МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

Карагандинский юридический институт
имени Баримбека Бейсенова

ПРАВИЛА
осмотра компьютерной техники и снятия с неё информации

КАРАГАНДА 2010

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

Карагандинский юридический институт
имени Баримбека Бейсенова

ПРАВИЛА
осмотра компьютерной техники и снятия с неё информации

Криминалистические рекомендации

КАРАГАНДА 2010

Правила осмотра компьютерной техники и снятия с нее информации / Составители: канд. юрид. наук ***Шакенов А. О., Шарипов С. Р.,*** канд. тех. наук ***Тажигулов А. А.*** — Караганда: КЮИ МВД РК им. Б. Бейсенова, 2010. — 20 с.

Р е ц е н з е н т ы:

Заместитель начальника ОКУ ДВД по Карагандинской области полковник полиции ***Куйбеда Н. Н.;*** доцент кафедры управления и психологии КЮИ МВД РК им. Б. Бейсенова, канд. тех. наук, подполковник полиции ***Баширов А. В.***

Работа предназначена для сотрудников правоохранительных органов, студентов, преподавателей и слушателей высших учебных заведений МВД РК.

Наиболее информативным в плане обнаружения следов преступления является осмотр места происшествия и вещественного доказательства, в качестве которых могут выступать устройства компьютерного типа и их комплектующие, средства коммуникации и т. д.

Осмотр СВТ (средств вычислительной техники) производят для достижения следующих целей:

- обнаружения следов, образовавшихся в результате происшествия или совершения преступления, других вещественных доказательств для установления, обстоятельств совершения преступления;
- выяснения обстановки происшествия для восстановления механизма совершения преступления;
- установления технического состояния СВТ.

Для реализации первой цели требуется участие специалиста-криминалиста и специалиста в области СВТ и информационных технологий. В решении двух других непосредственное участие специалиста-криминалиста не требуется. В зависимости от специфики осматриваемого СВТ в следственном действии должны принимать участие следующие специалисты:

- по обслуживанию и ремонту СВТ (для осмотра аппаратной части СВТ и соединительной арматуры; для ЭВМ — инженер-системотехник);
- в области сетевых технологий (для осмотра СВТ, используемых в системах дистанционной передачи данных — компьютерных сетях, периферийного оборудования удаленного доступа, удаленных терминалов);
- по средствам связи и телекоммуникациям (для осмотра оборудования электросвязи, используемого для передачи компьютерных данных и команд, а также СВТ, являющихся средствами связи);
- инженер-программист (для осмотра программного обеспечения СВТ, определения принципа его функционирования, установления следов преступной деятельности в среде машинной информации).

При отсутствии таких специалистов в государственных экспертных учреждениях их следует заблаговременно подбирать на предприятиях, в учреждениях, фирмах и компаниях, осуществляющих обслуживание и эксплуатацию компьютерной и коммуникационной техники разработку программного обеспечения, средств защиты компьютерной информации. Могут быть приглашены также специалисты из учебных заведений и научно-исследовательских организаций.

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано. На предварительном этапе необходимо провести следующую работу:

- наметить круг лиц, участвующих в осмотре;

- определить последовательность действий лиц при осмотре места происшествия;
- пригласить соответствующих квалифицированных специалистов;
- подготовить соответствующую компьютерную технику и программное обеспечение для считывания и хранения изъятой информации, исследования полученной информации, обнаружения информационных следов преступления;
- перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности;
- провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

Следователь и участники следственно-оперативной группы должны знать и соблюдать общие правила обращения с вычислительной техникой и носителями информации. Несоблюдение этих правил может привести к потере важной для расследования информации и нанесению материального ущерба, вызванного этими действиями.

