Отзыв

научного руководителя 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

Диссертация Смолиной А.Р. посвящена разработке методического и алгоритмического обеспечения производства компьютерно-технической экспертизы. Компьютерно-техническая экспертиза проводится при расследовании преступлений, связанных с компьютерной информацией (киберпреступлений), в т.ч. преступлений связанных с нарушением информационной безопасности и хищением (разрушением, модификацией) информации.

Киберпреступления имеют высокую степень скрытности, занимают одно из лидирующих положений по сумме ущерба, принесенного юридическим и физическим лицам, и этот ущерб неуклонно увеличивается с каждым годом. В результате производства компьютерно-технической экспертизы (КТЭ) 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. В связи с этим, компьютерно-техническая экспертиза и ее методическое обеспечение имеют особое значение.

Развитие науки и техники, появление новых видов и модификация существующих киберпреступлений опережает появление экспертного методического обеспечения. Результаты выполненного Смолиной А.Р. анализа отечественных методических рекомендаций, находящихся в свободном и закрытом доступе, ранее выполненных диссертаций по данной тематике и зарубежных методических рекомендаций, показали, что методическое обеспечение, полностью удовлетворяющее процессуальным нормам, положениям и требованиям, отсутствует. Было установлено, что потребность в экспертных методиках испытывают не только коммерческие учреждения, но и государственные организации, занимающиеся производством компьютерно-технических, компьютерных экспертиз. Из-за отсутствия должных методик, проводя экспертизу, давая заключение, эксперт напрямую зависит от личного опыта. Установлена проблема поиска частной методики производства КТЭ и выбора методов в рамках найденной методики, соответствующих потребностям экспертной организации (эффективных по заданному критерию ресурса).

Разработка методики и алгоритмов производства компьютерно-технической экспертизы является актуальной задачей. Дело в том, что их наличие способствует 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. Особенно принципиальной и важной является проблематика безопасности информационно-телекоммуникационных систем государственных органов власти.

Учитывая актуальность и значимость ускорения, упрощения поиска методики производства КТЭ необходимо максимально автоматизировать этот процесс. Смолина А.Р., в ходе диссертационного исследования решила следующие задачи:

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.

Важно отметить, что автором лично проведено значительное количество КТЭ, выявлены причины, влияющие на раскрываемость киберпреступлений. Практическую ценность результатов диссертационной работы Смолиной А.Р. представляют:

– 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;

– оригинальная классификация методик производства КТЭ, которая позволяет сократить время эксперта на поиск необходимых методов исследования при производстве экспертизы;

– предложенное автором 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);

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

Таким образом, Смолиной А.Р. в результате выполненного диссертационного исследования по разработке методического и алгоритмического обеспечения производства КТЭ, применимого для решения широкого круга вопросов экспертизы и соответствующего текущим требованиями законодательства, была достигнута поставленная задача.

Получены впервые следующие основные научные результаты:

1) впервые создана модель методики производства КТЭ для существующих требований законодательства, учитывающая различные типы 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.

При выполнении диссертации Смолина Анна Равильевна проявила инициативность, самостоятельность, ответственность, нацеленность на достижения новых научных результатов и практической значимости проводимых исследований в области повышения уровня защищенности информационных ресурсов и зарекомендовала себя, как высококвалифицированный исследователь, способный самостоятельно ставить и решать важные научные задачи.

Считаю, что диссертация Смолиной А,Р. представляет собой законченную научно-квалификационную работу, выполненную на актуальную тему.

Научная новизна полученных результатов, их обоснованность и достоверность, а также практическая значимость позволяют считать, что диссертация «Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы»

удовлетворяет «Положению о присуждении ученых степеней» ВАК РФ, предъявляемых к кандидатским диссертациям, 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».

Научный руководитель,
ректор Томского государственного
университета систем управления
и радиоэлектроники,
доктор, технических наук, профессор _____ Александр Александрович Шелупанов
Дата: 24 июня 2017 г.

