

ОТЗЫВ

официального оппонента на диссертацию Смолиной Анны Равильевны «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»

Актуальность темы диссертации

Несмотря на то, что специалистами, учеными, государственными и коммерческими организациями, занимающимися проблемами и задачами информационной безопасности, большое внимание уделяется вопросам противодействия киберпреступности, не решенным остается вопрос сокращения сроков производства компьютерно-технической экспертизы (при сохранении должного качества экспертных заключений, выданных даже экспертами низкой квалификации, в т.ч. начинающими экспертами). Во многом это обусловлено тем, что, разрабатывая методику для каждого конкретного случая, эксперт руководствуется только личным опытом, а средства, автоматизирующие этот процесс, отсутствуют, как и отсутствует единая методика, соответствующая современному состоянию развития науки и техники.

Работа Смолиной А.Р. посвящена разработке методического и алгоритмического обеспечения производства компьютерно-технической экспертизы (КТЭ). Работа направлена на ускорение и упрощение процесса разработки экспертами КТЭ частных экспертных методик, а также на автоматизацию этого процесса. Это, несомненно, имеет существенное значение для решения задач информационной безопасности, тема работы Смолиной А.Р. является актуальной.

Оценка структуры и содержания диссертации

Диссертация состоит из введения, четырех глав, заключения, двух приложений, а также списка литературы. Общий объем работы составляет 132 страницы, включая 13 рисунков и 3 таблицы. В целом работа имеет четкую логическую структуру.

Из положительных моментов можно отметить ясное изложение сути работы, ее результатов, а также хороший стиль и четкую логику. Автор хорошо владеет специальными терминами из рассматриваемой предметной области, имеет глубокие знания нормативных документов и законодательных актов, относящихся к теме работы.

Оформление диссертационной работы нареканий не вызывает.

Во введении дано обоснование актуальности темы диссертационной работы, поставлены цель и задачи исследования, перечислены основные полученные результаты, определена их практическая ценность.

В первой главе подробно рассмотрено текущее состояние компьютерно-технической экспертизы, в т.ч. вопросы экспертного методического обеспечения. Автор резюмирует изложенное и приходит к тому, что для ускорения, упрощения поиска методики производства КТЭ и обеспечения возможности автоматизации этого процесса необходимо решить ряд задач, решение которых он и излагает в последующих главах.

Вторая глава посвящена вопросам формализации, так, в этой главе разработана авторская классификация методик КТЭ, модель методики производства КТЭ, определен подход для выбора методов производства КТЭ и определения сроков производства комплексной экспертизы.

Третья глава посвящена описанию разработанного Смолиной А.Р. методического и алгоритмического обеспечения, детально изложена последовательность действий и методов для каждой из стадий производства КТЭ. При этом она сопровождается пошаговыми алгоритмами в виде IDEF0-диаграмм.

В четвертой главе автор на примерах реальных экспертиз, относящихся к различным видам КТЭ, демонстрирует внедрение результатов работы. Автор описывает положительный эффект от использования

результатов диссертации, подтверждая его итогами внедрения в работу для двух экспертных организаций изложен.

В приложения вынесены перечень вопросов, решаемых КТЭ, и акты о внедрении результатов диссертационной работы (два акта о внедрении в деятельность экспертных организаций и один акт о внедрении в учебный процесс ТУСУРа).

Научная новизна полученных результатов

Представленные соискателем результаты до работы автора и его публикаций ранее нигде не публиковались. Наиболее важными из них, обладающими признаками научной новизны, являются:

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.

Практическая ценность и внедрение результатов

Практическая значимость полученных результатов состоит в том, что применение предложенного методического и алгоритмического обеспечения позволяет ускорить и упростить процесс производства КТЭ, при сохранении необходимого качества экспертизы, а также снизить требования к квалификации экспертов КТЭ за счет формализации процедуры разработки частной методики КТЭ.

