На правах рукописи

Смолина Анна Равильевна

МЕТОДИЧЕСКОЕ И АЛГОРИТМИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОИЗВОДСТВА КОМПЬЮТЕРНО-ТЕХНИЧЕСКОЙ ЭКСПЕРТИЗЫ

Специальность:
05.13.19 – Методы и системы защиты информации,
информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Томск – 2017

Работа выполнена в Федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники»

Научный руководитель: Шелупанов Александр Александрович,
доктор технических наук, профессор

Официальные оппоненты: Громов Юрий Юрьевич,
доктор технических наук, профессор,
директор института автоматики и
информационных технологий Тамбовского
государственного технического университета

Пестунова Тамара Михайловна,
кандидат технических наук, доцент,
заведующая кафедрой информационной
безопасности Новосибирского
государственного университета экономики
и управления

Ведущая организация: Федеральное государственное казенное
образовательное учреждение высшего
образования «Воронежский институт
Министерства внутренних дел Российской
Федерации»

Защита состоится «26» октября 2017 г. в 15-15 часов на заседании диссертационного совета Д 212.268.03 при Томском государственном университете систем управления и радиоэлектроники (ТУСУР) по адресу: 634050, г.Томск, пр. Ленина 40, ауд. 201.

С диссертацией можно ознакомиться в библиотеке ТУСУРа по адресу: 634045, г. Томск, ул. Красноармейская, 146 и на сайте
https://storage.tusur.ru/files/62759/Dissertaciya_Smolina.pdf

Автореферат разослан «___ » _____ 2017 г.

Ученый секретарь
диссертационного совета Зыков Дмитрий Дмитриевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертации

В настоящее время киберпреступления (преступления, связанные с компьютерной информацией) занимают одно из лидирующих положений по количеству совершенных преступлений и сумме ущерба, принесенного юридическим и физическим лицам. Так, согласно данным информационного ресурса Ведомости, только за 2014 год правоохранительными органами было зарегистрировано 11 000 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.

Киберпреступления имеют высокую степень латентности (скрытности) – большая часть преступлений остается даже не зарегистрированной. 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 вопросы, требующие специальных познаний в области форензики (компьютерной криминалистики) – знаний о методах поиска, закрепления и исследования цифровых доказательств по киберпреступлениям.

Производство КТЭ и использование ее результатов является неотъемлемой частью 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.

Весомый вклад в развитие этого направления работ внесли Е.Р. Россинская, А.И. Усов, А.А. Шелупанов, К. Мандиа, К. Проспис, сотрудники компании «Group-IB», «Лаборатории Касперского», Томского государственного университета систем управления и радиоэлектроники, а также многие другие.

В настоящее время темпы развития науки и техники в области компьютерной криминалистики значительно опережают появление экспертного методического обеспечения. В результате расследование киберпреступлений и производство экспертиз по ним осложняется тем, что с постоянным развитием информационных технологий появляются объекты исследования, которых ранее просто не было, постоянно изменяются, модифицируются механизмы и методы совершения ранее известных видов преступлений, появляются абсолютно новые виды преступлений. Экспертам компьютерно-технической экспертизы для дачи полного, достоверного, научно обоснованного заключения необходимо постоянное повышение квалификации, совершенствование навыков, обновление имеющихся знаний

и использование соответствующей настоящему времени методической литературы. Это одно из отличий компьютерно-технической экспертизы от многих видов традиционной экспертизы (например: почерковедческой), где для дачи полного, достоверного, научно обоснованного заключения возможно использование методического обеспечения (экспертных методик) двадцатилетней давности, что неприменимо для компьютерно-технической экспертизы.

Под экспертной методикой принято понимать совокупность методов, используемых при производстве экспертизы. При использовании устаревшей методики возможно увеличение сроков производства экспертизы, ее стоимости, трудозатрат, а также получение недостоверных результатов и заключения, не пригодного в качестве доказательства.

В связи с вышеописанным, актуальна автоматизация и упрощение процесса разработки частных методик КТЭ. Для этого необходимо:

– формализовать методику производства КТЭ для дальнейшей разработки алгоритмического обеспечения производства КТЭ;

– классифицировать методики производства КТЭ (по критериям: категории задач, вопросы экспертизы, объекты исследования);

– определить подход, позволяющий получить, в рамках классифицированной методики, последовательность методов для каждой из стадии экспертизы, эффективную по заданному критерию ресурса (например: временные ресурсы, финансовые ресурсы, человеческие ресурс и т.д.).

Наличие алгоритмического обеспечения производства КТЭ позволит сократить количество 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 № 646), к одному из основных направлений обеспечения информационной безопасности в области государственной и общественной безопасности относится «повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям».

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 существующих средств защиты информации и обеспечения информационной безопасности.

Таким образом, разработка методики и алгоритмов производства компьютерно-технической экспертизы является актуальной задачей, решение которой будет способствовать обеспечению информационной безопасности объектов различных сфер деятельности (в т.ч. политической, оборонной,

социально-экономической и культурной сфер и т.д.) от внешних и внутренних угроз хищения/разрушения/модификации информации.

Целью диссертационного исследования является разработка методического и алгоритмического обеспечения производства компьютерно-технической экспертизы, применимого для решения широкого круга вопросов для производства экспертиз в соответствии с текущими требованиями законодательства.

