

«Современные возможности компьютерно-технической экспертизы».

Объектами судебной компьютерно-технической экспертизы (далее – СКТЭ) являются:

Аппаратные объекты:

- персональные компьютеры (настольные, портативные);
- наладонные компьютеры и интегрированные системы (органайзеры);
- периферийные устройства (принтеры, сканеры, модемы и др.);
- машинные носители данных (жесткие диски, дискеты, компакт-диски, карты памяти);
- сетевые аппаратные средства;
- мобильные телефоны;
- специализированные микропроцессорные устройства; (иммобилайзеры и др.)
- комплектующие указанных компонентов.

Программные объекты:

- системное программное обеспечение (операционные системы);
- средства разработки и отладки программ;
- служебная системная информация;
- прикладное программное обеспечение.

Информационные объекты:

- текстовые и графические документы, изготовленные с использованием компьютерных средств;
- данные в форматах мультимедиа;
- информация в форматах баз данных.

Типовые экспертные задачи

1. Поиск информации на машинных носителях.

Поиск информации необходим, когда в ходе следствия установлено, что средства компьютерной техники использовались для подготовки, пересылки, хранения данных в электронном виде - документов, электронных писем, списков адресов и телефонов и др.

2. Установление факта изготовления документов на комплекте компьютерной техники.

Данная задача является основной при расследовании преступлений, связанных с подделкой документов и ценных бумаг. Исследование носит комплексный характер и проводится методами компьютерно-технической экспертизы и судебно-технической экспертизы документов.

3. Установление обстоятельств работы в сети INTERNET.

Данная задача возникает при раскрытии и расследовании преступлений, сопряженных с работой в сети Интернет.

4. Исследование вредоносных программ

Данная задача возникает при раскрытии и расследовании фактов распространения вредоносных программ или несанкционированного доступа к компьютерным или сетевым ресурсам.

5. Исследование программных продуктов:

Исследование направлено на выявление фактов несанкционированного использования программных продуктов и их модификации, обеспечивающей такое использование. Следует отметить, что в настоящее время, инвентаризация программного обеспечения, установленного на жесткий диск системного блока, носит автоматизированный характер. Специальное программное обеспечение, предназначенное для экспресс-аудита компьютера, позволяет выявить признаки неправомерной активации программ.

6. Исследование баз данных

Исследование направлено на установление структуры баз данных, их назначения, содержания. Чаще всего связано с исследованием бухгалтерских программ, базы данных которых содержат информацию о движении денежных средств.

7. Исследование аппаратных средств компьютерной техники

Исследование имеет целью установить назначение аппаратных средств и диагностировать их работоспособность.

8. Исследование специализированных микропроцессорных устройств

Основными задачами исследования являются установление назначения устройств, диагностика их работоспособности и соответствия эталонным образцам (кассовые аппараты), установление фактов модификации микропрограмм и данных микропроцессорных устройств.

ТИПОВЫЕ ВОПРОСЫ, СТАВЯЩИЕСЯ ПЕРЕД ЭКСПЕРТАМИ ПРИ ИССЛЕДОВАНИИ МОБИЛЬНЫХ ТЕЛЕФОНОВ

Данный комплекс решаемых вопросов разработан для следователей и дознавателей силовых ведомств, сотрудниками РОССИЙСКОГО ФЕДЕРАЛЬНОГО ЦЕНТРА СУДЕБНОЙ ЭКСПЕРТИЗЫ ПРИ МИНИСТЕРСТВЕ ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ.

1. Какая пользовательская информация имеется на представленных мобильных телефонах?
2. Какое программное обеспечение установлено в представленных на исследование мобильных телефонах?
3. Какие сообщения, созданные в программах обмена мгновенными сообщениями, имеются в памяти представленных на исследование мобильных телефонов?
4. Какие сведения о соединениях между абонентами (звонки, sms-сообщения) имеются в памяти представленных на исследование мобильных телефонов и СИМ-карт?
5. Какие почтовые сообщения имеются в памяти представленных на исследование мобильных телефонов?
6. Какие сведения о посещении Интернет-ресурсов имеются в памяти представленных на исследование мобильных телефонов?
7. Какая иная пользовательская информация (геолокации, пользовательские графические файлы и видеозаписи) имеются в памяти представленных на исследование мобильных телефонов?

8. Какие данные о пользователях (имена, учетные записи) представленных на исследования мобильных телефонов имеются в их памяти?
9. Имеются ли в памяти устройств пользовательская информация или файлы, созданные или измененные после года?
10. Имеется ли среди программного обеспечения, программное обеспечение с признаками вредоносности? Если да, то какие функциональные особенности у выявленного программного обеспечения?

Необходимыми условиями для проведения качественного исследования мобильных устройств являются:

- предоставление эксперту графических паролей, PIN-кодов безопасности абонентской станции;
- предоставление эксперту PIN-кодов для доступа к запоминающему устройству SIM-карт.

Такие вопросы как:

- Каков вид (тип, модель, марка) представленного на экспертизу мобильного телефона?
- Какая информация имеется в SIM-карте (включая абонентский номер сим-карты) в представленном мобильном телефоне?

не требуют специальных экспертных познаний.

Соотносимость абонентских номеров к номерам SIM, не входит в компетенцию эксперта. Данная информация может быть получена у оператора сотовой связи, например «МТС».