунде отдельных краевых участков платы. Причина возникновения: попадание влаги внутрь корпуса в процессе эксплуатации или эксплуатация объекта в условиях повышенной влажности.

Следов и признаков неавторизованного ремонта на установочных элементах платы экспертом не установлено.

5. Какова давность их возникновения?

Определить время возникновения на плате исследуемого телефона прозрачного вещества светло-коричневого цвета и налета белого цвета эксперту не представляется возможным вследствие отсутствия методик на определение давности.

6. Является ли существенной неисправностью заявленный истицей дефект: телефон не заряжается?

Неисправность (дефект) аккумуляторной батареи, входящей в комплект мобильного телефона Samsung GT-C3010, относится к дефектам малозначительным, устранимым.

Полный текст заключения по данной экспертизе приобщен к материалам дела и находится в закрытом доступе.

4.2. Программно-компьютерная экспертиза (пример экспертизы № 2)

Постановлением старшего следователя было назначено проведение компьютерно-технической судебной экспертизы по материалам уголовного дела.

Эксперту в соответствии со ст. 57 УПК РФ разъяснены права и обязанности эксперта. По ст. 307 УК РФ об ответственности за дачу заведомо ложного заключения эксперт был предупрежден, о чем дал подписку.

На экспертизу поступили:

- постановления на 3-х листах в 1 экземпляре;
- жесткий диск Samsung;
- USB-flash накопитель;
- два оптических DVD-R диска.

Перед экспертом были поставлены вопросы:

1. Имеются ли на представленных носителях программные продукты, имеющие отличия от лицензионных программных продуктов, правообладателем которых являются корпорация Microsoft, корпорация Adobe Systems Incorporated, корпорация Corel? Если имеются, то когда установлены, когда последний раз с ними работали?

2. Совершался ли неправомерный доступ к компьютерной информации, повлекший уничтожение, блокирование, модификацию либо копирование информации с целью снятия защиты от нелицензионного использования программных продуктов, правообладателями которых являются корпорация Microsoft, корпорация Adobe Systems Incorporated, корпорация Corel?

3. Имеются ли на представленных носителях программы, заведомо приводящие к несанкционированному уничтожению, блокированию, модификации либо копированию информации с целью снятия защиты от нелицензионного использования программных продуктов, правообладателями которых являются корпорация Microsoft, корпорация Adobe Systems Incorporated, корпорация Corel?

4. Имеются ли на представленных носителях программы, модифицирующие либо удаляющие защиту лицензионных программ, правообладателем которых являются корпорация Microsoft, корпорация Adobe Systems Incorporated, корпорация Corel?

При исследовании применялось следующее оборудование:

- тестовый компьютер Pentium(R) Dual-Core CPU E5300, 2600 MHz;
- фотоаппарат SONY DSC-R1, 10,3 Mp;
- USB-адаптер AGESTAR USB 2.0 Multi-function Adapter;
- масштабная линейка.

Осмотр предметов, представленных на экспертизу, проводился в помещении экспертного учреждения. Осмотр проводился при искусственном освещении. Фиксация свойств объектов осмотра проводилась цифровым фотоаппаратом SONY DSC-R1.

Эксперт проводил экспертизу на основе изложенной выше методики. Несмотря на то что методика применялась для вида КТЭ, отличного от описанного в предыдущем пункте, она не требует от эксперта дополнительного обучения, так как предполагает единообразие в проведении исследования.

В результате были получены следующие выводы:

- *По первому вопросу постановления:*

При исследовании информации, содержащейся на представленных на экспертизу носителях информации, установлено наличие программных продуктов корпорации Microsoft, имеющих отличия от лицензионных программных продуктов корпорации Microsoft и продуктов, определяемых как скомпрометированные продукты. Информация о дате установке, запуске продуктов представлена в п. 2.1 заключения.

- *По второму вопросу постановления:*

В результате исследования были установлены признаки *несанкционированного* доступа. «Несанкционированный доступ (НСД) — доступ к информационной системе или к компьютерной информации в нарушение установленного порядка; этот термин является техническим, в отличие от юридического термина «неправомерный доступ», хотя означает почти то же самое».

По третьему вопросу постановления:

Имеются. Подробное описание приведено в п. 2.3 исследовательской части заключения.

- *По четвертому вопросу постановления:*

Программное обеспечение, указанное в данном вопросе постановления, на исследуемых носителях информации не обнаружено.

Полный текст заключения по данной экспертизе приобщен к материалам дела и находится в закрытом доступе.

4.3. Экспертиза данных (пример экспертизы № 3)

Постановлением дознавателя назначено проведение компьютерно-технической экспертизы по материалам уголовного дела.

Экспертам в соответствии со ст. 57 УПК РФ разъяснены права и обязанности эксперта. По ст. 307 УК РФ об ответственности за дачу заведомо ложного заключения предупреждены.

На экспертизу поступили:

- постановление на 2-х листах в 1 экземпляре;
- системный блок в корпусе бело-черного цвета;
- USB-flash накопитель в корпусе желтого цвета, с металлической крышкой.