Для достижения указанной цели в диссертационной работе поставлены и решены следующие **задачи**:

1) выполнены анализ требований законодательства к производству экспертизы в целом и компьютерно-технической, компьютерной в частности и исследование существующей методической базы, используемой при производстве КТЭ;

2) проведена классификация методик КТЭ с точки зрения задач исследования, целей исследования (вопросов экспертизы) и объектов исследования;

3) в соответствии с проведенной классификацией построена формальная модель методики производства КТЭ;

4) на основе формальной модели определен подход, позволяющий получить последовательность методов для каждой из стадии экспертизы, эффективную по заданному критерию (например: временные ресурсы, финансовые ресурсы, человеческие ресурсы и т.д.);

5) в рамках сформированного подхода к проведению судебной экспертизы предложена методика производства КТЭ с учетом требований возможности дальнейшей автоматизации;

6) для всех стадий экспертизы предложенной методики КТЭ разработано алгоритмическое обеспечение, предназначенное для решения наиболее востребованных частных задач КТЭ.

Объектом исследования является производство компьютерно-технической экспертизы, назначаемой для ответа на вопросы, связанные с расследованием компьютерных преступлений.

Предметом исследования являются частные методы и методики производства КТЭ, модели компьютерных преступлений и средства их расследования.

В качестве основных методов исследования применялись методы теории множеств, системного анализа, теории защиты информации и теории графов.

Научная новизна проведенных исследований и полученных в работе результатов заключается в следующем:

1. Впервые создана модель методики производства КТЭ для существующих требований законодательства, учитывающая тип методики КТЭ.

2. Предложена оригинальная классификация методик производства КТЭ, основанная на выявлении задач, целей и объектов КТЭ, отличающаяся от существующих детализацией элементов методики и минимизацией времени поиска необходимых методов исследования.

3. Решена задача выбора методов и разработки пошагового алгоритма производства КТЭ, эффективных по заданному критерию ресурса.

4. Создано методическое обеспечение производства КТЭ, содержащее рекомендации по применению экспертного инструментария для различных видов КТЭ и предполагающее использование предложенного алгоритмического обеспечения производства КТЭ.

Как выше было сказано, производство КТЭ является инструментом противодействия правонарушениям, совершаемым с использованием информационных технологий. Таким образом, работа соответствует п. 12 («Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления») и п. 13 («Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности») паспорта специальности 05.13.19.

Пункты научной новизны отражены в публикациях, указанных в разделе автореферата «*Основные положения диссертационной работы отражены в следующих публикациях*» под номерами:

– п. 1 в публикациях, указанных под №№ 1, 4;
– п. 2 в публикациях, указанных под №№ 3, 4;
– п. 3 в публикации, указанной под № 4;
– п. 4 в публикациях, указанных под №№ 2, 5-11.

Основными положениями, выносимыми на защиту, являются:

1. Модель методики производства КТЭ для существующих требований законодательства, учитывающая тип методики КТЭ, позволяющая ускорить и упростить поиск методики производства КТЭ, а также автоматизировать его.

2. Оригинальная классификация методик производства КТЭ, основанная на выявлении задач, целей и объектов КТЭ, отличающаяся от существующих детализацией элементов методики и позволяющая уменьшить время поиска необходимых методов исследования.

3. Решение задачи выбора методов и разработки пошагового алгоритма производства КТЭ, позволяющее разработать эффективную по заданному критерию методику.

4. Методическое обеспечение производства КТЭ, содержащее рекомендации по применению экспертного инструментария и предполагающее использование предложенного алгоритмического обеспечения производства КТЭ, позволяющее проведение различных видов КТЭ.

Обоснованность и достоверность результатов работы подтверждает положительный эффект, полученный в результате ее внедрения в практику

работы экспертных учреждений, о чем свидетельствуют соответствующие Акты о внедрении.

Практическая значимость диссертационной работы:

1. Предложенный подход, основанный на использовании модели методики производства КТЭ, позволяет ускорить и упростить поиск методики производства КТЭ на 20-40% (относительно общепринятой методики) и автоматизировать этот процесс.
2. Оригинальная классификация методик производства КТЭ позволяет сократить время эксперта на поиск необходимых методов исследования при производстве экспертизы.
3. Предложенное решение задачи выбора методов и разработки пошаговых алгоритмов производства КТЭ позволяет: разработать эффективную по заданному критерию методику (временные ресурсы, финансовые ресурсы, человеческие ресурсы и т.д.); сократить стоимость производства КТЭ на 10-30% (относительно общепринятой методики); сократить сроки производства КТЭ на 10-25% (относительно общепринятой методики).
4. Методическое обеспечение производства КТЭ, содержащее рекомендации по применению экспертного инструментария и предполагающее использование предложенного алгоритмического обеспечения производства КТЭ, применимо для различных видов КТЭ.

Личный вклад. Совместно с научным руководителем, д.т.н., профессором А.А. Шелупановым, осуществлялась постановка задач исследований. Положения, выносимые на защиту, получены автором лично. Автору принадлежит определяющая роль в результатах, использованных в диссертационной работе.

