4. Методика решения вопросов о принадлежности объектов к ручному стрелковому огнестрельному оружию, их исправности и пригодности к стрельбе : утв. Межведомств. науч.-метод. советом в обл. судеб. экспертизы при Межведомств. комиссии по вопросам судеб.-эксперт. деятельности при Совете Безопасности Респ. Беларусь. Протокол № 5 от 25 июня 2008 г. Минск, 2008.

5. Методика отождествления огнестрельного оружия по следам на гильзах : утв. Межведомств. науч.-метод. советом в обл. судеб. экспертизы при Межведомств. комиссии по вопросам судеб.-эксперт. деятельности при Совете Безопасности Респ. Беларусь. Протокол № 4 от 12 марта 2008 г. Минск, 2008.

6. Методика отождествления нарезного огнестрельного оружия по следам на пулях : утв. Межведомств. науч.-метод. советом в обл. судеб. экспертизы при Межведомств. комиссии по вопросам судеб.-экспертной деятельности при Совете Безопасности Респ. Беларусь. Протокол № 4 от 12 марта 2008 г. Минск, 2008.

УДК 343.983.25

***А.И. Семикаленова***

## СУДЕБНАЯ КОМПЬЮТЕРНО-ТЕХНИЧЕСКАЯ ЭКСПЕРТИЗА: ЗАДАЧИ ОПРЕДЕЛЕНИЯ ФУНКЦИОНАЛЬНЫХ ВОЗМОЖНОСТЕЙ КОМПЬЮТЕРНЫХ ПРОГРАММ[1]

Сегодня судебная компьютерная техническая экспертиза прочно вошла в правоприменительную практику. Это обусловлено возросшим числом правонарушений, напрямую связанных с информационно-компьютерными средствами, и необходимостью применения специальных знаний для установления фактических обстоятельств произошедшего события. Если в начале 2000-х гг. к такого рода правонарушениям в основном относили правонарушения, связанные с распространением запрещенной информации, с налоговыми правонарушениями, реже с обманом потребителя, то сегодня копилка пополнилась правонарушениями в банковской сфере, сфере государственной службы. Если раньше объектами судебной компьютерно-технической экспертизы по делам уголовной направленности практически всегда была информация, содержащаяся в цифровом виде на внешних и внутренних компьютерных носителях, за редким исключение вставали вопросы, связанные с аппаратными ресурсами, то сегодня основными объектами исследования компьютерно-технической экспертизы становятся программы. Таким образом, если

[1] Выполнено в рамках реализации ГРАНТ РФФИ 18-29-16003\18 «Концепция информационно-компьютерного обеспечения криминалистической деятельности» ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина.



раньше экспертами решались задачи информационно-компьютерной и аппаратно-компьютерной экспертизы [1], то сегодня на первый план выходят задачи программно-компьютерной экспертизы [2].

Самой востребованной группой задач программно-компьютерной экспертизы сейчас можно считать установление функциональных возможностей программного продукта. Здесь считаем необходимым отметить, что простая задача, на первый взгляд, на самом деле является составной и включает в себя ряд подзадач, требующих решения. Это связано в основном с тем, что современное программное обеспечение – не единичные программы, представляющие один исполняемый файл, как это было в начале 2000-х, а сложные продукты, включающие в себя большое количество как исполняемых, зависимых от основного модуля библиотек, базы данных, так и самостоятельных программ, включенных в сложную систему программного продукта, но при этом способных функционировать отдельно. Именно из-за того, что сегодня объект программного-компьютерной экспертизы является многосоставным, мы считаем необходимым для определения функциональности программы выделить ряд подзадач, без решения которых, на наш взгляд, невозможно решение основной.

В эту группу входят:

1. Анализ сопроводительной технической документации программного продукта.

На первый взгляд, данная задача не совсем вписывается в рамки программно-компьютерной экспертизы. Подсознательно ее хочется отнести к информационно компьютерной, но это не так. Техническая документация – это важная часть, сопровождающая программный продукт с момента его планирования (например, Техническое задание) до момента передачи заказчику (например, Методика и программа испытаний, Руководство оператора и др.). В ряде случаев для решения частно-экспертных задач бывает достаточно проанализировать документацию и уже на этом этапе ответить органу, назначившему экспертизу, по каким причинам не работает программный продукт. Например, в случае базы данных (БД) важным документом является Эскизный проект БД, в данном документе прослеживаются все связи структурных элементов, так называемых сущностей, и элементы их сопряжения (индексы и атрибуты), и уже на этапе исследования этого документа бывает возможно дать ответ, могла ли данная БД использовать, хранить и обрабатывать конкретную информацию.

