УТВЕРЖДАЮ
Начальник Воронежского
института МВД России
кандидат философских наук
генерал-майор полиции

А.П. Нахимов
«04» октября 2017 г.

ОТЗЫВ

ведущей организации федерального государственного казенного образовательного учреждения высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации» на диссертацию Смолиной Анны Равильевны на тему «Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы», представленную на соискание ученой степени кандидата технических наук по специальности 05.13.19 – методы и системы защиты информации, информационная безопасность

1. Структура и объем диссертации

Диссертационная работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Томский государственный университет систем управления и радиоэлектроники». Объем работы составляет 132 страницы машинописного текста, в том числе 13 рисунков, 3 таблицы и список литературы, состоящий из 119 наименований. Диссертационное исследование состоит из введения, четырех глав, заключения, списка литературы и двух приложений.

Во введении обоснована актуальность темы, сформулированы цель и задачи, предмет и объект исследования, отражены его научная новизна и практическая значимость, приведены положения, выносимые на защиту, и информация об апробации работы и публикациях автора по теме диссертации.

Первая глава посвящена исследованию современного состояния исследуемой области и постановке задач, решаемых в последующих главах диссертации. В данной главе определяются основные понятия судебной экспертизы в целом и компьютерно-технической экспертизы в частности, исследуются требования, предъявляемые законодательными актами, к методам и методикам производства компьютерно-технической экспертизы, анализируются современные методики. Автор также исследует большое количество зарубежной и отечественной технической литературы, посвященной исследуемой предметной области, кандидатские диссертации,

связанные с производством компьютерно-технической экспертизы. В результате им сделаны выводы, используемые в процессе решения задач данного диссертационного исследования.

Во второй главе решается ряд задач, сформулированных в первой главе диссертации: 1) проведение классификации методик компьютерно-технической экспертизы с точки зрения задач исследования, целей исследования (вопросов экспертизы) и объектов исследования; 2) построение (в соответствии с проведенной классификацией) формальной модели методики производства компьютерно-технической экспертизы; 3) определение (на основе формальной модели) подхода, позволяющего получить последовательность применения методов для каждой из стадии экспертизы, эффективной по заданному критерию. Решение данных задач направлено на преодоление проблемы поиска методики производства компьютерно-технической экспертизы и выбора методов в рамках найденной методики, соответствующих потребностям экспертной организации. Автором был предложен унифицированный подход к классификации экспертных методик. Описание процесса классификации выполнено в виде ориентированного графа с описанием множеств его вершин и дуг. Критерии классификации разделены на три уровня, определяющие свойства методик компьютерно-технической экспертизы. Получено 48 типов методик. Предложенная модель методики производства компьютерно-технической экспертизы может быть использована для разработки общих, частных и конкретных методик, относящихся к любому типу такого рода методик. Процесс разработки методик может быть автоматизирован. Разработанный подход определения последовательности применения методов производства компьютерно-технической экспертизы представляет собой классификацию и выбор методики, соответствующей предмету экспертизы, с последующим формированием частной методики, эффективной по заданному ресурсному критерию. Для решения задачи оценки трудозатрат, связанных с производством компьютерно-технической экспертизы в составе комплексной экспертизы, автором предложено использование методологии PERT. Полученные результаты использованы при разработке методического и алгоритмического обеспечения производства компьютерно-технической экспертизы.

В третьей главе изложено описание разработанного автором методического и алгоритмического обеспечения производства компьютерно-технической экспертизы. Методическое обеспечение ориентировано на использование экспертами частных и государственных экспертных учреждений. В нем содержатся рекомендации по выполнению всех стадий экспертизы и применению частных инструментальных методов. При этом предполагается использование пошаговых алгоритмов для стадий производства компьютерно-технической экспертизы, разработанных автором

на основе анализа соответствующих графовых моделей, и представленных в виде IDEF0-диаграмм. При оценке эффективности разработанной методики автором производится ее сравнение с общепринятым в настоящее время подходом, предполагающим использование экспертом преимуществ различных методик для каждой конкретной экспертизы. В процессе исследования автором проведено более 50 экспертиз. Разработанная методика позволяет добиться получения гарантированного выигрыша экспертом практически любой квалификации при разработке экспертного заключения, соответствующего требованиям законодательства, по следующей группе критериев: время разработки частной методики компьютерно-технической экспертизы; сроки производства экспертизы; стоимость производства.

