

Типовые вопросы информационно-компьютерной экспертизы (данных)

1. Как отформатирован носитель информации и в каком виде на него записаны данные?
2. Каковы характеристики физического размещения данных на носителе информации?
3. Каковы характеристики логического размещения данных на носителе информации?
4. Какие свойства, характеристики и параметры (объемы, даты создания-изменения, атрибуты и др.) имеют данные на носителе информации?
5. Какого вида (явный, скрытый, удаленный, архив) информация имеется на носителе?
6. К какому типу относятся выявленные (определенные) данные (текстовые, графические, база данных, электронная таблица, мультимедиа, запись пластиковой карты, данные ПЗУ и др.) и какими программными средствами они обеспечиваются?
7. Каким образом организован доступ (свободный, ограниченный и проч.) к данным на носителе информации и каковы его характеристики?
8. Какие свойства, характеристики имеют выявленные средства защиты данных и какие пути ее преодоления возможны?
9. Какие признаки преодоления защиты (либо попыток несанкционированного доступа) имеются на носителе информации?
10. Каково содержание защищенных данных?
11. Каково фактическое состояние выявленных данных и соответствует ли оно типовому состоянию на соответствующих носителях данных?
12. Какие несоответствия типовому представлению имеются в выявленных данных (нарушение целостности, несоответствие формата, вредоносные включения и проч.)?
13. Каковы пользовательские (потребительские) свойства и предназначение данных на носителе информации?



14. Какие данные для решения определенной функциональной (потребительской) задачи имеются на носителе информации?

15. Какие данные с фактами и обстоятельствами конкретного дела находятся на представленном носителе информации?

16. Какие данные о собственнике (пользователе) компьютерной системы (в том числе имена, пароли, права доступа и проч.) имеются на носителях информации?

17. Какие данные с представленных на экспертизу документов (образцов) и в каком виде (целостном, фрагментарном) находятся на носителе информации?

18. Каково первоначальное состояние данных на носителе (в каком виде, какого содержания и с какими характеристиками, атрибутами находились определенные данные до их удаления или модификации)?

19. Каким способом и при каких обстоятельствах произведены действия или операции (блокирование, модификация, копирование, удаление) определенных данных на носителе информации?

20. Какой механизм (последовательность действий) по решению конкретной задачи отражен в определенных данных на носителе информации?

21. Какая хронологическая последовательность действий (операций) с выявленными данными имела место при решении конкретной задачи (например, подготовки изображений денежных знаков, ценных бумаг, оттисков печатей и т.п.)?