Апробация результатов работы. На заседаниях кафедры Комплексной информационной безопасности электронно-вычислительных систем ТУСУР, а также конференциях и семинарах, перечисленных ниже, были доложены и обсуждались основные практические и научные результаты диссертационной работы:

1) Всероссийские научно-технические конференции студентов, аспирантов и молодых ученых «Научная сессия ТУСУР», г. Томск, 2013-2016 гг.
2) Томские – IEEE семинары «Интеллектуальные системы моделирования, проектирования и управления», г. Томск, 2013-2016 гг.
3) Международный Конгресс по интеллектуальным системам и информационным технологиям «IS&IT'15», г. Таганрог, 2015 г.
4) Международная научно-техническая конференция «Динамика систем, механизмов и машин», г. Омск, 2014 г.
5) VI Пленум СибРОУМО по образованию в области информационной безопасности и XV конференция «Проблемы информационной безопасности государства, общества и личности», г. Иркутск, 2014 г.

6) II Международная научно-практической конференции «Судебная экспертиза: российский и международный опыт», г. Волгоград, 2014 г.

Реализация результатов диссертационной работы. Результаты диссертационной работы внедрены в деятельность организаций ООО «Независимая экспертиза и оценка» (г. Томск) и ООО «Томский экспертно-правовой центр «Регион 70» (г. Томск), а также в учебный процесс ТУСУРа.

Публикации. Результаты диссертационной работы отражены в 11 публикациях, в том числе 4 публикации в рецензируемых журналах из перечня ВАК.

Структура и объем диссертационной работы. Диссертация состоит из введения, четырех глав, заключения, списка литературы из 119 наименований, 2 приложений. Общий объем работы составляет 132 страницы, в том числе 13 рисунков и 3 таблицы.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении показана актуальность темы диссертации, сформированы цели и задачи исследования, представлены основные научные результаты, определены их научная новизна и практическая значимость, приведено краткое содержание по главам.

В первой главе исследуется текущее состояние компьютерно-технической экспертизы:

1) определяются основные понятия судебной экспертизы;

2) 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);

3) определяется понятие экспертной методики;

4) рассматриваются требования, предъявляемые законодательством к методике (и методам) производства экспертизы;

5) проводится анализ существующих методик производства КТЭ.

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

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

Таким образом, в результате работы, изложенной в первой главе диссертации, для ускорения, упрощения поиска методики производства КТЭ и обеспечения возможности автоматизации этого процесса определены задачи, которые решались и излагались в следующих главах диссертации:

1) проведение классификации методик КТЭ с точки зрения задач исследования, целей исследования (вопросов экспертизы) и объектов исследования;

2) в соответствии с проведенной классификацией построена формальная модель методики производства КТЭ;

3) на основе формальной модели определен подход, позволяющий получить последовательность методов для каждой из стадии экспертизы, эффективную по заданному критерию (например: временные ресурсы, финансовые ресурсы, человеческие ресурсы и т.д.);

4) в рамках сформированного подхода к проведению судебной экспертизы предложена методика производства КТЭ с учетом требований возможности дальнейшей автоматизации;

5) для всех стадий экспертизы предложенной методики КТЭ разработано алгоритмическое обеспечение, предназначенное для решения наиболее востребованных частных задач КТЭ.

Во второй главе предлагается подход, позволяющий упростить процесс поиска методики производства КТЭ и обеспечить возможность автоматизации этого процесса. В рамках него проводится формализация критериев классификации методик КТЭ, разработана модель методики производства КТЭ, определен подход для выбора методов производства КТЭ и определения сроков производства комплексной экспертизы.

Были выявлены общие свойства методик КТЭ и сформированы основные критерии и признаки для их классификации. Процесс классификации по базовым критериям описан в виде ориентированного графа (рис. 1), с описанием множеств его вершин и дуг. Критерии классификации разделены на три уровня, определяющих свойства методик КТЭ. Были определены 12 обобщенных типовых методик производства КТЭ.

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 A из вершины b_0 в вершину b_e, где:

1) i – порядковый номер типа методики в предложенной классификации типов методик, $1 \le i \le 12$;

2) j – тип объекта (табл. 1).

В соответствии с разработанной классификацией методик КТЭ и на основании проанализированных методических документов был описан полный перечень возможных основных вопросов КТЭ.

Разработана модель методики производства КТЭ, построенная на алгоритмическом применении методов КТЭ множества S, представляющего собой подмножество декартового произведения множеств методов стадий экспертного исследования. Предложенная модель методики производства КТЭ необходима для разработки общих, частных и конкретных методик, относящихся к любому типу методик КТЭ, в том числе и по предложенной классификации методик.