Общими правилами обращения с вычислительной техникой и носителями информации являются следующие:

- включение (выключение) компьютеров и других технических средств производятся только специалистом или под его руководством;
- во избежание разрушения носителей информации и микросхем памяти ЭВМ применение средств криминалистической техники — магнитных искателей, ультрафиолетового осветителя, инфракрасного преобразователя должно быть согласовано со специалистом;
- необходимо исключить попадания мелких частиц и порошков на рабочие части компьютеров (разъемы, дисковод, вентилятор и др.);
- при работе с магнитными носителями информации запрещается прикасаться руками к рабочей поверхности дисков, подвергать их электромагнитному воздействию, сгибать диски, хранить без специальных конвертов (пакетов, коробок);
- диапазон допустимых температур при хранении и транспортировке должен варьироваться в температурных пределах от 0 до + 50 градусов Цельсия;
- со всеми непонятными вопросами, затрагивающими терминологию, устройство и функционирование вычислительной техники, необходимо обращаться только к специалисту.

При проведении осмотра СВТ на месте происшествия необходимо:

- удалить с места происшествия всех посторонних лиц и организовать его охрану. Обязательной охране подлежат следующие объекты:
  - место происшествия;
  - все СВТ, находящиеся на территории (в помещении);
  - пункты отключения электропитания СВТ, находящиеся в здании (учреждении, организации, на территории);
- зафиксировать обстановку, сложившуюся на момент осмотра места происшествия, произвести ориентирующую и обзорную фото – видеосъемку;
- исключить возможность соприкосновения с оборудованием посторонним лицам, а в некоторых случаях и участникам следственно-оперативной группы. Желательно лишить их возможности пользоваться телефоном, а при острой необходимости делать это только с разрешения следователя. «Не допускайте, чтобы кто-либо производил любые действия с компьютером. Риск, связанный с непосредственным вмешательством в систему, значительно больше, чем малый шанс дистанционного влияния на систему с другого устройства»[1]. Необходимо организовать охрану каждого компьютера (терминала), для чего возможно привлечение дополнительных си;
- опросить потерпевшего, материально ответственное лицо и очевидцев (операторов СВТ) об изменениях, внесенных в обстановку, о категории обрабатываемой информации (общедоступная или конфиденциальная), а также о действиях потерпевшего до прибытия СОГ. Вопросы необходимо конкретизировать по мере детального осмотра места происшествия, поиска следов и других вещественных доказательств;
- определить, соединены ли находящиеся в помещении компьютеры в локальную вычислительную сеть. На это могут указать коаксиальные кабели, идущие от компьютера к компьютеру, телефонные провода. При наличии локальной компьютерной сети наибольший интерес представляет центральный компьютер, (сервер), на котором хранится большая часть информации и к которому имеют доступ все ЭВМ. Этот компьютер необходимо обследовать более тщательно и осторожно;
- установить, имеются ли соединения компьютера с оборудованием или вычислительной техникой вне осматриваемого помещения. На это могут указывать кабели и провода, идущие от компьютера в другие помещения или здания. Если есть соединения, то существует реальная возможность непосредственного обмена информацией, независимо от желания специалиста, ее изменения или уничтожения с удаленных рабочих мест, находящихся за несколько метров или даже километров от обыскиваемого помещения. Для предотвращения этого на время съема информации вычисли-

тельную сеть необходимо отключить. Эту работу квалифицировано может выполнить только специалист в области вычислительной техники;

- выяснить, подключен ли компьютер к телефонной линии. В случае подключения на него могут поступать вызовы с дальнейшими приемами или передачами информации. Следует иметь в виду, что установить, запрограммирован ли компьютер на передачу, может только специалист. Если информация, поступающая на компьютер по электронной почте, факсимильной или телетайпной связи может иметь интерес, то отключать телефонную или телетайпную линии нет смысла. Необходимо лишь воздерживаться от телефонных разговоров по данной линии;
- определить, запущены ли программы на ЭВМ и какие именно. Для этого необходимо изучить изображение на экране и, по возможности, детально описать его в протоколе. Если до момента осмотра компьютера на него вводился оператором текст и этот текст может представлять интерес для следствия, то выход из редактора надо осуществлять только после сохранения набранного текста на жестком диске путем выбора соответствующего пункта меню. Установить название программы, которая последней выполнялась на компьютере, в операционной системе MS-DOS можно путем одновременного нажатия клавиш Ctrl-E. Многократное нажатие этой комбинации дает возможность проследить за всеми запускаемыми программами с момента последней перезагрузки компьютера. В операционных системах Windows перечень открытых в данный момент приложений (программ) можно увидеть на рабочей панели — возле кнопки «Пуск». Кроме того, эту задачу можно решить путем одновременного нажатия клавиш «Alt» и «Tab».Если специалисту удастся определить, что на компьютере работает программа уничтожения информации или ее зашифровки, то такие программы стоит приостановить и обследование начать именно с этого компьютера. Важно отметить, что следователю в любом случае не следует самому производить какие-либо манипуляции с вычислительной техникой. Их должен осуществлять специалист.