Обоснованность и достоверность полученных результатов и выводов

Автором адекватно используются методы теории множеств, системного анализа, теории защиты информации и теории графов, делаются корректные выводы на основе полученных данных. Достоверность результатов подтверждается положительным эффектом от их внедрения в работу действующих предприятий.

Пункты научной новизны, основные положения и выводы хорошо аргументированы, корректны и подтверждаются внедрением и экспериментальными данными.

Рекомендации по использованию результатов работы

Результаты диссертационной работы Смолиной А.Р. могут быть применены при производстве КТЭ и в процессе обучения экспертов. Информация о компьютерных преступлениях, которая собирается в ходе производства КТЭ, может быть использована для разработки и совершенствования средств защиты информации.

Публикации и апробация материалов диссертации

Основные результаты диссертации Смолиной А.Р. опубликованы в 11 работах, в числе в 4 статьях в журналах, рекомендованных ВАК РФ. Знакомство с отдельными публикациями соискателя свидетельствует о том, что в них достаточно полно отражены все основные положения, выводы и рекомендации диссертации.

Замечания к работе

1. Несмотря на значимость результатов компьютерно-технической экспертизы для анализа рисков нарушения информационной безопасности и уязвимости процессов переработки информации в IT-системах, на мой взгляд, в обзоре недостаточно внимания уделено работам, связанным с прогнозированием и

- исследованием рисков нарушения информационной безопасности в организациях, автор сосредоточился на работах в области судебной экспертизы.
2. Несмотря на наличие ряда разнообразных примеров, иллюстрирующих ключевые моменты работы, было бы полезно также наличие единого сквозного примера.
 3. Список сокращений, используемых в работе, неполный. В тексте диссертации встречаются сокращения, отсутствующие в разделе «Список сокращений», например, ТСЗАП, ПО, ГПК РФ, АПК РФ.

Общая оценка диссертации

Отмеченные выше замечания к диссертационной работе не носят принципиальный характер и не снижают ее общей положительной оценки. Диссертация Смолиной А.Р. является завершенной научно-квалификационной работой, в которой решена важная научно-техническая задача - разработка методического и алгоритмического обеспечения производства компьютерно-технической экспертизы. Диссертация соответствует паспорту специальности 05.13.19. – «Методы и системы защиты информации, информационная безопасность».

Изложение информации в работе выполнено грамотно, а графическое оформление – аккуратно. По каждой главе и работе в целом сделаны обоснованные выводы. Автореферат соответствует основному содержанию диссертации. Основные результаты диссертации опубликованы в авторитетных изданиях из перечня ВАК при Минобрнауки РФ с определяющим личным вкладом автора и представлены на ряде научных конференций и семинаров.

По своей актуальности, научной новизне, объему выполненных исследований и практической значимости результатов представленная работа

соответствует п.9. Положения о присуждении ученых степеней в редакции постановления Правительства РФ от 21.04.016 №335, предъявляемым к диссертациям на соискание ученой степени кандидата технических наук, а ее автор, Смолина Анна Равильевна, заслуживает присуждения ей ученой степени кандидата технических наук по специальности 05.13.19. – «Методы и системы защиты информации, информационная безопасность».

доктор технических наук,
профессор, директор Института
автоматики и информационных
технологий Федерального
государственного бюджетного
образовательного учреждения
высшего профессионального
образования «Тамбовский
государственный технический
университет»

 / Громов Юрий Юрьевич

5.09.12

Федеральное государственное бюджетное образовательное учреждение
Высшего образования «Тамбовский государственный
технический университет»
392032, г. Тамбов, ул. Советская, д. 106
Телефон: 8 (4752) 63-10-19
E-mail: tstu@admin.tstu.ru

05.13.06 – Автоматизация и управление технологическими процессами и производствами
(по отраслям)

Подпись профессора Громова Ю.Ю. заверяю:

Ученый секретарь Ученого совета
ФГБОУ ВО «Тамбовский государственный
технический университет»,
кандидат технических наук
«05» сентября 2017 года



Г.В. Мозгова