Вопросы, поставленные перед экспертами:

Имеются ли в системном блоке, флеш-карте, в том числе и в удаленных файлах файлы с названиями, либо имеющие фразы, слова, а также сканированные документы, информация и переписка с использованием электронной почты: (далее <перечень слов>)?

В случае обнаружения перечисленных документов и информации указать:

- места их хранения;
- даты изготовления, получения документов и информации;
- вид представления документов и информации;
- передавались ли документы, информация электронной почтой из Китайской Народной Республики, какие (какая) именно;
- изготавливались ли документы на представленном системном блоке и использовались ли документы для изготовления других документов, если да, то какое их первоначальное содержание;
- имеются ли удаленные файлы, подлежат ли они восстановлению, каково их первоначальное содержание.

При исследовании применялось следующее оборудование:

- тестовые компьютеры Pentium(R) Dual-Core CPU E5300, 2600 MHz;

- фотоаппарат Panasonic DMC-FX10 (6Mps);
- USB-адаптеры AGESTAR USB 2.0 Multi-function Adapter.

Осмотр предметов, представленных на экспертизу, проводился в помещении экспертного учреждения. Осмотр проводился при искусственном освещении. Фиксация свойств объектов осмотра проводилась цифровым фотоаппаратом Panasonic DMC-FX10.

Экспертиза проводилась на основании разработанной методики. Несмотря на то что методика применялась для вида КТЭ, отличного от описанного в предыдущем пункте, она не требует от эксперта дополнительного обучения, так как предполагает единообразие в проведении исследования.

В результате были получены следующие выводы.

На представленных на исследование носителях информации имеются файлы, удовлетворяющие вопросу постановления. Описание обнаруженных файлов приведено в Приложении к экспертному заключению.

Полный текст заключения по данной экспертизе приобщен к материалам дела и находится в закрытом доступе.

4.4. Компьютерно-сетевая экспертиза (пример экспертизы № 4)

Основанием для проведения экспертизы послужило постановление старшего следователя о назначении компьютерно-технической экспертизы, поступившее в экспертное учреждение.

Эксперту в соответствии со ст. 57 УПК РФ разъяснены права и обязанности эксперта. По ст. 307 УК РФ об ответственности за дачу заведомо ложного заключения эксперт был предупрежден, о чем дал подписку.

На экспертизу поступили:

- постановления на 3-х листах в 1 экземпляре;
- системный блок черного цвета.

Перед экспертом были поставлены вопросы:

1. Существуют ли технические возможности соединения с сетью Интернет с использованием системного блока, представленного на экспертизу. Если да, то какие сетевые настройки на нем установлены?

2. Какие индивидуальные номера (IP-адреса), сетевое имя имеет представленный на экспертизу накопитель информации, позволяющий его идентифицировать при выходе в сеть Internet?

Экспертиза проводилась на основании разработанной автором методики. Несмотря на то что методика применялась для вида КТЭ, отличного от описанного в предыдущем пункте, она не требует от эксперта дополнительного обучения, так как предполагает единообразие в проведении исследования.

При исследовании применялось следующее оборудование:

- тестовый компьютер Pentium(R) Dual-Core CPU E5300, частота 2600 MHz;
- фотоаппарат Panasonic DMC-FX10 (6 Mps);
- USB-адаптеры AGESTAR USB 2.0 Multi-function Adapter.

Осмотр предметов, представленных на экспертизу, проводился в помещении экспертного учреждения. Осмотр проводился при искусственном освещении. Фиксация свойств объектов осмотра проводилась цифровым фотоаппаратом Panasonic DMC-FX10.

В результате были получены следующие выводы:

- *По первому вопросу постановления.*

Техническая возможность выхода в сеть Internet с помощью исследуемой рабочей станции существует при условии, что маршрутизирующим устройством локальной сети, в которой находится исследуемый объект, для него предоставляется такая возможность. Сетевые настройки представлены в пункте 2.3 исследовательской части заключения.

- *По второму вопросу постановления.*

Исследуемый системный блок не имеет индивидуальных идентификаторов в сети Интернет.

Полный текст заключения по данной экспертизе приобщен к материалам дела и находится в закрытом доступе.

4.5. Резюме

Несмотря на то что изложенный подход применялся для разных видов КТЭ, от экспертов не потребовалось дополнительного обучения, так как предполагает унифицированное проведение исследования.

Перспективой развития является продолжение направления, заданного работами [110–119], и создание системы, позволяющей автоматизировать формирование частных методик производства компьютерно-технических экспертиз (далее — система). В системе для формирования частных методик следует использовать две группы входных параметров: предмет экспертизы (категории задач, вопросы экспертизы, объекты исследования); условия проведения экспертизы (временные ресурсы, финансовые ресурсы, человеческие ресурсы и т. д.). Данные параметры определяют последовательность методов, которые будут применены на стадиях производства КТЭ.

Первая группа входных параметров системы определяет общую методику для вида КТЭ с учетом вопросов КТЭ и объектов. Вторая группа входных параметров (условия проведения экспертизы) уточняет общую методику до частной методики.

