УДК 681.3.06

А.А. Шелупанов, А.Р. Смолина

Методика проведения подготовительной стадии исследования при производстве компьютерно-технической экспертизы

Предложена методика производства подготовительной стадии исследования при производстве компьютерно-технической экспертизы (КТЭ). Определены условия использования конкретных экспертных методов на подготовительной стадии КТЭ. Представлены преимущества использования методики при производстве КТЭ.
Ключевые слова: компьютерно-техническая экспертиза, подготовительная стадия, экспертная методика.
doi: 10.21293/1818-0442-2016-19-1-31-34

Расследование киберпреступлений [1], производство экспертиз по ним осложняются тем, что с постоянным развитием информационных технологий появляются объекты исследования, которых ранее просто не было, постоянно изменяются, модифицируются механизмы и методы совершения ранее известных видов преступлений, появляются абсолютно новые виды преступлений [2]. Экспертам компьютерно-технической экспертизы (КТЭ) [3] для дачи полного, достоверного, научно обоснованного заключения необходимо постоянное повышение квалификации, совершенствование навыков, обновление имеющихся знаний и использование соответствующей настоящему времени методической литературы. Это одно из отличий КТЭ от многих видов традиционной экспертизы (например, почерковедческой, дактилоскопической), где для дачи полного, достоверного, научно обоснованного заключения возможно использование методического обеспечения (экспертных методик) двадцатилетней давности. Для КТЭ это абсолютно невозможно. Отсюда и возникает потребность в разработке методики производства КТЭ, которая бы соответствовала современному уровню развития науки и техники [4].

Методика производства КТЭ должна содержать методические рекомендации для каждой из стадий производства экспертизы [4]. В рамках данной статьи будет рассмотрена предложенная авторами методика производства первой и обязательной стадии производства КТЭ – методика производства подготовительной стадии КТЭ.

Основная цель подготовительной стадии – уяснение экспертом экспертной задачи. Для этого экспертом рассматриваются поставленные вопросы, формируется общее представление о состоянии и признаках исследуемых объектов (в результате осмотра представленных объектов), происходит ознакомление с постановлением и материалами дела (имеющими отношение к экспертизе). На данной стадии выдвигаются рабочие гипотезы, определяются необходимые методы, приемы и средства исследования, а также алгоритм их применения, составляется план работы. В случае необходимости запрашиваются дополнительные материалы, изучается специальная и справочная литература.

Предложенная методика соответствует современному уровню развития науки и техники, а также требованиям отечественного законодательства [5–10]. Кроме этого, данная методика применима при производстве КТЭ по практически любым вопросам данного рода экспертизы.

Авторами предлагается методика производства подготовительной стадии производства КТЭ, представляющая следующую упорядоченную последовательность действий и методов:

1. Дается подписка о предупреждении об уголовной ответственности за дачу заведомо ложного заключения по ст. 307 Уголовного кодекса Российской Федерации (УК РФ) [10] или об административной ответственности по ст. 17.9 Кодекса Российской Федерации об административных правонарушениях (КоАП РФ) [11], а в необходимых случаях по ст. 310 УК РФ – за разглашение данных предварительного расследования.

2. Изучается постановление/определение, рассматриваются поставленные вопросы.

3. Осуществляется изучение материалов дела.

4. Выполняется осмотр и описание объектов, предоставленных на экспертизу. При осмотре эксперт изучает общие признаки исследуемых объектов. Осмотр рекомендуется сопровождать фотосъемкой объектов при их поступлении в экспертное учреждение – в упаковке и без упаковки, с целью фиксации внешних признаков исследуемых объектов.

5. После внешнего осмотра объектов осуществляется предварительный анализ информационного содержимого объектов с целью определения пригодности и достаточности объектов для ответа на вопросы экспертизы и определении методов исследования. Для этого объекты подключаются к тестовому компьютеру эксперта.

Перед подключением носителей информации к тестовому компьютеру должны быть обеспечены неизменность и сохранность информации [12]. Так, например, при подключении исследуемых накопителей на жестких магнитных дисках (НЖМД) к тестовому компьютеру для предотвращения утечки важной информации с подключаемого НЖМД должно быть осуществлено блокирование возможности сохранения данных на носителях, подключаемых к портам USB тестового компьютера. Блокирование возможности сохранения данных рекомендуется

осуществлять аппаратными блокираторами, допускается блокирование возможности сохранения данных программными средствами (средствами экспертной операционной системы (ОС), специализированным программным обеспечением (ПО)).

