А. С. Акимов, Е. А. Рыбкина
Московский инженерно-физический институт (государственный университет)

ОБЪЕКТЫ И ЗАДАЧИ КОМПЬЮТЕРНОЙ ЭКСПЕРТИЗЫ

Судебная компьютерно-техническая экспертиза как процессуальное действие состоит из проведения исследований и выдачи экспертом заключения по вопросам, разрешение которых требует специальных знаний в компьютерных и иных информационных видах техники и технологий.

В рамках Уголовно-процессуального кодекса Российской Федерации (УПК РФ) осуществляется процессуальное регулирование экспертной деятельности. Например, статья 57 УПК РФ свидетельствует о том, что эксперт вправе:

«1) знакомиться с материалами уголовного дела, относящимися к предмету судебной экспертизы;

2) ходатайствовать о предоставлении ему дополнительных материалов, необходимых для дачи заключения, либо привлечении к производству судебной экспертизы других экспертов…»

В статье 16 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации» указано, что эксперт обязан:

«- принять к производству порученную ему руководителем соответствующего государственного судебно-экспертного учреждения судебную экспертизу;

- провести полное исследование представленных ему объектов и материалов дела, дать обоснованное и объективное заключение по поставленным перед ним вопросам…»

Согласно статье 10 того же ФЗ «объектами исследований являются вещественные доказательства, документы, предметы, животные, трупы и их части, образцы для сравнительного исследования, а также материалы дела, по которому производится судебная экспертиза».

Вышеуказанное означает, что на компьютерно-техническую экспертизу должны быть предоставлены объекты исследования в виде компьютерных и иных информационных видов техники, в частности:

1) аппаратные объекты: персональные компьютеры, сетевые аппаратные средства (серверы, рабочие станции и т. д.), интегрированные системы (коммуникаторы, органайзеры, мобильные телефоны, смартфоны и т. п.), структурные комплектующие компоненты (аппаратные блоки, платы расширения, микросхемы и др.);

2) программные объекты: системное программное обеспечение (операционные системы, служебная системная информация и т. д.), прикладное программное обеспечение (текстовые и графические редакторы, системы управления базами данных, электронные таблицы и т. п.);

3) запоминающие устройства и электронные носители данных: магнитные и лазерные диски, флоппи-диски, флеш-носители, микросхемы памяти и др.

В соответствии со статьей 10 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации» «при проведении исследований вещественные доказательства и документы с разрешения органа или лица, назначивших судебную экспертизу, могут быть повреждены или использованы только в той мере, в какой это необходимо для проведения исследований и дачи заключения. Указанное разрешение должно содержаться в постановлении или определении о назначении судебной экспертизы либо соответствующем письме. Повреждение вещественных доказательств и документов, произведенное с разрешения органа или лица, назначивших судебную экспертизу, не влечет за собой возмещения ущерба их собственнику государственным судебно-экспертным учреждением или экспертом. В случае если транспортировка объекта исследований в государственное судебно-экспертное учреждение невозможна, орган или лицо, назначившие судебную экспертизу, обеспечивают эксперту беспрепятственный доступ к объекту и возможность его исследования».

Перечисленные требования в полной мере относятся и к объектам компьютерно-технической экспертизы.

Персональный компьютер как объект компьютерно-технической экспертизы — это ЭВМ, основной частью которой является системный блок, где расположены центральный процессор, материнская плата, оперативная память, модули памяти, встроенные дисководы, различные типы накопителей информации, контроллеры периферийных устройств и т. д. К системному блоку подключаются внешние периферийные устройства: устройства ввода информации (клавиатура, мышь, сканер и т. п.), устройства вывода информации (монитор, принтер и др.), устройства, предназначенные для обмена информацией с другими компьютерами (модемы, факс-модемы, радиомодемы, дополнительные внешние устройства хранения информации) и т. д. Основным носителем данных персональных компьютеров является накопитель на жестком магнитном диске, который может находиться как внутри компьютера, так и в отдельном блоке. Как правило, в персональном компьютере имеется один несъемный жесткий диск, но иногда устанавливаются и дополнительные жесткие диски, сведения о которых могут быть получены из справочной документации, из маркировки, нанесенной на диск, из установок программы SETUP, базовой системы ввода/вывода компьютера (BIOS) и т. д.

При экспертном исследовании персонального компьютера, являющегося орудием преступления, определяются его базовые реквизиты, информация о владельце и пользователе, круге их знакомств и связей, доступная и подлежащая восстановлению информация из файлов, подготовленных с использованием программных средств, с расширениями текстовых форматов (.txt, .doc и т. д.), графических форматов (.bmp, .jpg, .tif, .cdr, avi и т. д.), форматов баз данных (.dbf, .mdb и т. д.), электронных таблиц (.xls, .cal и т. д.) и др., подвергаются экспертному анализу модификация внешних устройств, данные протокола действий компьютеров, сведения о контрагентах из электронной почты, данные провайдеров о работе в сетях и т.д.