Методы форензики, применяемые на каждой из стадий КТЭ, должны соответствовать выбранной методике производства КТЭ в соответствии заданными входными параметрами первой группы. Так как во многих методиках КТЭ одновременно описываются несколько методов, предоставляющих возможность провести всестороннее и полное исследование и направленных на решение одних и тех же задач, предлагается определение методов исследования для частной методики производства КТЭ исходя из потребностей экспертной организации. Потребности экспертной организации учитываются в системе как дополнительная группа входных параметров при формировании частной методики.

ЗАКЛЮЧЕНИЕ

Форензика — наука, которая стремительно развивается. Еще стремительнее развивается информационно-телекоммуникационные технологии, многочисленные информационные системы и сетевые сервисы. Кроме того, специфика расследования преступлений в сфере высоких технологий требует крайней деликатности в изложении подходов и методов проведения КТЭ, а также приведения конкретных примеров расследований. Неудивительно, что в отечественной литературе практически не представлены изложения теоретических обоснований, методов КТЭ, обоснований по унификации подходов при проведении КТЭ. Имеющиеся источники либо ограничены отсутствием теоретических основ, изобилуя практическими методиками, либо весьма устарели и не представляют собой практического интереса. Авторы постарались устранить этот недостаток.

В результате КТЭ, проводимой при расследовании преступлений, связанных с нарушением информационной безопасности в открытых компьютерных сетях, хищением (разрушением, модификацией) информации и нарушением информационной безопасности, формируется информация об уязвимости процессов переработки информации в информационных системах. Эти сведения могут и используются специалистами по информационной безопасности для совершенствования существующих средств защиты информации и обеспечения информационной безопасности.

Не претендуя на всеобщность, авторы надеются, что предложенные ими выше подходы и результаты могут быть весьма полезными. Опыт проведения значительного числа КТЭ, результаты которых ни разу не были отклонены правоохранительными органами, подтверждают эти надежды. Авторы также понимают, что представленные подходы не исчерпывают всех возможных решений. Учитывая непрерывное совершенствование

инструментария и высокую квалификацию злоумышленников, следует постоянно совершенствовать методики, алгоритмы, вести подготовку высокопрофессиональных специалистов в области форензики для успешного противостояния преступным намерениям.

ЛИТЕРАТУРА

1. HI-TECH CRIME TRENDS 2017. — http://files.runet-id.com/2017/csf17/07feb.csf17-3.2-sachkov.pdf

2. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем. — М.: Право и закон, 2003.

3. Концептуальные основы судебной компьютерно-технической экспертизы. — http://www.dslib.net/kriminal-process/konceptualnye-osnovy-sudebnoj-kompjuterno-tehnicheskoj-jekspertizy.html

4. Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» (с изменениями на 8 марта 2015 года). — http://docs.cntd.ru/document/901788626

5. Гражданский процессуальный кодекс РФ (ГПК РФ 2015) (с изменениями на 30 декабря 2015 года). — http://docs.cntd.ru/document/grazhdanskij-processualnyj-kodeks-rf-gpk-rf

6. Уголовно-процессуальный кодекс РФ (УПК РФ) (с изменениями на 30 декабря 2015 года). — http://docs.cntd.ru/document/ugolovno-processualnyj-kodeks-rf-upk-rf

7. Арбитражный процессуальный кодекс РФ (АПК РФ 2015) (с изменениями на 30 декабря 2015 года). — http://docs.cntd.ru/document/arbitrazhnyj-processualnyj-kodeks-rf-apk-rf

8. Постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам». — https://rg.ru/2010/12/30/postanovlenie-dok.html

9. Handbook по дисциплине: «Современные возможности судебной экспертизы»: Программа магистерской подготовки по направлению «Юриспруденция». — http://e-biblio.ru/book/bib/04_pravo/Sovrem_VSD/hb.html

10. Россинская Е.Р. Судебная экспертиза в гражданском, арбитражном, административном и уголовном процессе. — http://www.vuzllib.su/books/2180-Судебная_экспертиза_в_гражданском,

арбитражном, административном и уголовном процессе / Е.Р. Россинс

11. Цели и задачи судебно-экспертного исследования: проблемы теоретического обоснования. — http://www.center-bereg.ru/f1879.html

12. Предмет судебной экспертизы. — http://www.law.edu.ru/doc/document.asp?docID=1311442

13. Зубаха В.С., Усов А.И., Саенко Г.В., Волков Г.А., Белый С.Л., Семикаленова А.И. Общие положения по назначению и производству компьютерно-технической экспертизы: Методические рекомендации. — М.: ГУ ЭКЦ МВД России, 2000. — 65 с.

14. Федотов Н.Н. Форензика — компьютерная криминалистика. — М.: Юридический мир, 2007.

15. Приказ Министерства юстиции Российской Федерации (Минюст России) от 27 декабря 2012 г. № 237 «Об утверждении Перечня родов (видов) судебных экспертиз, выполняемых в федеральных бюджетных судебно-экспертных учреждениях Минюста России, и Перечня экспертных специальностей, по которым представляется право самостоятельного производства судебных экспертиз в федеральных бюджетных судебно-экспертных учреждениях Минюста России». — https://rg.ru/2013/02/06/expertiz-dok.html

16. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: Учебное пособие / Под ред. проф Е.Р. Россинской. — М.: Экзамен; Право и закон, 2003. — 368 с.