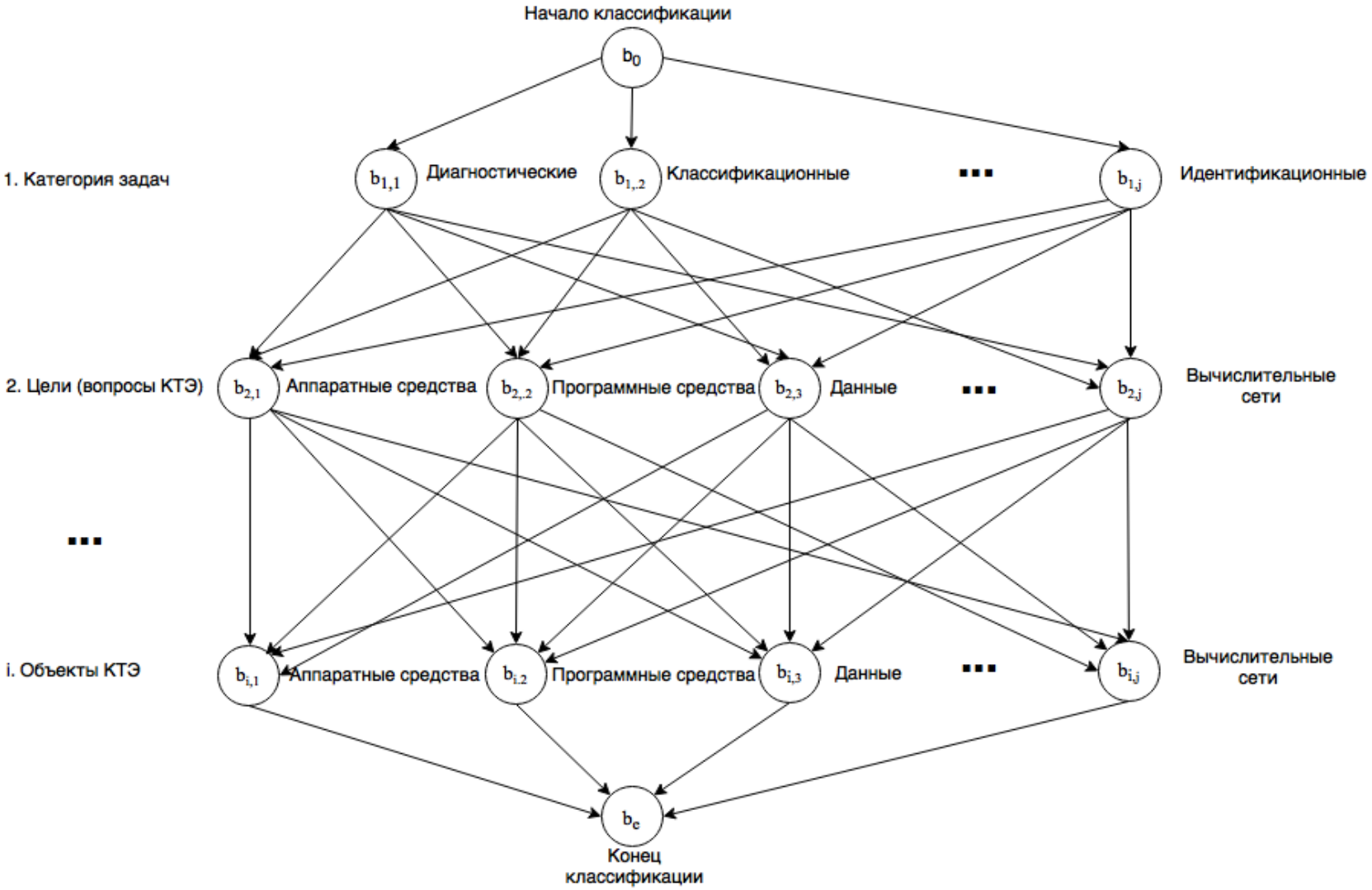

Рис. 1. Предлагаемый граф классификации методик производства КТЭ

Таблица 1. Множество *M* типов методик КТЭ

Тип методики КТЭ	Значение
$m_1=<b_{1,1}, b_{2,1}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к аппаратным средствам
$m_2=<b_{1,1}, b_{2,2}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к программным средствам
$m_3=<b_{1,1}, b_{2,3}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации)
$m_4=<b_{1,1}, b_{2,4}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение диагностических задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам
$m_5=<b_{1,2}, b_{2,1}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к аппаратным средствам
$m_6=<b_{1,2}, b_{2,2}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к программным средствам
$m_7=<b_{1,2}, b_{2,3}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации)
$m_8=<b_{1,2}, b_{2,4}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение классификационных задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам
$m_9=<b_{1,3}, b_{2,1}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к аппаратным средствам
$m_{10}=<b_{1,3}, b_{2,2}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к программным средствам
$m_{11}=<b_{1,3}, b_{2,3}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к данным (компьютерной информации)
$m_{12}=<b_{1,3}, b_{2,4}, b_{3,j}>$, $j \in \{1, 2, 3, 4\}$	Методики производства КТЭ, направленные на решение идентификационных задач, с целью ответа на вопросы, относящиеся к вычислительным сетям и их элементам

Автор предлагает унифицировать методику производства КТЭ, представив элементы методики КТЭ в виде множеств:

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

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

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

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

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

$H = \{h_1, h_2, \ldots, h_t\}$ – множество методов стадии формирования выводов, где j – количество методов стадии формирования выводов.

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

$$s_n \in S = (d_l, v_w, g_u, e_q, f_p, h_t), \quad (1)$$

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.

Предложенная модель методики производства КТЭ может быть использована для разработки общих, частных и конкретных методик, относящихся к любому типу методик КТЭ, согласно предложенной автором классификации. Этот процесс может быть автоматизирован. Контекстная диаграмма процедуры определения методики производства КТЭ представлена на рисунке 2.

В этой же главе диссертации был описан высокоуровневый алгоритм производства КТЭ – последовательность стадий производства экспертизы.

Рис. 2. IDEF0 диаграмма процесса определения методики 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. диссертации). 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 автором предлагается выбирать метод, с учетом наличия ресурсов в экспертной организации (финансовых, временных, человеческих и т.д.). Так, поиск методов автором предлагается выполнить, обратившись к теории графов, и решить данную задачу, как типовую задачу теории графов – задачу о поиске кратчайшего пути.