В четвертой главе показано внедрение разработанной методики в производственный процесс экспертного учреждения для каждого из четырех видов экспертиз: аппаратно-компьютерной, программно-компьютерной, информационно-компьютерной и компьютерно-сетевой. Внедрение результатов диссертационного исследования в деятельность экспертных организаций имело положительные результаты: сокращение затрат на производство экспертиз, увеличение количества экспертиз, повышение уровня подготовки экспертов, связанное со снижением требований к их квалификации.

В заключении приведены основные результаты и выводы по проделанной работе.

2. Актуальность темы диссертации

Компьютерно-техническая экспертиза является неотъемлемой частью расследования компьютерных преступлений и принятия судебных решений по ним. В рамках ее проведения решаются вопросы, имеющие ключевое значение в судебном процессе. Это определяет особую роль данного вида экспертизы в вопросах противодействия киберпреступности и деятельности по комплексному обеспечению информационной безопасности.

Кроме того, следует отметить быстрое старение методического обеспечения компьютерно-технической экспертизы, связанное с бурным развитием информационных технологий.

Указанные обстоятельства обуславливают актуальность темы диссертационного исследования Смолиной Анны Равильевны. Проведенное исследование направлено на создание нового подхода, позволяющего автоматизировать процесс разработки частных экспертных методик и не зависящего от появления новых объектов исследования и типов преступлений.

3. Научная новизна и практическая ценность результатов, полученных в диссертации

Полученные результаты диссертационного исследования являются новыми и могут быть классифицированы как изложение научно-обоснованных решений, внедрение которых внесет значительный вклад в науку и практику предотвращения и расследования компьютерных преступлений, обеспечения общественной безопасности Российской Федерации.

Наиболее важные результаты диссертационной работы, обладающие признаками научной новизны:

1. Впервые создана модель методики производства компьютерно-технической экспертизы для существующих требований законодательства, учитывающая ее тип.

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

3. Решена задача выбора методов и разработки пошагового алгоритма производства компьютерно-технической экспертизы, эффективных по заданному критерию ресурса.

4. Создано методическое обеспечение производства компьютерно-технической экспертизы, содержащее рекомендации по применению экспертного инструментария для различных ее видов и предполагающее использование предложенного алгоритмического обеспечения производства.

4. Обоснованность и достоверность полученных результатов и выводов диссертации

Цель диссертационного исследования и вытекающие из нее задачи изложены корректно, являются практически значимыми и реализуемыми. Решения задач исследования доведены до практических приложений. По приведенному списку литературы можно сделать вывод о полноте изучения диссертантом рассматриваемых вопросов.

Достоверность полученных Смолиной А.Р. результатов обеспечена строгостью применения методов исследования, согласованностью с результатами проведенных экспериментов и положительным эффектом, полученным в результате внедрения результатов работы в практическую деятельность экспертных организаций, о чем свидетельствуют соответствующие акты о внедрении.

5. Значимость результатов диссертации для развития соответствующей отрасли науки

Результаты диссертационной работы имеют несомненную значимость для развития науки в области информационной безопасности и защиты информации, что обосновывает их практическую значимость:

- предложенный подход, основанный на использовании модели методики производства компьютерно-технической экспертизы, позволяет ускорить и упростить поиск методики ее производства;
- оригинальная классификация методик производства компьютерно-технической экспертизы позволяет сократить время, затрачиваемое экспертом, на поиск необходимых методов исследования при производстве экспертизы;
- предложенное решение задачи выбора методов и разработки пошаговых алгоритмов производства компьютерно-технической экспертизы позволяет: разработать эффективную по заданному критерию методику; сократить стоимость производства компьютерно-технической экспертизы; сократить сроки производства компьютерно-технической экспертизы;
- методическое обеспечение производства компьютерно-технической экспертизы, содержащее рекомендации по применению экспертного инструментария и предполагающее использование предложенного алгоритмического обеспечения ее производства, применимо для различных видов компьютерно-технической экспертизы.