Для установления пригодности носителей информации для дальнейшего проведения исследования рекомендуется использование специализированного ПО. Например, для НЖМД возможно проведение тестирования на наличие сбойных кластеров (участков на поверхности диска, имеющих механическое либо другое повреждение). В качестве одной из программ, применимых для этого, может быть использована HDDScan. (HDDScan – это утилита для тестирования накопителей информации (HDD, RAID, Flash)). Программа предназначена для диагностики накопителей информации на наличие BAD-блоков, просмотра S.M.A.R.T-атрибутов накопителя, изменения специальных настроек (управление питанием, старт/стоп шпинделя, регулировка акустического режима).

Составляется рабочий план проведения исследования. Для этого проводится:

− Пересмотр нормативных документов и законодательных актов (*если требуется*).

− Определение возможности проведения экспертизы на основании: постановки цели, определения конечного результата проведения исследования; определения методов исследования; анализа применимости технической базы (программного обеспечения, оборудования) экспертного учреждения для решения конкретных поставленных задач; определения соответствия квалификации эксперта сложности вопросов, решаемых в рамках конкретной экспертизы.

− Анализ наличия среди ранее проведенных экспертиз аналогичных. В случае наличия – использование плана ранее проведенных экспертиз в качестве шаблона. При отсутствии – составление индивидуального плана проведения экспертизы.

− При необходимости использования на какомлибо из этапов разрушающих / частично разрушающих методов исследования – подача соответствующего ходатайства лицу, назначавшему экспертизу.

− В случае отклонения ходатайства – пересмотр методов проведения экспертизы. При невозможности проведения экспертизы без использования разрушающих / частично разрушающих методов – написание сообщения о невозможности проведения исследования.

− На тестовом компьютере эксперта осуществляется подготовка *рабочих зон* (директорий на тестовом компьютере эксперта, содержащих всю исследуемую информацию и информацию, имеющую доказательное значение в рамках дела). Подготовка рабочих зон осуществляется следующим образом:

− Выполняется клонирование / копирование данных с предоставленных на экспертизу носителей информации на рабочую станцию эксперта (тестовый компьютер). При проведении анализа данных, содержащихся непосредственно на самом носителе, без их предварительного копирования на рабочую станцию эксперта, данный этап отсутствует.

− На рабочей станции эксперта создается директория, в которой будут размещены файлы, содержащие информацию, необходимую для ответа на поставленные вопросы.

− На рабочей станции эксперта создается директория, в которой размещается информация, полученная с объектов, предоставленных на экспертизу, необходимая для проведения экспертизы, но в своем полном объеме не являющаяся доказательствами по делу. Таким образом, в данной директории могут быть размещены: полные образы носителей информации, все log-файлы, reg-файлы, история интернет-активности, index-файлы и т.д.

Такая организация рабочих зон весьма удобна при работе с большим количеством информации, но не является обязательной.

При выборе экспертом между исследованием клонов / копий / образов и исследованием информации непосредственно на носителе нужно руководствоваться тем, что в соответствии со стандартами криминалистики эксперты проводят исследование или анализ копий цифровых объектов – так исключается изменение или нарушение целостности данных оригинала.

Исследование непосредственно самого носителя возможно, если такой вид исследования физически не может внести изменения в информацию (например, из-за особенностей носителя – DVD-R) или невозможно получение копии, пригодной для проведения исследования (в этом случае необходимо разрешение лица, назначавшего экспертизу, на применение частично разрушающих методов).

Копия исходных цифровых данных для исследования обычно называется образом. Для того чтобы этот образ являлся юридическим эквивалентом оригинала, он должен представлять собой абсолютную копию исходных данных. Следовательно, каждый бит оригинала должны быть скопирован на образ. Существуют различные методы клонирования носителей информации. Выбор того или иного метода обусловливается конкретной ситуацией.

− Результаты предварительного исследования и регламентированная информация об эксперте, экспертном учреждении, экспертизе отражаются в вводной и частично исследовательской частях заключения.

На подготовительной стадии в вводной части заключения указываются:

− место и время производства экспертизы;

− основания производства;

− информация об экспертном учреждении, эксперте;

− отметка о предупреждении эксперта об уголовной ответственности;

− вопросы, поставленные на экспертизу;

− отметка о редакции вопроса (в случае редакции формулировки вопроса экспертом);

− информация об объектах, поступивших на исследование;

− предоставленные материалы дела, относящиеся к вопросам экспертизы;

− лица, присутствовавшие при производстве экспертизы (может быть указано / дополнено на последующих стадиях экспертизы);

− информация о заявленных ходатайствах, результаты их разрешения (может быть указано / дополнено на последующих стадиях экспертизы);

− отметка о производстве повторной или дополнительной экспертизы;

− использованная литература (может быть указано/дополнено на последующих стадиях экспертизы).

На подготовительной стадии в исследовательской части заключения указывается:

− информация о результатах внешнего осмотра объектов;

− информация о результатах исследования информационного пространства носителей информации и их пригодности для проведения исследования;

− информация о выбранных методах исследования носителей информации.