2. Определение фактического места положения программного продукта в компьютерной системе.

Казалось бы, банальное и всем давно известное правило «определи местонахождение исследуемого объекта на диске». Однако оно оказывается не столь очевидным, если вопрос касается сложных распределенных систем, и когда один программный продукт располагается на нескольких компьютерных средствах. В этом случае имеется реальная необходимость фиксировать не только логические диски и папки, в которых программный продукт находится, но и адреса в интернете (так называемые IP-адреса). Решение данной задачи в дальнейшем обезопасит эксперта от исследования «фейковых» программных продуктов, а в случае повторной или дополнительной экспертизы получить возможность исследовать тот же программный продукт, что и при производстве первичной экспертизы.

3. Определение фактического состояния программного объекта, состава соответствующих ему файлов, их параметров (объем, дата создания, атрибуты) и логического места положения в компьютерной системе.

Решение данной задачи является необходимой, на наш взгляд, в силу того, что позиционирование относительно носителей информации, имеющихся в компьютерной системе, определения логического пути доступа ко всем частям анализируемого продукта дает в дальнейшем возможность сделать вывод о причинах неработоспособности ряда задокументированных функций. Это связано с тем, что нарушение расположения на логических носителях файлов часто влечет невозможность их использования в дальнейшем системой. Она их попросту не видит. Установление и фиксация параметров, входящих в программный продукт файлов, нередко дает возможность увидеть присутствие посторонних компонентов, влияющих на работоспособность программы, или обнаружить недостачу файлов по сравнению с документально заявленной, что, в свою очередь, также влечет проблему реализации документированных функций.

4. Установление настроек программного обеспечения, времени его инсталляции (установки на машинный носитель).

Важным моментом для определения функциональных возможностей программного продукта является определение его настроек, не только тех, которые были установлены на момент проведения исследования, но и тех, которые должны были быть установлены в соответствии с технической документацией. Для определения функциональных возможностей программного продукта существенную роль играют сетевые настройки, особенно если анализируемая программа осуществляет взаимодействие с другими программами или со своими структурными компонентами, располагающимися на других компьютерных средствах. Например, в случае распределенной базы данных, когда информация хранится на разных компьютерах, при неправильных настройках возможно получение запрашиваемых сведений в неполном объеме или отказ в осуществлении поиска по запрашиваемому параметру. Сбои в такого рода настройках или их неправильная установка изначально влечет нарушение функционала исследуемого программного обеспечения при условии реализации его в самой структуре программы. Практически то же самое можно сказать и о настройках аппаратных составляющих системы. Например, неверная настройка сканера или принтера не позволит программе взаимодействовать с ними, хотя такие функции будут предусмотрены.



5. Выявление и исследование функциональных свойств продукта в целом, наличие или отсутствие каких-либо отклонений от типовых параметров (например, недокументированные функции).

Данная задача говорит сама за себя. Она по сути своей совпадает с задачей, вынесенной в название темы. Однако это ее более узкое изложение. Чаще всего современные эксперты довольствуются именно ее решением, что в корне неверно. Остановимся на этой задаче поподробнее. При ее решении основное, что выполняется, это тестирование программного продукта в соответствии с методикой испытаний, если такая присутствует. Если ее нет, то осуществляется проверка всех функций, до которых эксперт может добраться с использованием пользовательского интерфейса или специализированного программного обеспечения на уровне пользователя. Важным моментом здесь является то, что эксперт не просто должен на этом этапе исследования тестировать на выполнение определенного функционала систему, он еще и фиксирует ее отклики (экранные формы, формирования запросов, попытки соединений и т. д.). Именно обращая внимание на отклики системы, часто эксперт может сделать вывод о наличии недокументированных функций в программе. Однако это не единственный алгоритм действий, который необходимо совершить эксперту. Очень важным, но практически не реализуемым на практике сегодня является исследование функционала программного продукта на уровне.

6. Установление способов и форматов ввода-вывода информации.