17. Шляхов А.Р. Предмет и система криминалистической экспертизы // Тр. ВНИИСЭ. 1971. Вып. 3. С. 17.

18. Орлова В.Ф. Теория судебно-почерковедческой идентификации // Тр. ВНИИСЭ. 1973. Вып. 6. С. 230.

19. Митричев В.С. Общие положения методики криминалистического идентификационного исследования материалов документов // Тр. ВНИИСЭ. 1974. Вып. 9. С. 18.

20. Колмаков В.П. О методах, приемах и средствах в советской криминалистике // Правоведение. 1965. № 4. С. 118–120.

21. Курс лекций по учебной дисциплине «Судебная экспертиза». — http://distance.rpa-mu.ru/files/2_vys_bak/sudeb_expertiza.pdf

22. Ефимичев С.П. Комментарий к Федеральному закону «О государственной судебно- экспертной деятельности в Российской Федерации» (постатейный) / под ред. В.П. Кашепова. — М.: Юстицинформ, 2003.

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

24. Некоммерческое Партнерство поставщиков программных продуктов (НП ППП). Специальные знания при выявлении и расследовании дел, связанных с нарушениями авторских и смежных прав на программы для ЭВМ и базы данных. Второе издание. — М., 2012.

25. Зубаха В.С. и др. Общие положения по назначению и производству компьютерно-технической экспертизы. — М.: ГУ ЭКЦ МВД, 2001.

26. Расследование преступлений в сфере компьютерной информации. Учебно-методическое пособие / Под общ. ред. А.Н. Родионова — М., 1998.

27. Корухов Ю.Г. Криминалистическая диагностика для экспертов. — М.: Библиотека эксперта, 2007.

28. Кэрриэ Б. Криминалистический анализ файловых систем. — СПб.: Питер, 2007.

29. Bunting S. The Official EnCE: EnCase Certified Examiner Study Guide. Second Edition. — Wiley Publishing, Inc, 2007.

30. Мандиа К., Просис К. Защита от вторжений. Расследование компьютерных преступлений. — М.: ЛОРИ, 2005.

31. Кубэзиэк Р., Моррисси Ш. Криминалистическое исследование Mac OS X, iPod и iPhone. — http://computer-forensics-lab.org/pdf/Mac_OsX_Ipod_rus.pdf

32. Поуг К., Алтеид К., Хаверкос Д. Криминалистическое исследование Unix и Linux. — http://computer-forensics-lab.org/pdf/rus_unix_and_linux_forensic_analysis.pdf

33. Производство судебной компьютерно-технической экспертизы: III. Специализированный словарь компьютерной лексики для экспертов компьютерно-технической экспертизы / Л.Г. Эджубов, А.И. Усов, Е.С. Карпухина, Н.А. Хатунцев, А.С. Демов, Н.Л. Комраков, П.В. Костин. — М.: РФЦСЭ, 2009.

34. Digital Forensics with Open Source Tools by Cory Altheide and Harlan Carvey. — http://fcbi.unillanos.edu.co/segurinfo.unilla-

nos/archivos/materialApoyo/Forensics%20with%20Open%20Source%20tools.pdf

35. Юрин И.Ю. Способы установления первоначального имени PE-файла // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

36. Об определении классификационной принадлежности некоторых сложных технических устройств бытового назначения: Информационное письмо / Е.С. Карпухина, Н.А. Хатунцев, А.К. Сидорова // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

37. Юрин И.Ю. Определение MAC-адресов сетевых устройств // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

38. Коржов Ф.В. Применение ENSCRIPT при проведении СКТЭ // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

39. О производстве судебных экспертиз по делам, связанным с применением законодательства об авторском праве и смежных правах в судебно-экспертных учреждениях Министерства юстиции Российской Федерации: Информационное письмо / Е.С. Карпухина, Н.А. Хатунцев, В.Н. Мяснянкина // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

40. Денявский А.В. Установление следов работы в Интернете пользователя локальной вычислительной сети через постоянное подключение, предоставленное в общий (совместный) доступ // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

41. Тимофеев В.Н. Некоторые вопросы исследования программы 1С Бухгалтерия (Предприятие) версии 7.7 // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

42. Россинская Е.Р., Усов А.И. Возможности судебной экспертизы в раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств. — http://mvd-expo.ru/conferences/CRIM_MVD/doc28.htm

43. Усов А.И. Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использо-

ванием компьютерных средств. — http://jurfak.spb.ru/conference/18102000/usov.htm

44. Разумов М. Компьютерная экспертиза на платформах Windows, часть 1. — http://www.securitylab.ru/?ID=35920

45. Методическое пособие по расследованию преступлений в сфере компьютерной информации и осуществлению прокурорского надзора за исполнением законов при их расследовании. — http://bukva.h14.ru/book/source/booke_26.php

46. Мещеряков В.А. Основы методики расследования преступлений в сфере компьютерной информации. — http://bukva.h14.ru/book/s_disser/Mescheryakov-Avtref_8.php

47. Карви Х. Криминалистическое исследование Windows. Практические примеры. расследовании. — http://computer-forensics-lab.org/pdf/chapter_8_windows.pdf

48. Шелупанов А.А., Смолина А.Р. Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. № 1. С. 31–34.

