Организация ремонтного обслуживания аппаратуры и средств защиты

Организация ремонтного обслуживания аппаратуры и средств защиты осуществляется физическими и юридическими лицами в соответствии с имеющейся лицензией, выданной ФСТЭК России.

Кроме того, осуществляется изъятие компьютерной техники при расследовании уголовных преступлений с целью проведения специализированных экспертиз и исследования информации.

Все изымаемое аппаратное оборудование и носители информации опечатывать и упаковывать таким образом, чтобы исключить:

- возможность их включения и работы с ними при хранении;
- разборку и демонтаж отдельных компонентов;
- уничтожение или изменение состояния технических средств и информации;
- возможность повреждения и уничтожения технических средств и информации при транспортировке.

При упаковке компьютерной техники и носителей информации на сопроводительной бирке указывается:

- наименование того, что находится в пакете либо коробке с указанием количества;
- где, когда, у кого изъято, в ходе какого следственного действия;
- подписи с указанием фамилий и инициалов участников следственного действия.

К упаковке изымаемых компьютерно-технических устройств и носителей информации предъявляются следующие требования:

Вещественные доказательства упаковываются в картонные коробки или мешки, которые заклеиваются в местах вскрытия липкой лентой.

Упаковка должна обеспечивать исключение свободного перемещения объектов внутри.

Мелкие объекты (дискеты, компакт-диски, флэш-накопители, накопители на жестких магнитных дисках и др.) могут быть упакованы в отдельные металлизированные или бумажные пакеты, при этом перед помещением в бумажные пакеты их целесообразно завернуть в металлическую фольгу.

При невозможности упаковки средств компьютерной техники в отдельную коробку допустимо использование листов плотной бумаги, картона, прочных целлофановых пакетов или кусков ткани, со всех сторон закрывающих изымаемые объекты. Их можно закрепить при помощи липкой ленты, исключив при этом ее контакт с поверхностью объекта. Выполнение вышеуказанных требований позволит максимально исключить возможность повреждения объектов, поступающих для производства компьютерно-технических экспертиз, обеспечит сохранность их признаков и свойств, а также хранимой на них информации.

Криминалистическое исследование компьютерной (электронной, машинной) информации и техники является одним из самых молодых направлений в криминалистической технике. Данное направление начало складываться в первой половине 90-х гг. XX в. В настоящее время указанные исследования проводятся практически по всем категориям уголовных дел. Наиболее часто исследования компьютерной информации и техники проводятся при расследовании следующих видов преступлений: в сфере компьютерной информации; терроризм и экстремизм, экономические и налоговые преступления, распространение порнографической продукции, преступных нарушений авторских и смежных прав, изготовление поддельной печатной продукции (например, бланков документов, денежных знаков, ценных бумаг). В последние годы значительно выросло число исследований компьютерной информации в ходе раскрытия преступлений против личности. Экспертизы компьютерной информации стали повседневным явлением при рассмотрении гражданских, арбитражных и административных дел.

В ходе расследования преступлений обнаружение компьютерной информации, подлежащей исследованию, возможно в трех типичных следственно-экспертных ситуациях.

Во-первых, информация является объектом преступных посягательств: фальсифицированные данные бухгалтерского и иных учетов, измененные персональные данные, взломанные защитные программные

средства и др. Как правило, в этих случаях по материальным следам преступного воздействия на компьютерную информацию и свидетельским показаниям необходимо установить способ и механизм преступления.

Во-вторых, она является средством совершения преступления и (или) средством коммуникации, используемым для достижения криминальных целей. Это могут быть различные вредоносные программы (например, вирусы), компьютер преступника, мобильные устройства связи и т. п. В данной ситуации часто приходится преодолевать защитные средства (аппаратные и программные), используемые правонарушителем для защиты криминалистически значимой информации. Необходимо установить причинную связь между средством преступления и действиями преступника, преступным результатом.

В-третьих, компьютерная информация характеризует определенный объект по расследуемому делу, при этом она не является ни объектом преступного воздействия, ни средством совершения преступления. Например, статистическая информация о деятельности предприятия, данные с видеокамер о месте происшествия и др. Последняя ситуация наиболее проста для расследования. В этом случае, как правило, выполняются операции, позволяющие следователю получить доступ к данной информации, копировать ее, систематизировать и др.

В предмет криминалистического исследования компьютерной информации и техники входят:

- разработка приемов, способов, рекомендаций по обнаружению, фиксации, изъятию и хранению компьютерной информации и техники;
- изучение состояния и процессов обработки компьютерной информации; состояния и функционирования электронно-вычислительной техники.

<u>В ходе решения типовых диагностических задач устанавливаются следующие обстоятельства:</u>

- свойства и состояние компьютерной информации и техники;
- факт и условия внесения изменений в компьютерную информацию после ее создания; выявление признаков такого изменения;
- время создания (удаления, изменения) информации, хронологическая последовательность функционирования компьютера, их системы или сети; функции, выполняемые определенной программой;
- способ доступа к компьютерной информации и (или) оборудованию;
- фактическое состояние и исправность компьютерной техники;
- соответствие реквизитов электронных документов требованиям, предъявляемым к ним, выявление признаков изменения данных реквизитов;
- соблюдение установленных технических правил при работе с компьютерной информацией, в том числе правил, обеспечивающих ее защиту;
- причинная связь между действиями с компьютерной техникой и (или) информацией и наступившими последствиями (удалением файла, прекращением работы ЭВМ и т. п.);
- содержание защищенной кодовыми и иными криптографическими средствами информации, получение к ней доступа;
- способы и обстоятельства доступа в компьютерные и телекоммуникационные сети, в том числе в Интернет, операции, осуществляемые в данных сетях;
- конфигурации компьютерной (телекоммуникационной) сети или конфигурации ее отдельных фрагментов.

При подготовке к назначению компьютерной экспертизы следователь или суд решают следующие задачи: корректная фиксация состояния объектов, направляемых на экспертизу, обеспечивающая сохранение их неизменности; обеспечение защиты компьютерной информации от внешних воздействий, которые могут привести к утрате или изменению ее свойств (электромагнитное излучение, попадание воды и др.) при хранении и транспортировке; предоставление вместе с компьютерной информацией и техникой вышеуказанных вспомогательных объектов; направление материалов следственных действий с информацией о состоянии и обстоятельствах изъятия объектов (протоколы, планы, фотоснимки, видеоматериалы и т. п.).