УДК 004.056

А.А. Шелупанов, А.Р. Смолина

Теоретические аспекты автоматизации формирования частных методик производства компьютерно-технической экспертизы

Статья посвящена теоретическим аспектам автоматизации формирования частных методик производства компьютерно-технической экспертизы. Для автоматизации и упрощения процесса разработки частных методик КТЭ автором предлагается разрабатываемая им система поддержки формирования частных методик производства компьютерно-технических экспертиз (СП ФОРЧМЕТ). В статье предлагается решение трех задач, необходимых для автоматизации формирования частных методик производства компьютерно-технической экспертизы (КТЭ): классификация методик производства КТЭ (по параметрам: категории задач, вопросы экспертизы, объекты исследования); построение модели методики производства КТЭ; разработка подхода, позволяющего определить, в рамках классифицированной методики, последовательность методов для каждой из стадии экспертизы, исходя из условий (ограничений) проведения экспертизы (временные ресурсы, финансовые ресурсы, человеческие ресурс и т.д.).

Ключевые слова: компьютерно-техническая экспертиза, автоматизации формирования частных методик, экспертная методика.

doi: 10.21293/1818-0442-2016-19-2-67-70

Компьютерно-техническая экспертиза (КТЭ) – самостоятельный род судебных экспертиз. Целью КТЭ является получение ответа на вопросы, требующие специальных познаний в области компьютерной криминалистики [1].

В основе любой экспертизы лежит экспертная методика. Общая методика, адаптированная и доработанная под решение частных задач экспертизы, называется частной [2].

Процесс разработки частных методик производства КТЭ от разработки частных методик традиционных родов экспертизы отличают значительные ресурсные затраты. Эксперты КТЭ из-за быстрого устаревания методик, большого количества объектов исследования [3] и широкого круга вопросов данного рода экспертизы значительную часть времени тратят на адаптацию и доработку общих методик под частные задачи экспертизы, поиск необходимых методов – разработку частных методик производства КТЭ. Сложность и длительность разработки частных методик КТЭ увеличивается при наложении экспертной организацией ограничений на выбор методов производства экспертизы по ресурсам (сроки, стоимость экспертного программного обеспечения и др.) [4]. Исходя из вышеописанного, весьма актуальна задача автоматизации формирования (разработки) частных методик производства КТЭ.

До настоящего времени процесс формирования частных методик КТЭ не был автоматизирован. Благодаря подходам, предложенным автором, автоматизация этого процесса становится возможной.

Для автоматизации и упрощения процесса разработки частных методик КТЭ автором предлагается разрабатываемая им система поддержки формирования частных методик производства компьютерно-технических экспертиз (СП ФОРЧМЕТ).

В числе задач, решение которых было необходимо для разработки СП ФОРЧМЕТ, находится следующая группа задач:

– классификация методик производства КТЭ (по параметрам: категории задач, вопросы экспертизы, объекты исследования);

– построение модели методики производства КТЭ;

– разработка подхода, позволяющего определить, в рамках классифицированной методики, последовательность методов для каждой из стадий экспертизы, исходя из условий (ограничений) проведения экспертизы (временные ресурсы, финансовые ресурсы, человеческие ресурсы и т.д.).

В данной статье кратко излагается предлагаемое автором решение данных задач.

Классификация методик производства КТЭ

Содержание экспертных методик КТЭ базируется на задачах, целях и объектах рассматриваемого рода судебных экспертиз [5].

Описание методов и алгоритмов классификации зачастую основывается на представлении исходной информации о классифицируемых объектах в виде графов [6–8]. Для классификации методик КТЭ предлагается использование теории графов. Для классификации методик КТЭ используем ориентированный граф $X(Y, Z)$, в нем:

1. $Y = \{y_0, y_{1,1}, y_{1,2} \ldots, y_{i,j}, y_e\}$ – множество узлов графа X.
2. Z – множество ориентированных рёбер графа X.
3. Узел y_0 – начало классификации.
4. Узел y_e – конец классификации.
5. i - количество критериев классификации методик.
6. j – количество признаков конкретного критерия.

Предлагаемый подход к классификации методик КТЭ с использованием теории графов может быть использован независимо от состава и количе-

ства критериев классификации методик и признаков критериев классификации методик. Более того, данный подход может быть использован для классификации методик других родов и видов экспертиз, т.е. этот подход является унифицированным.

Для классификации методик КТЭ используются простые пути на графе. Задача эксперта КТЭ по выбору необходимой методики производства КТЭ сводится к поиску пути на графе, т.е. определение путей между узлами y_0 и y_e и будет процессом определения методики производства КТЭ.

Множеством простых путей между узлами y_0 и y_e определяется множество методик производства КТЭ (M).

В результате были выявлены общие свойства методик производства КТЭ и формализованы базовые критерии и признаки для их классификации [5]. Классификация по базовым критериям описана в виде ориентированного графа, посредством описания множеств его узлов и ориентированных ребер Критерии классификации представлены тремя уровнями, определяющими свойства методик КТЭ. Полученные 48 типов методик описаны в виде множества M.

