Д. В. Кузченко

О НЕКОТОРЫХ ОРГАНИЗАЦИОННО-ТАКТИЧЕСКИХ ОСОБЕННОСТЯХ ОСМОТРА КОМПЬЮТЕРНОЙ ТЕХНИКИ ПРИ РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

В статье освещены организационно-тактические особенности производства осмотра компьютерной техники при расследовании преступлений в сфере компьютерной информации.

Ключевые слова: компьютерная информация, компьютерная техника, операционная система, джамперы, материнская плата, микропроцессор.

D. V. Kuzchenko

ABOUT SOME ORGANIZATIONAL TACTICAL FEATURES OF MANUFACTURE OF SURVEY OF COMPUTER TECHNICS ARE SHINED AT INVESTIGATION OF CRIMES IN SPHERE OF THE COMPUTER INFORMATION

In article organizational tactical features of manufacture of survey of computer technics are shined at investigation of crimes in sphere of the computer information.

Keywords: computer information, computer technics, jumper, operating system, motherboard MB, microprocessor.

При расследовании преступлений, совершенных в сфере компьютерной информации, следователь сталкивается с нетрадиционными следами преступной деятельности, и здесь возникают новые объекты криминалистических исследований: компьютерная информация и средства компьютерной техники.

Средства компьютерной техники представляют собой достаточно специфический криминалистический объект, требующий специальных тактических приемов проведения осмотра [1].

В связи с этим большую помощь может оказать специально сформированный набор инструментов, специализированных компьютеров, технических и программных средств, а также набор каталогов и справочник по вычислительной технике — ToolBox криминалиста [[1]]. Как правило, в производстве осмотра компьютерной техники участвует специалист — программист.

Наиболее распространенным средством компьютерной техники являются ПЭВМ (персональные электронно-вычислительные машины) типа IBM PC (персональный компьютер), состоящие из двух основных элементов: системного блока и монитора.

Системный блок представляет собой основу персонального компьютера и включает в себя все основные элементы компьютера:

1. Корпус системного блока:

— горизонтальный — Desktop, FootPrint, SlimLine;

— вертикальный — MiniTower, MidiTower, BigTower, SuperBigTower.

2. Материнская плата с микропроцессором (Motherboard & Bus):

— устаревшие: Baby-AT; Mini-ATX; полноразмерная плата AT; LPX.

— современные: ATX; microATX; Flex-ATX; NLX; WTX, CEB.

— внедряемые: Mini-ITX и Nano-ITX; Pico-ITX; BTX, MicroBTX и PicoBTX.

3. Накопитель на жестких магнитных дисках (Hard (Magnetic) Disk Drive, HDD, HMDD).

4. Оптический привод компакт-дисков (CD-ROM/R/RW, DVD-ROM/R/RW, DVD-RAM, HD DVD, BD-ROM, GD-ROM).

5. Блоки расширения (дополнительные платы): VideoAdapter (видеоадаптер), Soundcard (звуковая плата), Netcard (сетевая плата для локальной сети).

Монитор представляет собой универсальное устройство визуального отображения всех видов информации, состоящее из дисплея и устройств, предназначенных для вывода текстовой, графической и видеоинформации на дисплей [2].

При проведении следственного осмотра ПЭВМ возможны следующие основные ситуации:

1. Осмотр компьютера производится на месте совершения преступления в сфере компьютерной информации:

— осматриваемый компьютер включен (находится в рабочем состоянии);

— осматриваемый компьютер выключен.

2. Осмотр компьютера производится вне места совершения преступления в сфере компьютерной информации (например, осмотр изъятого в ходе проведения следственного действия).

Внешний осмотр системного блока следует начинать с его тыльной стороны, где расположены все основные электрические выводы периферийных устройств, кабели электропитания, сетевые кабели и т. п.

При проведении осмотра ПЭВМ целесообразно произвести поиск следов пальцев рук пользователей данного компьютера на кнопках извлечения оптических компакт-дисков, кнопках «POWER» и «RESET», а также с тыльной стороны корпуса, в области крепления винтов защитного кожуха системного блока. Следует обратить внимание и при необходимости отразить в протоколе следственного действия следующее:

1) какие разъемы были задействованы, к каким внешним устройствам они были подключены, длина соединений;

2) наличие характерных царапин, сколов, загибов и иных повреждений на соединительных элементах и разъемах системного блока;

3) наличие свободных слотов для подключения внешних устройств и их защита от внешних воздействий.

Данные сведения могут оказать следователю определенную помощь, так как они в какой-то степени характеризуют пользователя и дают информацию о типовых вариантах использования осматриваемого компьютера.