В ходе проведения осмотра важно установить, не содержится ли на компьютере информация, которая может способствовать более плодотворному и целенаправленному осмотру (различные планы помещений, участков местности, пароли, коды доступа, шифры и т. п.). Для этого специалистом проводится экспресс-анализ компьютерной информации путем просмотра содержимого дисков. Интерес могут представлять также файлы с текстовой или графической информацией. Следует обращать внимание не только на наличие (отсутствие) физических повреждений компьютерной техники, магнитных носителей и т. п., но и на состояние окон, дверей и запорных устройств на них.

В этот период осмотра фиксируется текущее состояние компьютерной информации, делается вывод о произошедшем событии и его последствиях: уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, их системы или сети; устанавливается способ совершения преступления. Для этого с помощью специалиста наблюдается действие программ, содержимое текстовых файлов и баз данных. При этом особое внимание следует уделить изучению имеющихся в большинстве компьютерных систем файлов регистрации. Какое бы событие не произошло в системе, информация о нем (кто инициировал его, когда и в какое время оно произошло, какие при этом были затронуты файлы) регистрируется в этих файлах. В частности, в файлах регистрации может получить отражение информация о паролях пользователей, их именах, идентификационных номерах. Впоследствии данная информация может быть использована для установления компьютера, с которого произошел неправомерный доступ к компьютерной информации.

Большой информационной ценностью обладает протокол выхода в сеть Интернет с определенного компьютера. Он автоматически ведется на каждом компьютере, с которого возможен выход во всемирную сеть (количество дней его хранения определяется пользователем). Представляют интерес также данные о пользователе электронной почты (фамилия, имя, отчество, дата и место рождения, место жительства, работы и пр.). Сам пользователь заинтересован в предоставлении достоверной информации для получения электронных сообщений.

Следует отметить, что многие программы фирмы Microsoft создают резервные копии файлов, файлы-отчеты, сохраняют информацию о последних проделанных операциях и выполненных программах, а также содержат иную информацию, способную представлять значительный интерес для расследования. Вот лишь некоторые примеры:

Microsoft Outlook Express хранит в своей базе данных все письма, которые были отправлены, получены или удалены. Эти файлы расположены в директории \Windows\Aplication\Microsoft\ OutlookExpress\Mail\ с расширениями IDX и MBX.

Microsoft Internet Explorer — в директории \Windows\ Temporary Internet Files\ хранит места, которые посетил пользователь, находясь в сети Интернет.

Microsoft Windows — в директории \Wmdows\History\ хранит все файлы истории, то есть данные о ранее выполнявшихся программах; в директории \Windows\name.pwl — имена, телефоны и пароли для соединения с Интернет, которые расшифровываются с помощью специальных программ.

При этом специалист-криминалист производит поиск традиционных следов преступления, обращая внимание не только на наличие (отсутствие) физических повреждений компьютерной техники, магнитных носителей и т. п., но и на состояние окон, дверей и запорных устройствах на них. Если выясняется, что имел место непосредственный доступ к компьютерной технике и информации, то с помощью специалиста-криминалиста необходимо отыскивать следы пальцев рук, микрочастицы на клавиатуре, корпусе ЭВМ, мониторе, принтере и т. п.

Помимо специальных мероприятий с компьютером нужно четко организовать поисковые мероприятия, направление на поиск тайников, в которых могут находиться обычные документы и предметы. Таким тайником может служить и сам компьютер, в частности, системный блок.