49. Смолина А.Р. Компьютерно-техническая экспертиза в условиях ограниченного бюджета // Доклады VI Пленума СибРОУМО вузов России по образованию в области информационной безопасности и XV Всероссийской научно-практической конференции «Проблемы информационной безопасности государства, общества и личности»: Томск–Иркутск, 9–13 июня 2014 г. — С. 183-190.

50. Смолина А.Р. Проблемы поиска данных на носителях информации при производстве компьютерно-технических экспертиз // Судебная экспертиза: российский и международный опыт: материалы II Международной научно-практической Конференции, г. Волгоград, 21-22 мая 2014 г. — Волгоград: Изд-во: ВА МВД России, 2014. — С. 386-388.

51. Смолина А.Р. Программные способы восстановления удаленной информации при расследовании компьютерных преступлений // Научная сессия ТУСУР-2013: Материалы Всероссийской научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 15—17 мая 2013 г. — Томск: В-Спектр,

2013: В 5 ч. — Ч. 4. — С. 232-233. — https://storage.tusur.ru/files/43229/2013_4.pdf

52. Предмет, объекты и задачи экспертизы. — http://www.sudexpert.ru/possib/comp.php

53. Смолина А.Р. Результаты анализа методик производства компьютерно-технической экспертизы // Научная сессия ТУСУР-2016: материалы Международной научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 25–27 мая 2016 г. — Томск: В-Спектр, 2016: в 6 ч. — Ч. 5. — С. 96–99. — https://storage.tusur.ru/files/44767/2016_5.pdf

54. Прикладная статистика: Классификации и снижение размерности: Справ. изд. / С.А. Айвазян, В.М. Бухштабер, И.С. Енюков, Л.Д. Мешалкин; Под ред. С.А. Айвазяна.— М.: Финансы и статистика, 1989. — 607 с.

55. Подходы и критерии оценки рисков информационной безопасности / Прищеп С.В., Тимченко С.В., Шелупанов А.А. // Безопасность информационных технологий. 2007. № 4. С. 15-21.

56. Зыков В.Д. Модели и средства обеспечения управления информационной безопасностью медицинских информационных систем: Автореферат диссертации ... кандидата технических наук. — http://old.tusur.ru/export/sites/ru.tusur.new/ru/science/edueducat/diss/2010/09/02.pdf

57. Алексеев В.В., Гаврилов Г.П., Сапоженко А.А. (ред.) Теория графов. Покрытия, укладки, турниры. Сборник переводов. — М.: Мир, 1974. — 224 с.

58. Зыков А.А. Основы теории графов. — М.: Наука, 1987. — 384 с.

59. Калмыков Г.И. Древесная классификация помеченных графов. — М.: Физматлит, 2003. — 192 с.

60. Кристофидес Н. Теория графов. Алгоритмический подход. Пер. с англ. — М.: Мир, 1978. — 432 с.

61. Майника Э. Алгоритмы оптимизации на сетях и графах. Пер. с англ. — М.: Мир, 1981. — 328 с.

62. Оре О. Графы и их применение: Пер. с англ. — М.: Мир, 1965. — 176 с.

63. Кратчайшие пути. — http://life-prog.ru/1_23938_kratchayshie-puti.html

64. Черных Р.А. Обоснование выбора алгоритма поиска кратчайшего пути для построения схемы сети лесовозных дорог. — http://forest-culture.narod.ru/HBZ/Stat_11_1-2/chernih21.pdf

65. Shortest Paths. — https://www.cs.princeton.edu/~rs/AlgsDS07/15ShortestPaths.pdf

66. Поиск путей в графе. — http://life-prog.ru/1_23938_kratchayshie-puti.html

67. Лекции по управлению программными проектами. — http://life-prog.ru/1_23938_kratchayshie-puti.html

68. Оценка длительности задач с помощью анализа по методу PERT. — https://support.office.com/ru-ru/article/Оценка-длительности-задач-с-помощью-анализа-по-методу-PERT-864b5389-6ae2-40c6-aacc-0a6c6238e2eb

69. Методы управления проектом, риском и конфигурацией. — http://www.intuit.ru/studies/courses/2190/237/lecture/6138

70. Метод критического пути. — http://bussin-proj.ru/shpargalki-po-proekt-menedzhmentu/131-metod-kriticheskogo-puti.html

71. Critical Path Analysis and PERT Charts. — https://www.mindtools.com/critpath.html

72. Acronis TrueImage 7.0. — http://www.acronis.com/ru-ru/company/inpress/2004/09-04-ru-ixbt-trueimage-1-creating-image.html

73. Официальный экзамен EnCE: Сертифицированный пользователь EnCase. Учебное руководство. — http://computer-forensics-lab.org/pdf/encase_EnCE.pdf

74. ГОСТ Р 34.11-2012 Информационная технология. Криптографическая защита информации. Функция хэширования. — http: // protect.gost.ru / v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=172313