Для формализации и наглядного представления бизнес-процессов методики производства подготовительной стадии КТЭ была использована методология функционального моделирования IDEF0 [13]. Основываясь на ней, вышеописанная упорядоченная последовательность действий и методов подготовительной стадии КТЭ была представлена с помощью набора взаимосвязанных функциональных блоков. IDEF0-модель методики производства подготовительной стадии КТЭ представлена в диссертационном исследовании одного из соавторов данной статьи – А.Р. Смолиной. Данная модель в дальнейшем будет использована для автоматизации производства КТЭ.

Заключение

В данной статье описана разработанная авторами методика производства подготовительной стадии КТЭ, соответствующая современному уровню развития науки и техники, а также требованиям отечественного законодательства. Использование данной методики при производстве КТЭ способствует предотвращению:

1. Необоснованного применения экспертом частично разрушающих или разрушающих методов исследования – внесению изменений в информацию, содержащуюся на исследуемых объектах. В результате чего под сомнение может быть поставлена не только пригодность заключения в качестве доказательства, но и самих объектов исследования.

2. Упущения важных артефактов, неверной трактовки их (эксперт может дать не полное, не достоверное заключение).

3. Получения самоотвода или отвода эксперта из-за отсутствия у него необходимых знаний (информации о методах исследования, условиях их применения, экспертном инструментарии и т.д.).

4. Увеличения сроков производства экспертизы.

5. Увеличения трудозатрат и стоимости производства экспертизы.

6. Сокрытия преступления.

Разработанная IDEF0-модель методики производства подготовительной стадии КТЭ в дальнейшем будет использована для автоматизации производства КТЭ.

Литература

1. Свердлова В.Н. Компьютерные преступления // сб. статей: Научная сессия ТУСУР–2006. В 5 ч. – Томск: В-Спектр, 2006. – Ч. 3. – С. 129–132.

2. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия // Доклады ТУСУРа. – 2010. – № 1(21), ч. 1. – С. 41–45

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

4. Концептуальные основы судебной компьютерно-технической экспертизы [Электронный ресурс]. – Режим доступа: http://www.dslib.net/kriminal-process/konceptualnye-osnovy-sudebnoj-kompjuterno-tehnicheskoj-jekspertizy.html, платный (дата обращения: 20.12.2015).

5. Федеральный закон «О государственной судебно-экспертной деятельности в Российской Федерации» (с изменениями на 8 марта 2015 года) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/901788626, свободный (дата обращения: 25.02.2016).

6. Гражданский процессуальный кодекс РФ (ГПК РФ 2015) (с изменениями на 30 декабря 2015 года) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/grazhdanskij-processualnyj-kodeks-rf-gpk-rf, свободный (дата обращения: 25.02.2016).

7. Уголовно-процессуальный кодекс РФ (УПК РФ) (с изменениями на 30 декабря 2015 года) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ugolovno-processualnyj-kodeks-rf-upk-rf, свободный (дата обращения: 25.02.2016).

8. Арбитражный процессуальный кодекс РФ (АПК РФ 2015) (с изменениями на 30 декабря 2015 года) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/arbitrazhnyj-processualnyj-kodeks-rf-apk-rf, свободный (дата обращения: 25.02.2016).

9. Постановление Пленума Верховного Суда Российской Федерации от 21 декабря 2010 г. № 28 «О судебной экспертизе по уголовным делам» [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/902253012, свободный (дата обращения: 25.02.2016).

10. Уголовный кодекс РФ (УК РФ 2015) (с изменениями на 30 декабря 2015 года) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/ugolovnyj-kodeks-rf-uk-rf, свободный (дата обращения: 25.02.2016).

11. Кодекс РФ об административных правонарушениях (КоАП РФ 2015) (с изменениями на 15 февраля 2016 года) [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/kodeks-rf-ob-administrativnyh-pravonarushenijah-koap-rf, свободный (дата обращения: 25.02.2016).

12. Давыдов И.В. Технические требования к оборудованию в проведении компьютерно-технических экспертиз : доклад, тезисы доклада / И.В. Давыдов, А.А. Шелупанов // Научная сессия ТУСУР–2005: сб. статей. В 5 ч. – Томск: В-Спектр, 2005. – Ч. 2. – С. 91–93.

13. Методология функционального моделирования IDEF0. Руководящий документ [Электронный ресурс]. – Режим доступа: http://www.nsu.ru/smk/files/idef.pdf, свободный (дата обращения: 25.02.2016).

Шелупанов Александр Александрович
Д-р техн. наук, профессор, ректор
Томского государственного университета
систем управления и радиоэлектроники (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.

The methodology of preparatory stage of computer forensics

The methodology of preparatory stage of computer forensics is proposed. The specific uses of expert methods are shown. The advantages of using the methodology in the production computer forensics are shown.

Keywords: computer forensics, preparatory stage, expert methods.