Последний обладает некоторыми особенностями построения, делающими его более удобным для организации тайников. Во-первых, внутри системного блока очень много свободного места, поскольку там резервируется место для расширения и наращивания возможностей компьютера путем установки дополнительных плат.

Во-вторых, системный блок компьютера в силу его модульного построения очень удобен и быстр в разборке-сборке, которая производится, как правило, без применения каких-либо дополнительных приспособлений (отвертки, гаечных ключей и пр.). Это способствует удобному доступу к узлам компьютера без оставления следов.

В третьих, внутри компьютера используются электронные схемы с малым напряжением, не опасным для жизни человека. Единственное место с напряжением 220 вольт — блок питания, который всегда помещен в защитный кожух; подаваемое питание на платы не превышает 12 вольт. Это дает возможность для вскрытия корпуса без его отключения от сети питания.

В-четвертых, самая большая плата системного блока, так называемая материнская плата, крепится зажимами к стенке или к низу корпуса, между которыми остается достаточно большой зазор, очень удобный для хранения документов. Доступ к подобному тайнику для специалиста не представляет какой-либо трудности.

Для хранения информации часто используются лазерные диски. Лазерные диски внешне не отличаются от аудио- и видеодисков, что делает возможным их хранение среди музыкальной или видеоколлекции.

Поиск тайников с магнитными носителями затруднен тем, что нельзя использовать металлоискатель или рентгеновскую установку, поскольку их применение может привести к стиранию информации на носителях.

При наличии в осматриваемом помещении локальной сети следует точно установить местоположение серверов. Как правило, на крупных предприятиях под серверную выделена специальная комната, вход в которую ограничен. Однако помимо центральной серверной в подразделениях могут находиться местные локальные серверы. Определить местоположение компьютеров при наличии локальной сети поможет проводка. Достаточно проследить трассы кабеля или коробов (в случае, когда кабель спрятан в специальный короб).

Следует обратить внимание на неподключенные разъемы на коаксиальном кабеле и свободные розетки (розетки для подключения компьютеров в локальную сеть, использующие витую пару, имеют вид импортных телефонных розеток), так как в этих местах, возможно, находились компьютеры или подключались портативные компьютеры, которые в момент проведения обыска могут находиться в другом месте или были спрятаны.

Особое внимание следует обратить на места хранения дискет и других носителей информации. Если при внешнем осмотре компьютеров в их составе обнаружены устройства типа стримера, магнитооптического накопителя и им подобные, то необходимо найти места хранения носителей информации к соответствующим накопителям.

На предприятиях, имеющих развитую локальную сеть, как правило, производится регулярное архивирование информации на какой-либо носитель. Следует определить место хранения данных копий.

Специалист в области компьютерных средств, участвующий в осмотре, используя данные, полученные от системного администратора, должен произвести копирование информации на заранее приготовленные носители. Для этой цели удобнее всего использовать внешние жесткие диски или флеш-карты. Носители, на которые была переписана информация, должны быть упакованы в пластиковые коробки, если это жесткий диск, то его необходимо упаковать в антистатический пакет и предотвратить его свободное перемещение в упаковке при транспортировке, которую необходимо.

Следует иметь в виду, что для исследования больших вычислительных систем требуется значительное время. В процессе расследования возможны ситуации, когда физически невозможно перевезти компьютеры для их изучения и исследования. В таких случаях необходимо руководствоваться следующими рекомендациями:

1) после осмотра средств компьютерной техники необходимо обязательно блокировать не только соответствующее помещение, но и отключить источники энергопитания аппаратуры или, в крайнем случае, создать условия

лишь для приема информации с одновременным опломбированием всех необходимых узлов, деталей, частей и механизмов компьютерной системы;

2) при наличии магнитных носителей машинной информации их следует перемещать в пространстве и хранить только в специальных опломбированных и экранированных контейнерах или в стандартных дискетных или иных алюминиевых футлярах заводского изготовления, исключающих разрушающее воздействие различных электромагнитных и магнитных полей, направленных излучений.

