

ОТЗЫВ ОФИЦИАЛЬНОГО ОППОНЕНТА

на диссертационную работу 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.

1. Актуальность темы исследований

При расследовании широкого круга компьютерных преступлений, рост числа которых представляет собой характерную тенденцию современности, важным этапом является организация производства компьютерно-технических экспертиз (далее – КТЭ). Диссертация посвящена решению актуальной проблемы, направленной на совершенствование процессов формирования подходящих частных методик КТЭ, от которых зависит эффективность КТЭ в каждом конкретном случае. Для её решения автором предлагается унифицированная методика, основанная на классификации КТЭ по ряду сформированных критериев с последующей формализацией процесса выбора методик на основе применения аппарата теории графов.

2. Краткий обзор содержания работы

Диссертационная работа Смолиной А.Р. состоит из введения, четырех глав, заключения, списка литературы, а также двух приложений к работе.

Во введении изложена актуальность диссертационной работы, цель и задачи исследования, основные научные результаты, их научная новизна и практическая значимость.

В первой главе автором представлен аналитический обзор нормативно-правовой базы в области судебной экспертизы в целом и КТЭ в частности, текущего состояния методического и программно-алгоритмического обеспечения КТЭ, на основе которого определён круг существующих проблем исследуемой области и сформулированы задачи, решаемые в следующих главах диссертационной работы.

Во второй главе рассмотрены вопросы формализации методики производства КТЭ, классификации соответствующих частных методик и выбора методов их формирования с учетом ресурсных ограничений экспертных организаций. По результатам анализа известного методического обеспечения для производства КТЭ составлен достаточно полный опросник для эксперта, структурированный в соответствии с рассмотренной классификацией. Представлена теоретико-графовая модель производства КТЭ, описано применение алгоритмов поиска кратчайших путей для решения задачи выбора

частных методик на базе построенной модели, рассмотрено применение методологии PERT для оценки затрат на производство КТЭ в составе комплексной экспертизы.

В третьей главе описано созданное методическое и алгоритмическое обеспечение производства КТЭ на основе разработанных моделей. Для унифицированной методики, охватывающей десять типов классифицированных автором методик, подробно описаны алгоритмы для всех стадий производства КТЭ. Приведены результаты сравнения эффективности созданной методики с общепринятым комплексным подходом, практикуемым квалифицированными экспертами.

В четвертой главе изложены примеры экспертиз, выполненных с использованием разработанного автором методического обеспечения. Описаны результаты его внедрения в действующих экспертных организациях.

В конце каждой главы и в заключении к работе автором сделаны обобщающие выводы, позволяющие составить более полное системное представление о полученных результатах. Библиографический список включает 119 позиций, в т.ч. нормативные правовые акты, методические и научные труды российских и зарубежных ученых, интернет-ресурсы по профилю исследования.

Оформление текста диссертации и автореферата соответствует требованиям ГОСТ Р 7.0.11-2011.

3. Научная новизна полученных результатов.

Соискателем получены следующие новые научные результаты.

1. 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.

4. Обоснованность и достоверность полученных результатов и выводов

Обоснованность и достоверность полученных результатов и выводов подтверждаются:

- корректным применением формальных методов дискретной математики (теория множеств, теория графов), системного анализа и теории защиты информации;
- практикой успешного применения разработанного методического обеспечения при проведении более пятидесяти КТЭ за последние шесть лет;
- положительным эффектом при внедрении результатов теоретических исследований в практическую деятельность действующих экспертных организаций;
- экспериментальным сравнением по ряду критериев эффективности производства КТЭ на основе использования разработанного методического обеспечения и с применением общепринятых подходов

Подтверждением качества результатов диссертационных исследований А.Р.Смолиной является и тот факт, что подготовленные автором диссертации и экспертными организациями более 70 экспертных заключений на основе предложенного методического обеспечения за указанный выше период не получили ни одного отклонения в суде при оценке их на допустимость, по ним также не было назначено дополнительных и повторных экспертиз.

5. Теоретическое и практическое значение результатов работы

Полученные А.Р.Смолиной результаты диссертационных исследований имеют теоретическую и практическую значимость.

Теоретическая значимость заключается во вкладе автора в совершенствование научно-методической базы для унификации процессов производства КТЭ. Разработанные модели, методическое и алгоритмическое обеспечение могут использоваться в качестве теоретической основы при разработке автоматизированных информационно-аналитических экспертных систем для поддержки принятия решений в этой области.

Практическая значимость работы не вызывает сомнений, так как предложенная в диссертации методика и соответствующие ей алгоритмы позволяют сократить затраты экспертных организаций на производство КТЭ, обеспечить требуемое качество экспертного исследования и заключения даже при производстве экспертизы экспертами низкой квалификации. При практическом применении предложенная методика позволила уменьшить время разработки частных методик КТЭ в зависимости от особенностей экспертизы на 20-40% и сократить сроки её проведения на 10-25%. За счёт этих факторов и ослабления требования к квалификации экспертов удалось достичь заметного

снижения финансовых затрат (на 10-30%).