Описание поиска методов КТЭ выполним с помощью ориентированного графа *RR (R, RE)*, где:

1) $R = \{r_0, r_{1,1}, r_{1,2} \ldots, r_{i,j}, r_e\}$ – множество вершин графа *RR*;

2) *RE* – множество дуг d_{ij} графа *RR*, упорядоченных пар вершин $r \in R$. каждой дуге *RE* сопоставлен вес k_{ij};

3) вершина r_0 – начало производства КТЭ;

4) вершина r_e – завершение производства КТЭ;

5) вершина r_{ij} – метод этапа одной из стадий производства КТЭ;

6) i – количество альтернативных методов на определенном этапе стадий производства КТЭ, $i \geq 1$;

7) j – количество этапов стадий производства КТЭ, $j \geq 1$;

8) k_{ij} – вес дуги, обозначает длину дуги – неотрицательное число, характеризующее затраты ресурса (количество затрачиваемого времени, либо необходимое количество экспертов, либо финансовые затраты), по которому проводится определение методов.

Частный случай графа поиска методов КТЭ в рамках выбранной методики представлен ниже на рисунке.

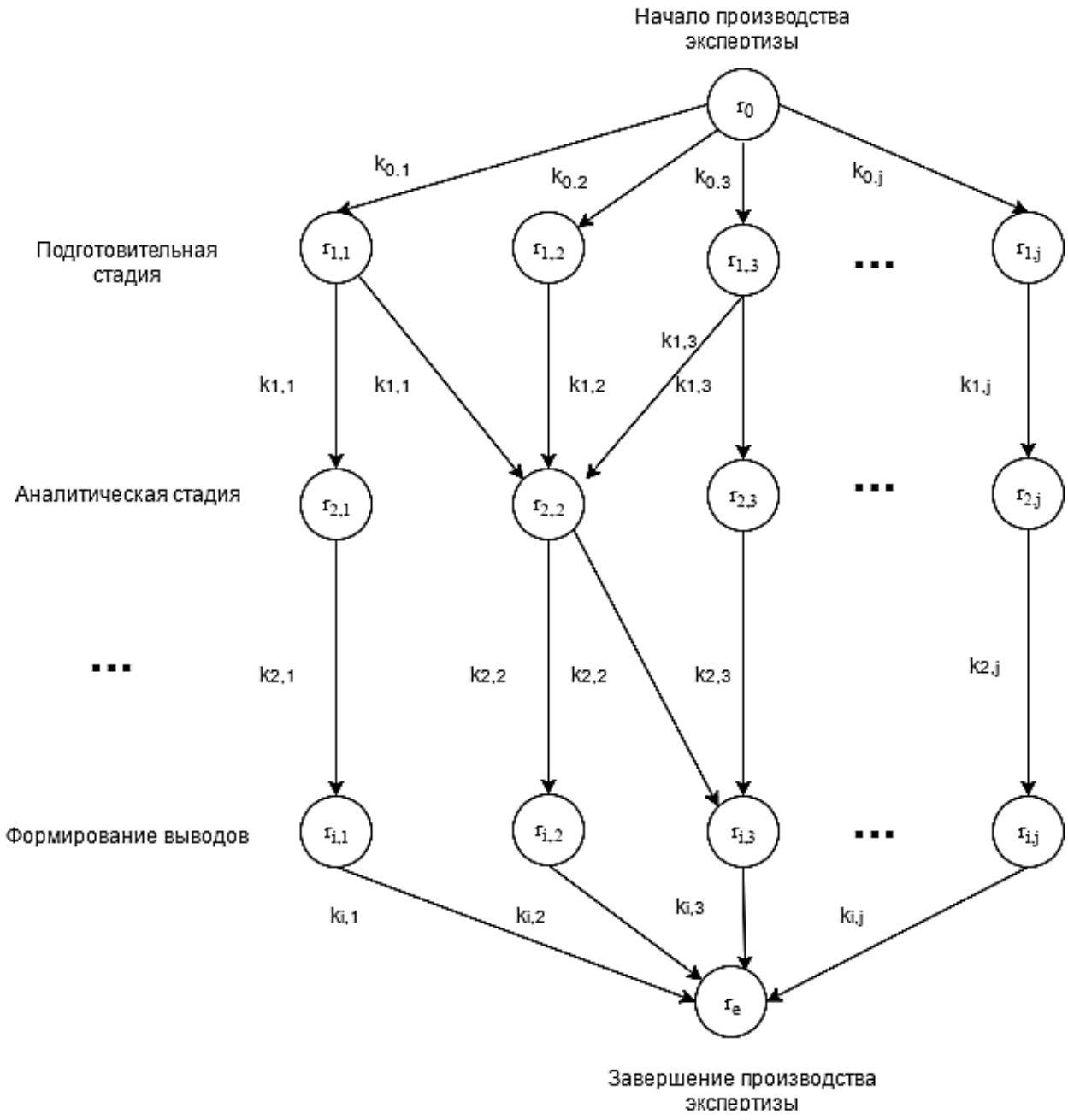

Рис. 3. Частный случай графа поиска методов производства КТЭ

Для решения этой задачи предлагается использование классического алгоритма решения задачи о поиске кратчайшего пути на графе – алгоритм Дейкстры. Алгоритм Дейкстры основан на следующем тезисе Декстры: если кратчайший путь проходит через вершину r_{ij}, то длина части пути от r_o до r_{ij} должна быть минимально возможной.