Принтеры и сканеры исследуются при производстве комплексной экспертизы совместно с технической экспертизой документов.

В экспертной практике встречаются накопители на гибких магнитных дисках, на оптических дисках (основаны на считывании и записи информации с помощью луча лазера), на компакт-дисках (CD-ROM, CD-RW, DVD-ROM), магнитооптические накопители, ZIP, Jaz-устройства, перепрограммируемые карты памяти (Flash-card) и др.

Электронные носители данных являются в экспертном понимании источником получения криминалистически значимой компьютерной информации.

Перечень объектов исследуемой экспертизы подлежит постоянному уточнению по мере развития теоретических, методических и практических основ экспертной деятельности в сфере современных информационных технологий.

Следует отметить, что получение доступа к компьютерной информации на носителях данных и последующее экспертное всестороннее ее исследование является одной из основных задач компьютерно-технической экспертизы.

Задачи эксперту формируют суд, судьи, органы дознания, лица, производящие дознание, следователи или прокуроры в целях установления обстоятельств, подлежащих доказыванию по конкретному делу в сфере информационной безопасности.

Статья 195 УПК РФ гласит, что «следователь выносит постановление о назначении судебной экспертизы, а в случаях, предусмотренных пунктом 3 части второй статьи 29 УПК РФ, возбуждает перед судом ходатайство». По ходатайству сторон или по собственной инициативе суд может назначить судебную экспертизу на основании статьи 283 «Производство судебной экспертизы» УПК РФ. При назначении судебной компьютерно-технической экспертизы председательствующий предлагает сторонам представить в письменном виде вопросы эксперту. Поставленные вопросы должны быть оглашены, и по ним заслушаны мнения участников судебного разбирательства. Рассмотрев указанные вопросы, суд своим определением или постановлением отклоняет те из них, которые не относятся к уголовному делу сферы информационной безопасности или компетенции эксперта, формулирует новые вопросы. Судебная компьютерно-техническая экспертиза производится в порядке, установленном нормами главы 27 УПК РФ. Суд по ходатайству сторон либо по собственной инициативе назначает повторную либо дополнительную судебную экспертизу при наличии противоречий между заключениями экспертов, которые невозможно преодолеть в судебном разбирательстве путем допроса экспертов.

Судебная экспертиза считается назначенной со дня вынесения соответствующего определения или постановления согласно статье 19 Федерального закона «О государственной судебно-экспертной деятельности в Российской Федерации». Орган или лицо, назначившие судебную компьютерно-техническую экспертизу, предоставляют объекты исследований и материалы дела, необходимые для проведения исследований и дачи заключения экспертом.

При производстве компьютерно-технической экспертизы решаются следующие задачи:

А. Определение вида (типа, марки), свойств компьютера, его технических и функциональных характеристик (например, емкость накопителя, время доступа к данным, скорость передачи данных, способ и плотность магнитной записи и др.).

Б. Определение фактического состояния и исправности компьютера, наличия физических дефектов.

Эти задачи обосновывают возможность компьютера служить орудием преступления (то есть исправен ли он, технически и технологически пригоден ли для совершения расследуемого информационного преступления).

В. Определение условий (обстановки) применения компьютерной техники.

Г. Восстановление хронологической последовательности деятельности информационного правонарушителя и вероятного места действия.

Д. Извлечение криминалистически значимой информации.

Е. Установление причинной связи между действиями компьютерного правонарушителя и противоправными результатами.

Данные задачи обусловливают роль компьютера как орудия преступления.

Вопросы эксперту в данном случае формулируются следующим образом:

1. Находится ли компьютер в работоспособном состоянии, если нет, то какие имеются неисправности?

2. Мог ли информационный правонарушитель совершить расследуемое преступление с помощью именно этого компьютера?

3. Если мог, то какова хронологическая последовательность информационно-преступных действий?

4. Имеется ли в компьютере криминалистически значимая информация?

5. Есть ли возможность установления причинной связи между использованием данного компьютера и противоправными последствиями?

При исследовании программной среды компьютеров решаются следующие экспертные задачи:

1) исследуются признаки контрафактности представленных на экспертизу программных продуктов;

2) выявляются настройки программного обеспечения, его функциональные свойства, время инсталляции;

3) определяется фактическое состояние программного объекта, параметры его файлов (даты создания, атрибуты), наличие каких-либо недокументированных функций;

4) устанавливается состояние программы при начальной инсталляции;

5) выявляются возможные изменения свойств и состояния программного обеспечения (например, преднамеренное изменение каких-либо функций);

6) устанавливается способ осуществления изменений в программе (например, воздействием вредоносной программы, ошибками программной среды и т. д.);

7) изучается возможность причинной связи между действиями пользователя компьютерной системы в отношении программного обеспечения и наступившими последствиями.