В ходе процессуальной фиксации в протоколе следственного действия должна быть отражена следующая информация:

- наименование и назначение объекта, где совершено преступление;
- территориальное расположение объекта осмотра (на улице, в помещении, в банке, в магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контрольно-пропускном пункте и т. д.) и его ориентация относительно сторон света;
- ближайшее окружение объекта и подступы к нему — здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые) и расстояние до них; наличие дорог, подъездных путей (в т. ч. и водного транспорта), парковок и автостоянок; наличие линий и пунктов (колодцев, концентраторов т. д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло- , водо- и газоснабжения, вентиляции и т. д.);
- технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и состояние электрооборудования и др.);
- наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации — постов охраны, охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную территорию (неавтоматический, полуавтоматический или автоматический), освещения, металлических решеток, штор, жалюзи, рольставен, замков и запорных механизмов, экранов, заземлений, специальных стекол и пленок, генераторов шума, фильтров и т. д.;
- расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также других рабочих мест (если таковых несколько в одном помещении);

- расположение в одном помещении вместе с СВТ других электрических устройств и приборов — телефонных и иных аппаратов электросвязи, систем электрочасофикации, оргтехники (ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишущих машинок и т. п.), приборов электроосвещения (настольных, напольных, настенных, потолочных, подвесных и т. д.), абонентских громкоговорителей, телевизоров и мониторов, радиоприемников и магнитол, электроплиток, печей, чайников, кондиционеров и т. д.;
- наличие в одном помещении со СВТ линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (электросвязи, электропередачи, антенны провода, водо- и газоснабжения);
- наличие или отсутствие технических средств сопряжения СВТ с каналами электросвязи и между собой (на это могут указывать кабели и провода, которыми СВТ соединены между собой, а также с аппаратами или линией электросвязи);
- наличие или отсутствие соединений СВТ с оборудованием или вычислительной техникой, находящейся вне территории (помещения) осмотра; на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется);
- наличие на объекте, путях подхода и отхода следов преступления и преступника, специфическими среди которых являются: следы орудий взлома, повреждения, уничтожения и/или модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов, капли припоя, канифоли; следы проплавления, прокола, надреза изоляции проводов СВТ, наличие участков механического сдавливания и приклеивания сторонних предметов;
- наличие или отсутствие учетно-справочной документации к СВТ — технического паспорта и подобного ему документа; журнала оператора или протокола автоматической фиксации расчетно-кассовых и иных операций; журнала учета машинных носителей информации (МНИ), машинных документов, заказов (заданий или запросов); журнала (карточки) учета выдачи МНИ и машинных документов; журнала (карточки) учета массивов

(участков, зон), программ, записанных на МНИ; журнала учета уничтожения брака бумажных МНИ и машинных документов; актов на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов.

- тип, марка, конфигурация, цвет и заводской (инвентарный, учетный) номер изделия;
- тип (назначение), цвет и индивидуальные признаки соединительных и электропитающих проводов;
- состояние СВТ на момент проведения осмотра (выключено или включено);
- техническое состояние — внешний вид, целостность корпуса, комплектность СВТ - наличие и работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой, наличие расходных материалов, тип используемого машинного носителя информации и т. д. (проверку проводит соответствующий специалист);
- тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенных к нему электроприборов, число разъемов — розеток и т. д.);
- наличие заземления («зануления») СВТ и его техническое состояние;
- наличие и техническая возможность подключения к СВТ периферийного оборудования и/или самого СВТ к такому оборудованию, либо к каналу электросвязи (определяется специалистом по наличию у СВТ соответствующих портов и разъемов);
- повреждения, непредусмотренные стандартом конструктивные изменения в архитектуре строения СВТ, его деталей (частей, блоков), особенно те, которые могли возникнуть в результате происшествия или преступления, а также спровоцировать создание внештатной технической ситуации;
- следы преступной деятельности (орудий взлома корпуса СВТ, проникновения внутрь корпуса СВТ, пальцев рук, несанкционированного подключения к СВТ сторонних технических устройств, а также канифоли, припоя, флюсов и других химических веществ, обрезки монтажных проводов и изоляционных материалов, кровь, пот, волосы, волокна ткани и т. д.);
- расположение СВТ в пространстве относительно периферийного оборудования и других электротехнических устройств;