75. Hidden Disk Areas — HPA/DCO. — http://www.osforensics.com/hidden-areas-hpa-dco.html

76. Service Pack and Update Center. — https://support.microsoft.com/en-us/help/14162/windows-service-pack-and-update-center

77. How to Associate a Username with a Security Identifier (SID). — https://support.microsoft.com/en-us/kb/154599

78. WindowsSCOPE. — http://www.windowsscope.com/index.php?page=shop.product_details&flypage=flypage.tpl&product_id=35&category_ id=3&option=com_ virtuemart

79. Mandiant RedLine. — https://www.mandiant.com/resources/download/redline

80. Computer Online Forensic Evidence Extractor (COFEE). — https://cofee.nw3c.org

81. HELIX3. — http://www.e-fense.com/h3-enterprise.php

82. Password Recovery Toolkit (PRTK). — http://accessdata.com/product-download/digital-forensics/password-recovery-toolkit-prtk-version-7.6.0

83. Passware Kit. — http://www.softportal.com/software-420-passware-kit-enterprise.html

84. Ophcrack. — http://ophcrack.sourceforge.net

85. Shellbag Analyzer & Cleaner. — http://privazer.com/download-shellbag-analyzer-shellbag-cleaner.php#.VU9UvKk9-ZJ

86. WebHistorian. — http://www.mandiant.com/resources/download/web-historian

87. Tzworks. — https://www.tzworks.net/prototype_page.php?proto_id=11

88. Event Log Explorer. — http://www.eventlogxp.com/rus/

89. Event Log Analyzer. — https://www.manageengine.com/products/eventlog/

90. AnalyzeMFT. — http://www.rocketdownload.com/program/analyzemft-446546.html

91. Ntfswalk. — http://download.famouswhy.ca/ntfswalk/

92. Network E-mail Examiner. — http://www.forensicmall.ru/cat/paraben/network-e-mail-examiner-v3-8/

93. Recover My Email. — http://rutracker.org/forum/viewtopic.php?t=1980864

94. Outguess. — http://www.securitylab.ru/software/232888.php

95. Steganography Analyzer Artifact Scanne (StegAlyzerAS). — http://www.forensicmall.ru/cat/back-bone-security /stegalyzerss/

96. WinHex. — http://www.x-ways.net

97. Registry Recon. — http://www.arsenalrecon.com/apps/recon/

98. Recovery Toolbox for Rar. — http://www.recoverytoolbox.com/rar.html

99. Handy Recovery. — http://www.handyrecovery.ru/

100. R-Studio. — http://www.data-recovery-software.net/ru/

101. Демов А.С., Васильев Я.И. Использование специализированных программно-аппаратных комплексов при проведении СКТЭ (на примере из экспертной практики) // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

102. Костин П.В., Комраков Н.Л. К вопросу о понятии исправности и работоспособности средств компьютерной техники // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

103. Костин П.В. Особенности проведения компьютерно-технических экспертиз по установлению фактов размещения информации в сети Интернет // Теория и практика судебной экспертизы: Научно-практический журнал. 2008. № 3 (11).

104. Сергаева Г.А., Пронин В.Н. Пособие по программе «Основы судебной экспертизы» (для подготовки экспертов к аттестации на право самостоятельного производства судебных экспертиз) — Нижний Новгород, 2009.

105. Уголовный кодекс РФ (УК РФ 2015) (с изменениями на 30 декабря 2015 года). — http://docs.cntd.ru/document/ugolovnyj-kodeks-rf-uk-rf

106. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ) от 30.12.2001 № 195-ФЗ,. — http://www.consultant.ru/document/cons_doc_LAW_34661/

107. 21 популярная программа для проведения компьютерно-технических экспертиз. — http://sudexpa.ru/articles/0040/

108. Производство судебной компьютерно-технической экспертизы: I. Общая часть / Л.Г. Эджубов, Е.С. Карпухина, А.И. Усов, Н.А. Хатунцев. — М.: РФЦСЭ, 2009.

109. Производство судебной компьютерно-технической экспертизы: II. Диагностические и идентификационные исследования аппаратных средств / Л.Г. Эджубов, Е.С. Карпухина, А.И. Усов, Н.А. Хатунцев. — М.: РФЦСЭ, 2009.

110. Шелупанов А.А., Смолина А.Р. Формальные основы системы поддержки формирования частных методик производства компьютерно-технической экспертизы // Информационно-управляющие системы. 2017. № 3(88). С. 99–104.

111. Смолина А.Р., Шелупанов А.А. Классификация методик производства компьютерно-технической экспертизы с помощью подхода теории графов // Безопасность информационных технологий. 2016. № 2016-2. С. 73–77.

112. Шелупанов А.А., Смолина А.Р. Теоретические аспекты автоматизации формирования частных методик производства компьютерно-технической экспертизы // Доклады Томского государственного университета систем управления и радиоэлектроники. 2016. № 2016-2. С. 67–70.