Кроме вышеуказанных задач может быть исследовано диагностирование алгоритма программного продукта, типы поддерживаемых аппаратно-программных платформ и т. д.

Вопросы эксперту в данном случае формулируются следующим образом:

1. Имеются ли признаки контрафактности представленных на экспертизу программных продуктов?

2. Присутствуют ли какие-либо недокументированные функции?

3. Нет ли свидетельств преднамеренных изменений каких-либо функций?

4. Каковы способы осуществления изменений в программе?

5. Есть ли возможность установления причинной связи между использованием данного программного обеспечения и противоправными последствиями?

При исследовании информации, находящейся в компьютере, решаются следующие экспертные задачи:

1) установление наличия информации в компьютере;

2) определение фактического состояния информации (доступная или нуждающаяся в восстановлении);

3) изучение первоначального состояния криминалистически значимой информации на носителе данных;

4) анализ условий изменения свойств исследуемой информации (например, внесения изменений в содержимое файла, запись с внешнего магнитного носителя и т. п.);

5) определение времени (периода) хронологической последовательности воздействий на информацию (например, время подготовки текстовых документов, графических файлов и т. п.);

6) установление отдельных этапов (стадий) подготовки информационного преступления по имеющейся информации на носителе данных (например, подготовка писем и их рассылка факсимильной программой в разные адреса);

7) выявление признаков, характеризующих определенные профессиональные и пользовательские навыки, умения, привычки информационного правонарушителя, установление условий, при которых была создана (модифицирована, удалена, скопирована) информация;

8) установление причинной связи между имевшими место манипуляциями с компьютерной информацией и наступившими противозаконными последствиями.

Вопросы эксперту в данном случае формулируются следующим образом:

1. Имеется ли криминалистически значимая информация в компьютере?

2. Подобная информация доступна или нуждается в восстановлении?

3. Можно ли определить стадии подготовки информационного преступления по имеющейся информации на носителях данных?

4. Сохранились ли электронные следы возможных участников события?

5. Имеются ли признаки профессионализма информационного правонарушителя, его пользовательских навыков, умений и т. д.?

6. Существует ли причинная связь между действиями правонарушителя с компьютерной информацией и наступившими противозаконными последствиями?

В случае наличия данных о работе компьютера в сети формируются следующие экспертные задачи:

1) определение сетей, с которыми работал информационный правонарушитель, и сетевых провайдеров;

2) выявление свойств и характеристик сети, установление ее архитектуры, конфигурации, средств сетевой технологии, установленных сетевых компонентов, организации доступа к данным, определение принадлежности средства к серверной или клиентской части приложений и т. д.;

3) установление первоначального состояния вычислительной сети и определение причин изменения свойств вычислительной сети (например, установление факта нарушения режимов эксплуатации сети; следов использования «вредоносных» программ и т. п.);

4) выделение свойств и характеристик компьютерной техники и установленного программного обеспечения, определение исправности сетевого средства, наличия физических дефектов, состояния системного журнала, компонентов управлением доступа;

5) определение событий в сети по их результатам (например, факта несанкционированного доступа, доказательств распространения в сети вредоносных функций и т. д.);

6) установление причинной связи между незаконным использованием сетевых технологий и противоправными результатами их применения.

Вопросы эксперту в данном случае формулируются следующим образом:

1. Можно ли определить сети, с которыми работал информационный правонарушитель, и сетевых провайдеров?

2. Имеются ли факты нарушения режимов эксплуатации сети либо следы использования информационным правонарушителем «вредоносных» программ?

3. Есть ли какие-либо факты несанкционированного доступа в чужие компьютерные сети и базы данных и доказательства распространения в сети вредоносных функций?

4. Возможно ли установление причинной связи между незаконным использованием сетевых технологий и противоправными результатами их применения?

Важность данной статьи заключается в соединении авторами одновременно процессуальных основ судебной компьютерно-технической экспертизы, технической классификации объектов, представляемых на данную экспертизу, в виде компьютерной и иной информационной техники, техногенных задач, обуславливающих проведение подобных экспертиз, и вопросов правового характера к экспертам, формируемых органами дознания, следствия, прокуратуры и суда.

Таким образом, можно отметить, что эффективность результатов судебной компьютерно-технической экспертизы зависит от объема представленных объектов экспертизы в виде компьютерной и иной информационной техники. На качество проведенной экспертизы влияют состояние представленных объектов, конкретизация задач и вопросов, поставленных перед экспертом, а также профессионализм и квалификация экспертов в вопросах, разрешение которых требует специальных знаний в компьютерных и иных информационных видах техники и технологий.