Контекстная IDEF0-диаграмма процесса формирования частной методики, эффективной по заданному ресурсному критерию, представлена на рисунке ниже. Входными данными является решение о составе и последовательности методов методики, полученное выше (см. рисунок 2.). Т.к. в рамках работы не предусмотрена разработка программного обеспечения 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 методов частной методики.

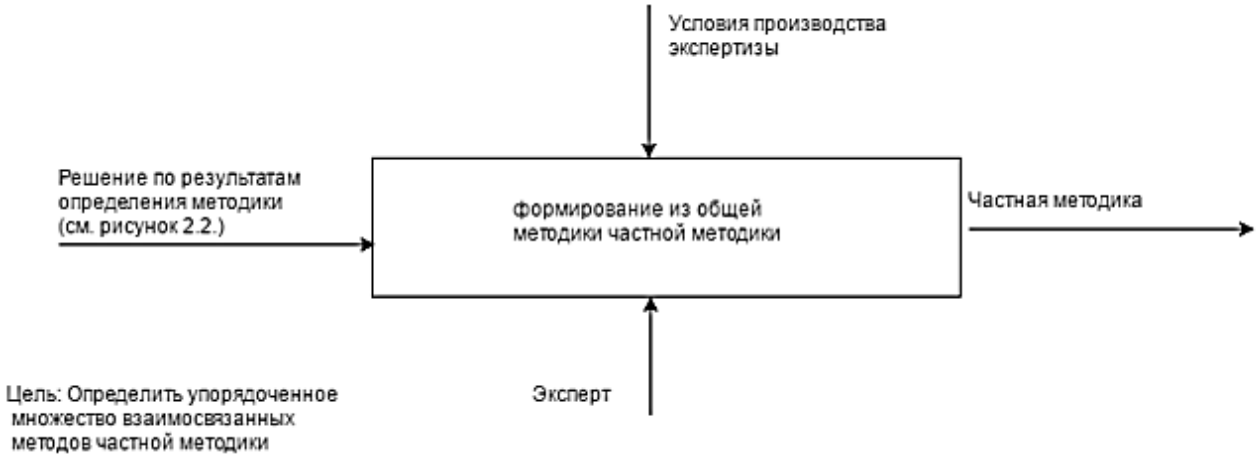

Рис. 4. IDEF0 диаграмма процесса формирования частной методики, эффективной по заданному ресурсному критерию.

Для решения задачи оценки трудозатрат при производстве КТЭ в составе комплексной экспертизы автором предложено использование методологии PERT (Project Evaluation and Review Technique) - построение сетевой диаграммы PERT. В зависимости от объектов, задач и вопросов комплексной экспертизы, вид сетевой диаграммы изменяется. Ниже представлена сетевая диаграмма оценки трудозатрат для частного случая - производства комплексной экспертизы, вопросами которой являются:

– 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:

1) подписка об уголовной ответственности (подготовительная стадия)

2) результаты подготовительная стадия: t_0 – время проведения подготовительной стадии всеми экспертами комплексной экспертизы;

3) предварительные выводы по первому вопросу: t_1 – время проведение исследования экспертом КТЭ по первому вопросу экспертизы;

4) предварительные выводы по второму вопросу эксперта видео-, фототехнической экспертизы: t_2 – время проведения исследования по второму вопросу экспертом видео-, фототехнической экспертизы;

5) предварительные выводы по второму вопросу эксперта искусствоведческой экспертизы: t_3 – время проведения исследования по второму вопросу экспертом искусствоведческой экспертизы;

6) предварительные выводы по второму вопросу эксперта-психолога: t_4 – время проведения исследования по второму вопросу экспертом экспертом-психологом;

7) общие выводы по второму вопросу: t_5 – время формирования общих выводов по второму вопросу;

8) предварительные выводы по третьему вопросу: t_6 – время проведение исследования экспертом КТЭ по третьему вопросу экспертизы;

9) 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.