Работа также представляет учебно-методическую ценность для подготовки кадров в сфере производства КТЭ. С одной стороны, в ней детально исследован пример формализации содержательных задач этой предметной области, что может быть использовано при подготовке студентов, обучающихся по направлениям в сфере информационной безопасности и информационных технологий. С другой стороны, освоение будущими и практикующими экспертами разработанной методики позволит повысить качество их профессиональной работы в сфере КТЭ.

Значимость диссертационной работы подтверждена актами внедрения её результатов в практической деятельности в Томском экспертно-правовом центре «70 регион», ООО «Независимая оценка и экспертиза», а также в учебном процессе в Томском государственном университете систем управления и радиоэлектроники при подготовке специалистов по защите информации.

6. Рекомендации по использованию результатов исследования

Результаты, полученные в процессе диссертационных исследований А.Р.Смолиной, рекомендуется использовать:

- при разработке частных и конкретных методик производства КТЭ,
- при проектировании и разработке программного инструментария для поддержки принятия решений и автоматизации работы экспертов КТЭ;
- в процессе обучения и повышения квалификации экспертов КТЭ.

7. Полнота опубликования и апробации результатов работы

По материалам диссертации соискателем опубликовано 11 научных работ, из которых 4 статьи в журналах из списка ВАК и 7 работ в материалах всероссийских и международных конференций. Результаты, приведенные в диссертации, достаточно полно отражены в перечисленных публикациях и апробированы на конференциях. В автореферате адекватно и достаточно полно отражено основное содержание диссертации.

8. Замечания по диссертации и автореферату

1. Представляется недостаточно обоснованным выбор алгоритма Дейкстры как наиболее подходящего для исследуемых в диссертации графовых моделей (стр. 47). Этот выбор аргументируется ссылкой на работу Р.А.Черных [64], где модели теории графов применяются в другой предметной области. Перечень предположений о специфике графов, учитываемых в работе [64], шире и включает ряд дополнительных ограничений по сравнению с перечнем особенностей, сформулированных А.Р.Смолиной для своей модели, а идентичные словесные формулировки могут отражать разное количественное

содержание (например, «большое количество вершин»).

2. Ряд представленных в работе диаграмм в нотации IDEF0 не соответствует стандарту данной нотации. Примерами ошибок являются отсутствие точки зрения на контекстных диаграммах (стр. 42 и 48), отсутствие названий выходных потоков из функциональных блоков (стр. 71, 82, 83 и др.), отсутствие применяемой в IDEF0 кодировки функциональных блоков и несоблюдение стандартов именования диаграмм, обеспечивающих взаимосвязь разных уровней декомпозиции процессов (на всех диаграммах). Следует отметить, что информативность приведённых контекстных диаграмм без декомпозиции весьма незначительна. С другой стороны, представление основных стадий рассматриваемого процесса КТЭ изолированно (без диаграмм верхнего уровня) привело к утрате в IDEF0 высокоуровневых взаимосвязей декомпозированными подпроцессами (стадиями).

3. В работе присутствуют опечатки, имеются погрешности форматирования и пунктуации, особенно в оформлении перечислений (стр. 15, 23, 25, 38 и др.).

9. Общая оценка диссертации

Диссертация Смолиной А.Р. представляет собой законченную научно-квалификационную работу, в которой содержится решение актуальной задачи по разработке методического обеспечения для производства компьютерно-технической экспертизы. Исследования направлены на совершенствование методов производства КТЭ, как инструментов противодействия нарушениям информационной безопасности с использованием информационных технологий, что необходимо в процессе реализации политик информационной безопасности (в частности, политики реагирования на инциденты). Тем самым диссертация соответствует п. 12 и п.13 паспорта научной специальности «Методы и средства защиты информации, информационная безопасность»

Содержание работы хорошо структурировано, повествование построено последовательно и логично, текст в достаточной степени сопровождается графическими иллюстрациями, схемами, диаграммами. Работа обладает необходимыми признаками научной новизны, теоретической и практической значимости и в достаточной мере апробирована.

Следует отметить, что хотя указанные замечания несколько снижают впечатление от диссертации, они не подвергают сомнению основные научные результаты автора, их научную новизну и значимость.

Научная новизна полученных результатов, их обоснованность и достоверность, теоретическая и практическая значимость позволяют считать, что диссертация удовлетворяет требованиям 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.

Официальный оппонент
заведующий кафедрой информационной безопасности,
ФГБОУ ВО «Новосибирский государственный
университет экономики и управления «НИНХ»,
кандидат технических наук (специальность 05.13.16),
доцент

Т.М. Пестунова

Подлинность подписи Т.М. Пестуновой удостоверяю
Начальник управления
кадровой политики НГУЭУ
«29» сентября 2017г.



Т.Г.Абрамова

Пестунова Тамара Михайловна,
630099, г. Новосибирск, ул. Каменская, 52/1, НГУЭиУ
тел. +7(383)2439528, t.m.pestunova@nsuem.ru