Далее следует отсоединить провод, обеспечивающий подачу электропитания в системный блок, затем — соединения, обеспечивающие подачу электропитания от системного блока к внешним устройствам. Отсоединение остальных связей системного блока нужно производить последовательно — сверху вниз. Также следует убедиться в полном отсутствии какого-либо напряжения на корпусе или выходах системного блока, например, от внутренней батарейки материнской платы или других автономных источников тока, помещенных внутрь системного блока. Необходимость выполнения данной операции обусловлена существованием и использованием в некоторых случаях средств защиты информации, срабатывающих от вскрытия корпуса (разрыва соответствующей электрической цепи), и уничтожающих информацию на магнитных носителях (винчестерах). Кроме того, нужно обратить внимание и на некоторые моменты, которые при необходимости отражаются в протоколе следственного действия:

1) наличие механизма защиты корпуса системного блока от вскрытия и его состояние;

2) способ крепления внешнего защитного корпуса и его состояние.

При осмотре содержимого системного блока акцентируется внимание на наличии, каких-либо нестандартных устройств, что следует отразить в протоколе следственного действия. При этом отмечают:

1) тип, модель и количество используемой ОЗУ (оперативно запоминающее устройство);

2) места размещения периферийных устройств;

3) маркировку, год выпуска, техническое состояние и серийные номера каждого из элементов ПЭВМ;

4) наличие джамперов (перемычек) и их расположение на момент осмотра.

Полученные на данном этапе сведения могут помочь установить ориентировочную дату комплектации осматриваемого компьютера, фирмы, осуществившие поставку и сборку, а также возможные места ремонта и модернизации персонального компьютера.

Далее необходимо произвести подключение питания и запуск персонального компьютера. При выполнении данного действия следует отразить в протоколе:

1) порядок загрузки операционной системы и других программ, загружаемых в оперативную память при включении ПЭВМ;

2) параметры загрузки операционной системы и прикладных программ, установленные «по умолчанию»;

3) содержание основных файлов конфигурации персонального компьютера (config. sys, autoexec. bat, win. ini, system. ini) и системного реестра.

Специфическим моментом осмотра отдельных видов компьютерных объектов является использование специальных инструментов, технических и программных средств. Каждый факт использования таких средств должен быть отражен в протоколе с указанием его особенностей. Например, если содержимое винчестера определялось с использованием стандартного программного средства (например Norton Commander или команды операционной системы MS-DOS), то необходимо указать:

— как она появилась на осматриваемом средстве вычислительной техники (была установлена ранее или установлена лицом, проводившим осмотр);

— как осуществлялся запуск этого программного средства (все передаваемые параметры, опции и установки);

— каким образом осуществлялся вывод результатов осмотра и каким образом результаты осмотра были приобщены к протоколу осмотра (копирование на магнитный носитель, распечатка на бумаге и т. п.).

В заключительной части протокола осмотра при расследовании преступлений в сфере компьютерной информации, кроме традиционных записей (о характеристиках использовавшихся фотоматериалов и фотоаппарата, изъятых объектах и следах, а также замечаний участников осмотра по поводу произведенных действий), следует указать:

— количество полученных изображений с помощью цифрового фотоаппарата, их размер (в байтах) и формат представления;

— номер или другой идентификационный признак носителя информации, на котором записаны результаты фото- или видеосъемки;

— открытые атрибуты цифровой подписи, использовавшейся для фиксации результатов осмотра на магнитном носителе.

Подводя итог всему сказанному выше, можно сформулировать следующие предложения о порядке и форме документирования результатов следственного осмотра компьютерной техники:

1) протокол следственного осмотра следует оформлять в виде единого гипертекстового документа [3], представленного на оптическом носителе, включающего результаты фото-, видеосъемки и звукового сопровождения и организованном в виде иерархического описания от обзорной информации и отдельных элементов до детальной информации по каждому из названных объектов осмотра;

2) для фиксации неизменности результатов осмотра, представленных в цифровом виде, целесообразно применение технологии цифровой подписи;

3) для фиксации результатов осмотра необходимо широкое применение цифровых фотоаппаратов и цифровых видеокамер, обеспечивающих получение изображений и видеоряда в виде цифровых файлов, пригодных для хранения на оптических носителях;

4) для придания юридической силы протоколу следственного осмотра, представленному на оптическом носителе, необходимо придерживаться положений ГОСТ СССР 6. 10. 4-84 от 9 октября 1984 г. «Придание юридической силы документам на машинном носителе и

машинограмме, создаваемым средствами вычислительной техники».

Надеемся, что предложенные тактические рекомендации для производства осмотра компьютерной техники будут способствовать максимальной эффективности данного следственного действия.

Список библиографических ссылок

1. Россинская Е. Р. Судебная экспертиза в уголовном, гражданском и арбитражном процессе. М., 1996. С. 173—179.

2. Алекс Эклер. Справочник по цифровой вычислительной технике. Харвест, 2007. С. 147.

3. Компьютерные технологии в юридической деятельности: учебник и практ. пособие / под ред. проф. Н. Полевого, к. ю. н. В. Крылова. М., 1994. С. 198—206.