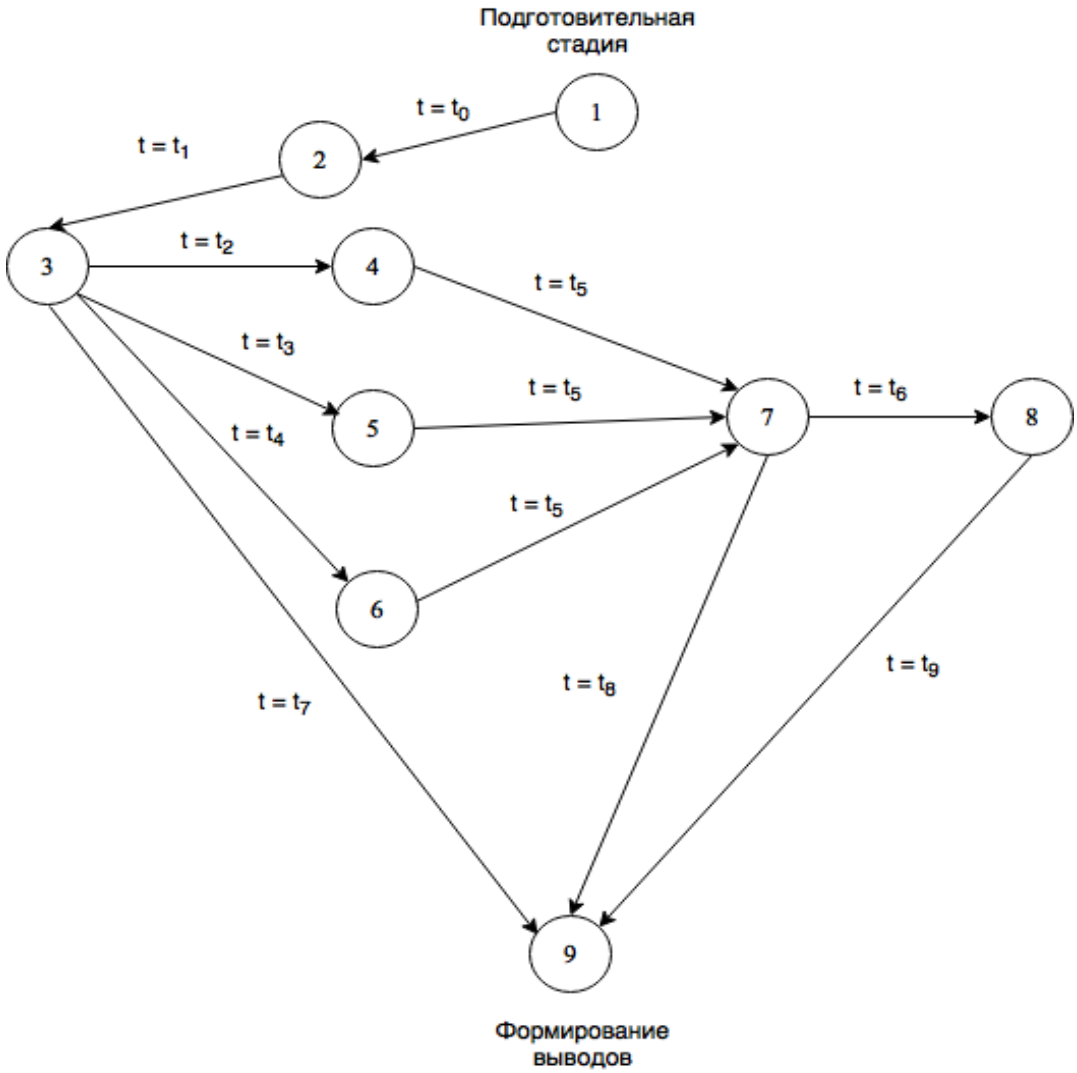

Рис. 5. Частный случай сетевой диаграммы PERT (производство комплексной экспертизы)

Таким образом, в рамках исследования, изложенного в данной главе, решен ряд задач, обозначенных в первой главе:

– проведена классификация методик КТЭ с точки зрения задач исследования, целей исследования (вопросов экспертизы) и объектов исследования;

– в соответствии с проведенной классификацией построена формальная модель методики производства КТЭ;

– на основе формальной модели определен подход, позволяющий получить последовательность методов для каждой из стадии экспертизы, эффективную по заданному критерию (например: временные ресурсы, финансовые ресурсы, человеческие ресурсы и т.д.);

– также, определен подход для предметной области КТЭ, позволивший решать задачу оценки трудозатрат при производстве КТЭ в составе комплексной экспертизы.

Указанные результаты использованы при разработке методического и алгоритмического обеспечения производства КТЭ, описание которого содержится в следующей главе.

В третьей главе содержится описание разработанного автором методического и алгоритмического обеспечения производства КТЭ.

Разработанное методическое обеспечение производства КТЭ, разработанная методика, является унифицированной, т.к. применима для решения широкого круга частных задач, среди которых есть и диагностические, и классификационные, и идентификационные задачи.

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

В данной главе описана последовательность действий и методов для каждой из стадий производства КТЭ. Описана структура заключения эксперта о результатах производства КТЭ.

Методическое обеспечение предполагает использование пошагового алгоритма производства КТЭ. В тексте диссертации он представлен в виде IDEF0-диаграмм, для каждой стадии производства КТЭ:

– Подготовительной стадии;
– Аналитической стадии;
– Эксперимента;
– Синтезирующей стадии;
– Результативной стадии;
– Стадии формирования выводов.

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

В настоящее время 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, т.к. большое значение в таком подходе играет опыт эксперта. При этом сам подход является допустимым судом для производства КТЭ.

Наиболее опытные эксперты используют комплексный подход, добиваясь на нем большей эффективности. Потому сравнение разработанной методики было выполнено с ним.

Разработанное автором методика по сравнению с комплексным подходом позволяет добиться выигрыша по следующей группе критериев, гарантируя получение экспертом даже 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%.

Заключения экспертов (более 70), выполненные автором и экспертными организациями (где было осуществлено внедрение) в соответствии с разработанной методикой в период с 2010 по 2015 год, не получили ни одного отклонения в суде при оценке их на допустимость.

По заключениям, выполненным в соответствии с разработанной методикой, не было назначено повторных или дополнительных экспертиз.

Таким образом, в данной главе излагается методическое и алгоритмическое обеспечения производства КТЭ.