Важным шагом определении соответствия функциональных возможностей программ является установление форматов и способов ввода – вывода данных. В чем особенность и необходимость установления этих параметров системы? Ответ на этот вопрос находится в современной структуре информационно-компьютерных систем. Сегодня программные продукты, разрабатываемые для решения различных задач, должны быть полностью интегрированы в ту аппаратно-программную

среду, в которой их собираются эксплуатировать. Особенно это касается тех компьютерных программ, которые реализуют такие программы, как электронное правительство, создание электронного документооборота в здравоохранении, в работе системы социального страхования и др. Неурегулированные процесс и форма ввода – вывода и объема данными в таких системах влечет несогласованную работу всей системы, в которую встраивается программный продукт и невозможность выполнения определенных ее функций. Следовательно, плохо отлаженный механизм ввода-вывода и обмена данными влечет неполную реализацию функциональных возможностей программного продукта. Ситуация может быть неочевидной при рассмотрении исследуемой программы отдельно от той системы, в которую она будет встраиваться, а может быть установлена либо при анализе всей системы в целом, что часто является проблематичным, либо при анализе способа и форматов ввода-вывода данных объекта исследования.

Диагностирование алгоритма программного продукта (представленного как в виде программного продукта, так и графического или текстового файла).

В п. 5 мы уже говорили об определении функциональных возможностей. Однако это не единственный алгоритм действий, который необходимо совершить эксперту. Очень важным, но практически нереализуемым на практике является исследование функционала программного продукта на уровне алгоритма. Мы говорим и об алгоритме, зашитом в тело уже готового программного продукта, и об алгоритмах, представленных в виде графических схем и текстовых файлов. Проанализированная нами экспертная практика говорит о том, что до данного этапа большинство экспертов никогда не доходят, а это неверно. Анализируя алгоритм программы с помощью трассировщиков программных продуктов, дизассемблирования и отладки, возможно установить большое количество значимой информации. Например, наличие незадокументированных функций, зашитых в программный продукт, наличие функций реализованных, но с которых по неосторожности забыли снять признак «комментарии», ошибки в самом алгоритме, не позволяют выполнять конкретные функции и ведут к «фатальной» ошибке. Анализ текстов алгоритмов программных продуктов и графических их исполнений (чаще всего можно обнаружит в сопроводительной документации) дает возможность проанализировать логику программного продукта этапы его реализации, что в дальнейшем дает возможность оценить функционал не только на этапе конкретного готового продукта, но и его версионное изменение.



Подводя итог, хотелось бы отметить, что, на наш взгляд, сегодня, анализируя компьютерную программу, нельзя останавливаться на стадии определения функциональности пользовательским методом (см. п. 5), необходимо учитывать все особенности современного состояния информационно-программной индустрии и анализировать ее с применением всех предложенных нами стадий.

1. Россинская Е.Р., Усов А.И. Классификация компьютерно-технической экспертизы и ее задачи // Уголовный процесс и криминалистика на рубеже веков. М., 2000.

2. Семикаленова А.И. Судебная программно-компьютерная экспертиза по уголовным делам : дис. ... канд. юрид. наук : 12.00.09. М., 2005.

УДК 343.9

***Э.Г. Хомяков***

## НЕКОТОРЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ТРАСОЛОГИИ И ТРАСОЛОГИЧЕСКОЙ ЭКСПЕРТИЗЫ

Одним из наиболее разработанных направлений в области криминалистической техники можно считать трасологию – учение о следах. Появившееся в трудах Г. Гросса упоминание следов как улик и вещественных доказательств нашло отражение в работах И.Н. Якимова. Э. Локар рассмотрел отдельные вопросы следообразования, связанные с совершением преступлений, а М.Н. Гернет и Б.И. Шевченко предложили и закрепили в отечественной криминалистике термин «трасология» (первоначально – «трасеология»). Советская криминалистика отметилась серьезной научной разработкой основных положений трасологии. Российская криминалистика подвергла серьезному анализу и синтезу все то, что было теоретически разработано и практически использовалось в этой области весь предыдущий период. Итогом можно считать появление серьезных фундаментальных источников, направленных на получение глубоких научных знаний в этой области, а также необходимых практических умений и навыков в рамках высшего образования [1–3]. Не менее значимым в плане закрепления трасологической терминологии явилась разработка государственного российского стандарта ГОСТ Р 57428-2017 «Судебно-трасологическая экспертиза. Термины и определения».

Вместе с тем любая наука или ее отдельное направление не может считаться догмой, она требует постоянного развития и совершенствования. Так и трасология (трасологическая экспертиза) является одной из