6. Рекомендации по использованию результатов диссертационной работы

1. Рекомендуется внедрение результатов диссертационного исследования в государственные экспертные организации.

2. Рекомендуется разработка программного обеспечения для поддержки формирования экспертных методик на основе результатов диссертационного исследования с возможностью его интеграции с существующими программными средствами поддержки производства компьютерно-технической экспертизы и судопроизводства.

7. Публикации, апробация и внедрение результатов диссертационной работы

Представленная диссертация выполнена с соблюдением требований, установленных ВАК при Министерстве образования и науки Российской Федерации. Стиль изложения соответствует требованиям к научным работам. Ссылки на библиографические источники и литературу, включая собственные публикации автора, оформлены в соответствии с требованиями.

Список литературы подчеркивает глубину изучения автором рассматриваемого в работе научного направления.

Научные и практические результаты диссертационной работы докладывались и обсуждались на конференциях и семинарах, в том числе международного уровня. Основные материалы диссертации отражены в 11 научных статьях автора, 4 из которых опубликованы в рецензируемых журналах из перечня ВАК при Министерстве образования и науки Российской Федерации.

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 ТУСУР.

8. Замечания по диссертации

1. В обзоре недостаточно внимания уделено рассмотрению программных средств поддержки производства компьютерно-технической экспертизы и судопроизводства.
2. Предложенная автором классификация (по объектам, целям, категориям задач экспертизы) не является единственно возможной. В диссертации не приведены преимущества предложенной классификации в сравнении с альтернативными, в частности, с классификацией по видам экспертизы.
3. Часть материалов, вынесенных в приложения, а именно перечень вопросов компьютерно-технической экспертизы, было бы полезно использовать в основном тексте диссертационной работы для иллюстрации ключевых ее положений.
4. Алгоритмическое обеспечение и диаграммы, представленные в диссертации на стр. 42, 49, поделены на блоки. Это затрудняет не только восприятие логики, но и не дает возможности оценить работу программы в целом. Было бы логичнее выстроить блок-схему в традиционном представлении.
5. В первом разделе третьей главы, содержащем описание результатов исследования границ применимости разработанного методического обеспечения, недостаточно полно представлены выводы по исследованию, что усложняет понимание области возможного применения.

9. Заключение

Диссертация Смолиной А.Р. является законченной научно-квалификационной работой, в которой на основании выполненных автором исследований решена научная задача, имеющая важное хозяйственное значение. Полученные результаты вносят определенный вклад в развитие

таких областей информационной безопасности, как формирование политики ее обеспечения информационной безопасности и совершенствование существующих средств защиты информации.

Диссертация отвечает требованиям «Положения о порядке присуждения ученых степеней» ВАК при Министерстве образования и науки Российской Федерации, утвержденного постановлением Правительства Российской Федерации № 842 от 24.09.2013 г., а ее автор, Смолина Анна Равильевна, заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв подготовлен профессором кафедры информационной безопасности Воронежского института МВД России доктором технических наук, профессором Авсентьевым Олегом Сергеевичем

Специальности д.т.н., профессора Авсентьева О.С.:

05.13.18 – Математическое моделирование, численные методы и комплексы программ;

05.13.19 – Методы и системы защиты информации, информационная безопасность.

Отзыв ведущей организации на диссертацию Смолиной А.Р. рассмотрен и одобрен на заседании кафедры информационной безопасности Воронежского института МВД России (протокол №2 от «19» сентября 2017 г.)

Начальник кафедры информационной безопасности
Федерального государственного казенного образовательного учреждения высшего образования «Воронежский институт Министерства внутренних дел Российской Федерации»,
кандидат технических наук, доцент Бабкин Александр Николаевич

«19» сентября 2017 г.

394065, г. Воронеж, пр. Патриотов, д. 53
тел.: (473) 200 52 36
e-mail: ib@vimvd.ru

Подпись Бабкина А.Н.
удостоверяю
начальник отделения
делопроизводства и режима
Воронежского института
МВД России
Е.М. Долгих