Разработанное методическое и алгоритмическое обеспечение КТЭ может быть использовано для автоматизации и упрощения процесса разработки частных методик производства КТЭ путем разработки системы поддержки формирования частных методик производства компьютерно-технических экспертиз.

Четвертая глава посвящена внедрению и апробации полученных результатов.

Внедрение продемонстрировано для каждого из четырех видов компьютерно-технической экспертизы (аппаратно-компьютерной, программно-компьютерной, информационно-компьютерной и компьютерно-сетевой).

Разработанная методика была внедрена в деятельность двух экспертных организаций ООО «Независимая экспертиза и оценка» (г. Томск) и ООО «Томский экспертно-правовой центр «Регион 70» (г. Томск). Результаты диссертационной работы также внедрены в учебный процесс ТУСУРа. Внедрение подтверждается соответствующими Актами.

В ООО «Томский экспертно-правовой центр «Регион 70» внедрение результатов диссертационного исследования позволило:

– сократить затраты на проведение экспертиз до 20%;

– увеличить количество проводимых экспертиз до 25%;

– снизить требования к квалификации экспертов КТЭ (за счет использования разработанного методического и алгоритмического обеспечения производства КТЭ).

В ООО «Независимая экспертиза и оценка» внедрение результатов диссертационного исследования позволило получить:

– сокращение сроков производства КТЭ до 15%;

– сокращение сроков определения необходимой методики производства КТЭ до 38%;

– сокращение сроков подготовительной стадии производства КТЭ до 25%;

– уменьшение затрат на производство экспертизы до 22%.

Расчетные значения критериев выигрыша использования разработанной методики по сравнению с комплексным подходом, полученные автором на основании выборки в 50 экспертиз (п. 3.8. диссертации), находятся в диапазоне значений результатов внедрения диссертационного исследования в деятельность экспертных организаций.

Результаты внедрения подтверждаются соответствующими Актами внедрения (см. Приложение 2 диссертации) и демонстрируют выигрыш использования разработанной методики по сравнению с комплексным подходом.

Перспективой развития данного диссертационного исследования является создание системы, позволяющей автоматизировать формирование частных методик производства компьютерно-технических экспертиз.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ ДИССЕРТАЦИОННОЙ РАБОТЫ

1. Впервые создана модель методики производства КТЭ для существующих требований законодательства, учитывающая тип методики КТЭ.

2. Предложена оригинальная классификация методик производства КТЭ, основанная на выявлении задач, целей и объектов КТЭ, отличающаяся от существующих детализацией элементов методики и минимизацией времени поиска необходимых методов исследования.

3. Решена задача выбора методов и разработки пошагового алгоритма производства КТЭ, эффективных по заданному критерию ресурса.

4. Создано методическое обеспечение производства КТЭ, содержащее рекомендации по применению экспертного инструментария для различных видов КТЭ и предполагающее использование предложенного алгоритмического обеспечения производства КТЭ.

Результаты диссертационной работы внедрены в деятельность организаций ООО «Независимая экспертиза и оценка» (г. Томск); ООО «Томский экспертно-правовой центр «Регион 70» (г. Томск), а также в учебный процесс ТУСУРа.

ОСНОВНЫЕ ПОЛОЖЕНИЯ ДИССЕРТАЦИОННОЙ РАБОТЫ ОТРАЖЕНЫ В СЛЕДУЮЩИХ ПУБЛИКАЦИЯХ

Статьи в ведущих рецензируемых журналах, рекомендованных Высшей аттестационной комиссией (ВАК) для публикации результатов кандидатских и докторских диссертационных работ:

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

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

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

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

В других изданиях, сборниках трудов и тезисов конференций:

5. Смолина А.Р. Решение задачи определения интернет-активности пользователя при производстве компьютерно-технической экспертизы [Электронный ресурс] / А.Р. Смолина // 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 частях. – Ч. 5. – С. 26-29. – Режим доступа: https://storage.tusur.ru/files/44767/2016_5.pdf .

6. Смолина А.Р. Результаты анализа методик производства компьютерно-технической экспертизы [Электронный ресурс] / А.Р. Смолина // 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 частях. – Ч. 5. – С. 96-99. – Режим доступа: https://storage.tusur.ru/files/44767/2016_5.pdf .

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

8. Смолина А.Р. Проблемы методического обеспечения компьютерно-технической экспертизы / А.Р. Смолина // Материалы Международной научно-технической конференции «Динамика систем, механизмов и машин» - Омск: Издательство: Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Омский государственный технический университет» – 2014. – № 4 – С. 96-98.

9. Смолина А.Р. Компьютерно-техническая экспертиза в условиях ограниченного бюджета / А.Р. Смолина // 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. – 2014. – С. 183-190.

10. Смолина А.Р. Проблемы поиска данных на носителях информации при производстве компьютерно-технических экспертиз / А.Р. Смолина // 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.

11. Смолина А.Р. Программные способы восстановления удаленной информации при расследовании компьютерных преступлений [Электронный ресурс] / А.Р. Смолина // 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 частях. – Ч. 4. – С. 232-233. – Режим доступа: https://storage.tusur.ru/files/43229/2013_4.pdf

Заказ . Тираж 100 экз.

Томский государственный университет
систем управления и радиоэлектроники

634050, г. Томск, пр. Ленина, 40.

Тел. (3822) 533018.