634050, Томск, пр. Ленина, 40
Тел.: +7 (3822)510530
E-mail: saa@keva.tusur.ru

Подпись А.А. Шелупанова заверяю
Ученый секретарь ученого Совета Томского государственного
университета систем управления
и радиоэлектроники _____ Е.В. Прокопчук

Отзыв

научного руководителя 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

Диссертация Смолиной А.Р. посвящена разработке методического и алгоритмического обеспечения производства компьютерно-технической экспертизы. Компьютерно-техническая экспертиза проводится при расследовании преступлений, связанных с компьютерной информацией (киберпреступлений), в т.ч. преступлений связанных с нарушением информационной безопасности и хищением (разрушением, модификацией) информации.

Киберпреступления имеют высокую степень скрытности, занимают одно из лидирующих положений по сумме ущерба, принесенного юридическим и физическим лицам, и этот ущерб неуклонно увеличивается с каждым годом. В результате производства компьютерно-технической экспертизы (КТЭ) 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. В связи с этим, компьютерно-техническая экспертиза и ее методическое обеспечение имеют особое значение.

Развитие науки и техники, появление новых видов и модификация существующих киберпреступлений опережает появление экспертного методического обеспечения. Результаты выполненного Смолиной А.Р. анализа отечественных методических рекомендаций, находящихся в свободном и закрытом доступе, ранее выполненных диссертаций по данной тематике и зарубежных методических рекомендаций, показали, что методическое обеспечение, полностью удовлетворяющее процессуальным нормам, положениям и требованиям, отсутствует. Было установлено, что потребность в экспертных методиках испытывают не только коммерческие учреждения, но и государственные организации, занимающиеся производством компьютерно-технических, компьютерных экспертиз. Из-за отсутствия должных методик, проводя экспертизу, давая заключение, эксперт напрямую зависит от личного опыта. Установлена проблема поиска частной методики производства КТЭ и выбора методов в рамках найденной методики, соответствующих потребностям экспертной организации (эффективных по заданному критерию ресурса).

Разработка методики и алгоритмов производства компьютерно-технической экспертизы является актуальной задачей. Дело в том, что их наличие способствует 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. Особенно принципиальной и важной является проблематика безопасности информационно-телекоммуникационных систем государственных органов власти.

Учитывая актуальность и значимость ускорения, упрощения поиска методики производства КТЭ необходимо максимально автоматизировать этот процесс. Смолина А.Р., в ходе диссертационного исследования решила следующие задачи:

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.

Важно отметить, что автором лично проведено значительное количество КТЭ, выявлены причины, влияющие на раскрываемость киберпреступлений. Практическую ценность результатов диссертационной работы Смолиной А.Р. представляют:

– 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;

– оригинальная классификация методик производства КТЭ, которая позволяет сократить время эксперта на поиск необходимых методов исследования при производстве экспертизы;

– предложенное автором 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);

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

Таким образом, Смолиной А.Р. в результате выполненного диссертационного исследования по разработке методического и алгоритмического обеспечения производства КТЭ, применимого для решения широкого круга вопросов экспертизы и соответствующего текущим требованиями законодательства, была достигнута поставленная задача.

Получены впервые следующие основные научные результаты:

1) впервые создана модель методики производства КТЭ для существующих требований законодательства, учитывающая различные типы 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.

При выполнении диссертации Смолина Анна Равильевна проявила инициативность, самостоятельность, ответственность, нацеленность на достижения новых научных результатов и практической значимости проводимых исследований в области повышения уровня защищенности информационных ресурсов и зарекомендовала себя, как высококвалифицированный исследователь, способный самостоятельно ставить и решать важные научные задачи.

Считаю, что диссертация Смолиной А,Р. представляет собой законченную научно-квалификационную работу, выполненную на актуальную тему.

Научная новизна полученных результатов, их обоснованность и достоверность, а также практическая значимость позволяют считать, что диссертация «Методическое и алгоритмическое обеспечение производства компьютерно-технической экспертизы»

удовлетворяет «Положению о присуждении ученых степеней» ВАК РФ, предъявляемых к кандидатским диссертациям, 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».

Научный руководитель,
ректор Томского государственного
университета систем управления
и радиоэлектроники,
доктор, технических наук, профессор _____ Александр Александрович Шелупанов
Дата: 24 июня 2017 г.

634050, Томск, пр. Ленина, 40
Тел.: +7 (3822)510530
E-mail: saa@keva.tusur.ru

Подпись А.А. Шелупанова заверяю
Ученый секретарь ученого Совета Томского государственного
университета систем управления
и радиоэлектроники _____ Е.В. Прокопчук