Модель методики производства КТЭ

В общем смысле под экспертной методикой (методикой экспертного исследования) понимается последовательность изучения свойств объекта экспертизы с целью решения экспертной задачи, путем упорядоченного применения научно разработанной системы методов экспертного познания [2].

Автором предлагается выполнить унификацию методики производства КТЭ, представив элементы методики КТЭ в виде множеств:

$A=\{a_1,a_2,\ldots,a_l\}$ – множество методов подготовительной стадии исследования, где l – количество методов, необходимых на подготовительной стадии исследования;

$B=\{b_1,b_2,\ldots,b_w\}$ – множество методов аналитической стадии исследования, где w – количество необходимых методов аналитической стадии исследования;

$C=\{c_1,c_2,\ldots,c_u\}$ – множество методов стадии эксперимента, где u – количество методов, необходимых на стадии эксперимента;

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

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

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

$$s_n \in S=(a_i,b_w,c_u,e_q,f_p,h_t),$$

где $$a_i \in A, b_w \in B, c_u \in C, e_q \in E, f_p \in F, h_t \in H. \quad (1)$$

Множество методов, используемых при производстве КТЭ, – подмножество декартового произведения множеств методов стадий экспертного исследования:

$$S \subset A \times B \times C \times E \times F \times H. \quad (2)$$

Модель методики производства КТЭ – упорядоченное множество методов КТЭ S.

Если S содержит помимо всеобщих методов познания и общенаучных методов познания частные методы, то на основании множества S определяется частная методика производства КТЭ.

Подход к определению последовательности методов КТЭ, исходя из условий ее производства

Автором предлагается выбирать методы исследования, исходя из наиболее оптимального использования ресурсов (финансовых, временных, человеческих и т.д.). Поиск методов, обеспечивающих оптимальное использование ресурсов, предлагается выполнить, обратившись к теории графов, и решить данную задачу, как типовую задачу теории графов – задачу о поиске кратчайшего пути [9].

Используем следующие обозначения:

1. $R = \{r_0, r_{1.1}, r_{1.2}, \ldots r_{i,j}, r_e\}$ – множество вершин графа RR.
2. RE – множество ребер d_{ij} графа RR. Каждому ребру RE сопоставлен вес k_{ij}.
3. Вершина r_0 – начало производства КТЭ.
4. Вершина r_e – завершение производства КТЭ.
5. i – количество альтернативных методов на определенной стадии производства КТЭ, $i \geq 1$.
6. j – количество стадий производства КТЭ, $j \geq 1$.
7. k_{ij} – вес ребра, обозначает длину ребра – неотрицательное число, характеризующее затраты ресурса (количество затрачиваемого времени, либо необходимое количество экспертов, либо финансовые затраты), по которому проводится определение методов.

Эта задача имеет ряд особенностей:

– используется ориентированный граф для определения последовательности методов;

– граф имеет большое количество вершин;

– отсутствуют ребра с отрицательным весом;

– все вершины, включенные в схему (методику), должны быть соединены с первой вершиной путями минимальной «длины»;

– в конечной схеме методов не может быть циклов;

– в конечную схему методов могут быть включены не все вершины графа;

– при построении сети методов необходима информация как о «длине» кратчайшего пути до вершины, так и о списке вершин, через которые он проходит;

– на вес ребра могут влиять несколько несвязанных параметров (например, затраты на производство экспертизы и сроки производства экспертизы).

Из-за того, что задача имеет ряд особенностей, важен выбор алгоритма ее решения, учитывающего их. Исходя из особенностей задачи, следует, что алгоритм поиска кратчайшего пути должен обладать определенными свойствами. Сравнение алгоритмов для решения задач с такими особенностями выполнено в рамках работы Р.А. Черных [10]. Основываясь на результатах данного сравнения, для решения задачи был выбран *алгоритм Дейкстры* [11]. Алгоритм Дейкстры основан на следующем тезисе Дейкстры: если кратчайший путь проходит через вершину r_{ij}, то длина части пути от r_o до r_{ij} должна быть минимально возможной.

Таким образом, был разработан подход определения последовательности методов производства компьютерно-технической экспертизы, основанный на теории графов. Данный подход представляет собой классификацию и выбор общей методики производства КТЭ, исходя из предмета экспертизы, и последующее формирование из общей методики частной методики, исходя из условий проведения экспертизы. Формирование частной методики решается как типовая задача теории графов – задача о поиске кратчайшего пути. Для ее решения выбран алгоритм Дейкстры.

Заключение

В данной статье показана актуальность задачи автоматизации формирования частных методик КТЭ. Актуальность этой задачи обусловлена наличием больших временных затрат экспертов КТЭ на адаптацию и доработку общих методик под частные задачи экспертизы, поиск необходимых методов при разработке частных методик производства КТЭ. При этом трудозатраты экспертов при разработке частных методик КТЭ увеличиваются при наложении экспертной организацией ограничений на выбор методов производства экспертизы по ресурсам (сроки, стоимость экспертного программного обеспечения и др.).