113. Смолина А.Р. Решение задачи определения интернет-активности пользователя при производстве компьютерно-технической экспертизы // Научная сессия ТУСУР-2016: материалы Международной научно-технической конференции студентов, аспирантов и молодых ученых, Томск, 25–27 мая 2016 г. — Томск: В-Спектр, 2016: в 6 ч. — Ч. 5. С. 26–29. — https://storage.tusur.ru/files/44767/2016_5.pdf

114. Янковская А.Е., Шелупанов А.А., Миронова В.Г., Смолина А.Р. Основы создания интеллектуальной системы поиска угроз безопасности информации // Труды Конгресса по интеллектуальным системам и информационным технологиям IS& IT'15. Научное издание в 3-х т. — Таганрог: Изд-во ЮФУ, 2015. — Т.2. — С.339–346.

115. Смолина А.Р. Проблемы методического обеспечения компьютерно-технической экспертизы // Материалы Международной научно-технической конференции «Динамика систем, механизмов и машин». — Омск: Изд-во: Омского государственного технического университета, 2014. № 4 С. 96–98.

116. Мицель А.А., Шелупанов А.А., Ерохин С.С. Модель стратегического анализа информационной безопасности // Доклады Томского государственного университета систем управления и радиоэлектроники. 2007. Т. 2. С. 34–41.

117. Епифанцев Б.Н., Шелупанов А.А., Белов Е.Б. Подход к оптимизации ресурсов для защиты информации в организационных системах // Доклады Томского государственного университета систем управления и радиоэлектроники. 2010. Т. 1, № 1. С. 7–9.

118. Миронова В.Г., Шелупанов А.А. Методология формирования угроз безопасности конфиденциальной информации в

неопределенных условиях их возникновения // Известия ЮФУ. Технические науки. 2012. № 12 (137). С. 39–45.

119. Давыдов И. В., Шелупанов А.А. Практические аспекты экспертной деятельности: доклад, тезисы доклада // Научная сессия ТУСУР-2005. — Томск: Издательство ТУСУР, 2005. Ч. 2. С. 93–96.

120. Зайцев А.П., Мещеряков Р.В., Шелупанов А.А. Технические средства и методы защиты информации. Учебник. — М.: Горячая линия — Телеком, 2012.

121. Миронова В.Г., Шелупанов А.А., Югов Н.Т. Реализация модели TAKE-GRANT как представление систем разграничения прав доступа в помещения // Доклады Томского государственного университета систем управления и радиоэлектроники. 2011. № 2–3 (24). С. 206–210.

122. Прищеп С.В., Тимченко С.В., Шелупанов А.А. Подходы и и критерии оценки рисков информационной безопасности // Безопасность информационных технологий. 2007. № 4. С. 15–21.

123. Шумский А.А., Шелупанов А.А. Системный анализ в защите информации. Учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности. — М.: Гелиос, 2005.

Перечень вопросов КТЭ

Полученный на основании методических документов [2, 10, 16–18, 20] полный перечень возможных основных вопросов КТЭ описан в соответствии с предложенной классификацией методик, состоящей из 12 основных типов методик КТЭ.

Вопросы, относящиеся к аппаратным средствам и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач

1. Какой тип, марку, модель, конфигурацию и технические характеристики имеет представленный объект?

2. Позволяет ли представленная компьютерная система решить функциональные задачи (указывается перечень задач)?

3. Находится ли представленный на экспертизу объект в рабочем состоянии?

4. Какие неисправности имеются в работе представленного на экспертизу объекта?

5. Присутствуют ли признаки, свидетельствующие о нарушении правил эксплуатации объекта?

6. Когда было подключено данное (указывается тип устройства) устройство к системному блоку, когда были установлены (инсталлированы) программы, обеспечивающие возможность (указываются возможности, например, «распечатка машинограмм»).

Вопросы, относящиеся к программным средствам и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач

1. Какова общая характеристика объекта представленного на экспертизу, каковы его компоненты (модули)?

2. Каково наименование, версия, тип, вид представления (скрытый, явный, удаленный) программного обеспечения?

3. Каков состав компонентов программного обеспечения, представленного на экспертизу? Определить их характеристики (даты создания, объемы, атрибуты).

4. Каково функциональное предназначение программного средства?

5. Имеются ли на объекте, представленном на экспертизу, программное обеспечение, позволяющее реализовать определенную функциональную задачу?

6. Каковы требования, предъявляемые данным программным обеспечением к аппаратному обеспечению?

7. Совместимо ли данное программное обеспечение с аппаратно-программным обеспечением (указываются конкретные характеристики)?

8. Какова работоспособность программного обеспечения по реализации отдельных (конкретных) функциональных требований?

9. Каким образом выполняется операция/функция (указывается конкретно) в представленном на экспертизу программном обеспечении?

10. Имеет ли программное обеспечение отличия от предоставленного сравнительного образца? Если да, то какие?

11. Определить способ организации защиты информации на представленном объекте?

12. Каков алгоритм работы представленного на экспертизу программного обеспечения?

13. Каковы программно-инструментальные средства, использованные для разработки представленного на экспертизу программного обеспечения?

14. Позволяют ли изменения, внесенные в программное обеспечение, преодолеть его защиту?

15. Каков способ внесения изменений в программу (воздействие вредоносной программы, преднамеренное воздействие, аппаратный сбой, ошибка программной среды, иное.)?

16. Какова последовательность изменений в программном обеспечении?

17. Какова история использования программного обеспечения с момента его установки (либо за определённый промежуток времени)?

Вопросы, относящиеся к данным (компьютерной информации) и решаемые с использованием методик про-

изводства КТЭ, направленных на решение диагностических задач

1. Каким образом было выполнено форматирование объекта? В каком виде записаны данные на него?

2. Какие характеристики имеет физическое размещение данных на представленном на экспертизе объекте?

3. Каковы характеристики логического размещения данных на объекте, представленном на экспертизу?

4. Каковы характеристики, свойства, параметры данных, содержащихся на объекте, представленном на экспертизу?

5. Каков вид информации на объекте, представленном на экспертизу (явный, скрытый, удалённый)?

6. Каков тип доступа к информации на объекте, представленном на экспертизу, (свободный, ограниченный и пр.) и каковы его характеристики?

7. Каковы свойства и параметры средств защиты информации, каковы возможные пути их преодоления?

8. Какие признаки преодоления защиты содержатся на объекте, представленном на экспертизу?

9. Каково содержание защищенной/зашифрованной информации?

10. Каким образом выполнено действие (указывается какое)?

11. Какова последовательность действий по выполнению конкретной задачи? Каковы признаки ее выполнения?

12. Имеется ли зависимость (связь) между действиями (указывается перечень действий) и событием (указывается событие)?

Вопросы, относящиеся к вычислительным сетям и их элементам и решаемые с использованием методик производства КТЭ, направленных на решение диагностических задач

1. Каковы свойства и характеристики аппаратного средства и программного обеспечения?

2. Каковы место, роль и функциональные предназначения исследуемого объекта в сети?

3. Каковы свойства и характеристики вычислительной сети, ее архитектура, конфигурация?

4. Какова организацию доступа к данным?

5. Каково фактическое состояния сетевого средства, имеется ли наличие физических дефектов, каково состояние системного журнала, компонентов управления доступом?

6. Какова причина изменения свойств вычислительной сети?

7. Какова структура механизмов и обстоятельств события (указывается перечень) в сети?

Вопросы, относящиеся к аппаратным средствам и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач

1. Представленный на экспертизу объект относится ли к компьютерным средствам или их компонентам?

2. Каковы технические характеристики представленного на экспертизу объекта?

Вопросы, относящиеся к программным средствам и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач

1. К какому классу программного обеспечения относится представленный на экспертизу объект?

2. Относится ли представленный на экспертизу объект к классу (указывается класс)?

Вопросы, относящиеся к данным (компьютерной информации) и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач

1. Каков тип данных обнаруженных в результате производства экспертизы (графические, текстовые, данные ПЗУ, электронная таблица, запись пластиковой карты, база данных, мультимедиа и др.), с помощью какого программного обеспечения осуществляется работа с ними?

Вопросы, относящиеся к вычислительным сетям и их элементам и решаемые с использованием методик производства КТЭ, направленных на решение классификационных задач

1. К какому классу сетевых средств относится объект экспертизы?

2. К какой части программного обеспечения относится объект экспертизы (серверной или клиентской)?

Вопросы, относящиеся к аппаратным средствам и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач

1. Какое (указывается тип устройства, например «знакопечатающее») устройство было подключено к представленному на исследование системному блоку, каковы его модель, серийный номер и т. п.?

Вопросы, относящиеся к программным средствам и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач

1. Какова версия и наименование программного обеспечения?

2. Содержится ли на представленном на экспертизу объекте программное обеспечение, являющееся копией (название программы)? Идентифицирующей образец программы прилагается.

Вопросы, относящиеся к данным (компьютерной информации) и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач

1. Каковы данные с фактами и обстоятельствами по рассматриваемому делу, содержащиеся на представленном объекте?

2. Каковы пользовательские данные, содержащиеся на представленном на экспертизу объекте?

Вопросы, относящиеся к вычислительным сетям и их элементам и решаемые с использованием методик производства КТЭ, направленных на решение идентификационных задач

1. Идентифицировать отправителя электронного сообщения (к сообщению регламентируется).

2. Кем и каким образом была осуществлена транзакция денежных средств на сервисе (название сервиса, например «Сбербанк-онлайн»)?

ОГЛАВЛЕНИЕ

Адрес издательства в Интернет WWW.TECHBOOK.RU

Научное издание

Шелупанов Александр Александрович
Смолина Анна Равильевна

ФОРЕНЗИКА. ТЕОРИЯ И ПРАКТИКА РАССЛЕДОВАНИЯ КИБЕРПРЕСТУПЛЕНИЙ

Монография

Обложка художника В. Г. Ситникова
Редактор Ю. Н. Чернышов
Компьютерная верстка Ю. Н. Чернышова

Подписано в печать 07.11.2018. Печать цифровая. Формат 60×88/16.
Уч. изд. л. 6,5. Тираж 500 экз. (5-й завод – 50 экз.) Изд. № 180769
ООО «Научно-техническое издательство «Горячая линия – Телеком»