Для решения вышеописанной задачи автором предлагается система поддержки формирования частных методик производства КТЭ – СП ФОРЧМЕТ.

Для решения задачи автоматизации формирования частных методик КТЭ было необходимо решение следующих задач:

– классификация методик производства КТЭ (по параметрам: категории задач, вопросы экспертизы, объекты исследования);

– построение модели методики производства КТЭ;

– разработка подхода, позволяющего определить в рамках классифицированной методики последовательность методов для каждой из стадий экспертизы, исходя из условий (ограничений) проведения экспертизы (временные ресурсы, финансовые ресурсы, человеческие ресурсы и т.д.).

Предложенный подход к формированию частных методик, используемый в СП ФОРЧМЕТ, внедрен и используется в двух экспертных организациях Томской области. В результате его внедрения в экспертных организациях получен следующий положительный эффект:

– сокращение сроков производства экспертизы от 15 до 25%;

– сокращение сроков разработки частной методики КТЭ на 38%;

– уменьшение затрат на производство экспертизы от 20 до 22%.

В дальнейшем планируется расширение базы данных (БД) методов КТЭ. В настоящее время БД методов КТЭ, используемая в разрабатываемой СП ФОРЧМЕТ, содержит методы, описанные в унифицированной методике КТЭ, разработанной автором статьи в рамках диссертационного исследования.

Таким образом, благодаря использованию в СП ФОРЧМЕТ формального подхода, основанного на графовой модели, обеспечивается более эффективное по сравнению с традиционными методами решение задачи формирования частных методик производства компьютерно-технических экспертиз.

Литература

1. Давыдов И.В. Практические аспекты экспертной деятельности : доклад, тезисы доклада / И.В. Давыдов, А.А. Шелупанов // Научная сессия ТУСУР–2005. – Томск: В-Спектр, 2005. – Ч. 2. – С. 93–96.

2. Россинская Е.Р. Судебная компьютерно-техническая экспертиза / Е.Р. Россинская, А.И. Усов. – М.: Право и закон, 2001. – 416 с.

3. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1 (31). – С. 28–35.

4. Давыдов И.В. Технические требования к оборудованию в проведении компьютерно-технических экспертиз / И. В. Давыдов, А.А. Шелупанов // Научная сессия ТУСУР–2005. – Томск: В-Спектр, 2005. – Ч. 2. – С. 91–93.

5. Усов А.И. Судебно-экспертное исследование компьютерных средств и систем: Основы методического обеспечения: учеб. пособие / А.И. Усов; под ред. Е.Р. Россинской. – М.: Экзамен, Право и закон, 2003. – 368 с.

6. Айвазян С.А. Прикладная статистика: Классификации и снижение размерности / С.А. Айвазян, В.М. Бухштабер, И.С. Енюков, Л.Д. Мешалкин; под ред. С.А. Айвазяна. – М.: Финансы и статистика, 1989. – 607 с.

7. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

8. Зыков В.Д. Модели и средства обеспечения управления информационной безопасностью медицинских информационных систем: автореф. дис. … канд. техн. наук [Электронный ресурс]. – Режим доступа: http://old.tusur.ru/export/sites/ru.tusur.new/ru/science/edueducat/diss/2010/09/02.pdf свободный (дата обращения: 16.07.2016).

9. Кратчайшие пути [Электронный ресурс]. – Режим доступа: http://life-prog.ru/1_23938_kratchayshie-puti.html, свободный (дата обращения: 02.05.2016).

10. Черных Р.А. Обоснование выбора алгоритма поиска кратчайшего пути для построения схемы сети лесовозных дорог [Электронный ресурс]. – Режим доступа: http://forest-culture.narod.ru/HBZ/Stat_11_1-2/chernih21.pdf, свободный (дата обращения: 29.05.2016).

11. Shortest Paths [Электронный ресурс]. – Режим доступа: https://www.cs.princeton.edu/~rs/AlgsDS07/15ShortestPaths.pdf, свободный (дата обращения: 02.05.2016).

Шелупанов Александр Александрович
Д-р техн. наук, профессор, ректор ТУСУРа
Тел.: 8 (382-2) 51-05-30
Эл. почта: saa@tusur.ru

Смолина Анна Равильевна
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: 8-923-411-34-03
Эл. почта: atoj@rambler.ru

Shelupanov A.A., Smolina A.R.

Theoretical aspects of particular methodologies design support system for computer forensics provision

This article is devoted to theoretical aspects of particular methodologies design support system for computer forensics provision. Three tasks which are necessary for design this system are proposed. First task is classification of techniques of production computer forensics. Second task is the model of methodology of the computer forensics methods sequence production. And the third task is the approach of determining of the computer forensics methods sequence production. Two groups of input parameters are considered in this approach. The first group contains the expertize objects (the category of the task, questions of expertize, research facilities). The second group includes the expertize conditions and constraints (time resources, financial resources, human resources etc.).

Keywords: computer forensics, design support system for computer forensics provision, expert methods.