- точный порядок соединения СВТ с другими техническими устройствами;
- программу, исполняемую (или исполненную) компьютером на момент проведения (или до проведения) следственного действия. Для этого следует детально изучить и описать существующее на экране монитора компьютера изображение, все функционирующие при этом периферийные устройства и результат их деятельности. Многие сервисные программные средства позволяют определить и просмотреть наименование всех ранее вызывавшихся программ и исполненную в последнюю очередь. Например, с использованием TOTAL COMMANDER, последняя исполнявшаяся программа определяется по положению курсора;
- результат действия обнаруженной программы;
- манипуляции со средствами компьютерной техники (включая нажатия на клавиши клавиатуры), произведенные в процессе проведения следственного действия, и их результат (например, при копировании программ и файлов, определении их атрибутов, даты, времени создания и записи, а также при включении и выключении аппаратуры, отсоединении ее частей);
- категорию информации, циркулирующей в СВТ (общедоступная или конфиденциальная);
- наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нем информации от несанкционированного доступа;
- расположение рабочих механизмов СВТ и изображение на его экране (мониторе) или визуально-контрольном окне (для принтеров, контрольно-кассовых машин, контрольно — пропускных механизмов, цифровых аппаратов связи и т. д.) в том случае, если на момент осмотра они находится в рабочем состоянии;
- все основные действия, производимые специалистом при осмотре СВТ (порядок нажатия на клавиши и запорные механизмы, корректное приостановление работы и закрытие исполняемой операции или программы, выключение СВТ, отключение от источника электропитания, рассоединения или соединения СВТ и ее составляющих, отсоединение коммуникационных и электропитающих проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т. п.).

В ходе осмотра компьютерной техники следует учитывать возможность следующих негативных обстоятельств:

- возможные попытки со стороны персонала повредить ЭВМ с целью уничтожения информации и ценных данных;

- возможное наличие на компьютере специальных средств защиты от несанкционированного доступа, которые, не получив в установленное время специальный код, автоматически уничтожат всю информацию;
- наличие на ЭВМ иных средств защиты от несанкционированного доступа;
- постоянное совершенствование компьютерной техники, следствием чего может быть наличие на объекте новых программно-технических средств.

Кроме того, нередки попытки уничтожения преступником вещественных доказательств, в данном случае электронной информации. Так, например, может использоваться специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер требовать пароль периодически. При этом при отсутствии подтверждения данные в компьютере автоматически уничтожатся. Изобретательные владельцы компьютеров устанавливают иногда скрытые команды, удаляющие или архивирующие с паролями важные данные, если некоторые процедуры запуска машины не сопровождаются специальными действиями, известными только им[2].

С целью предотвращения возможных негативных последствий необходимо соблюдать следующие рекомендации:

- перед выключением питания по возможности корректно закрыть все используемые программы, а в сомнительных случаях просто отключить компьютер (в некоторых случаях некорректное отключение компьютера приводит к потере информации в оперативной памяти и даже к частичному стиранию информационных ресурсов на данном компьютере)[3];
- принять меры к установлению пароля доступа в защищенных программах;
- получать информацию у разных сотрудников путем опроса порознь. Такой метод позволит получить максимально правдивую информацию и избежать преднамеренного вредительства;
- при нахождении ЭВМ в локальной вычислительной сети необходимо иметь бригаду специалистов для быстрого реагирования на движение информации по сети;
- наряду с осмотром компьютера обеспечить осмотр документов о пользовании, в которых следует обратить особое внимание на рабочие записи операторов ЭВМ, так как именно в этих записях часто можно обнаружить коды, пароли и другую ценную для следствия информацию. При осмотре должен присутствовать кто-либо из сотрудников предприятия,

способный дать пояснения по установленному на ЭВМ программному обеспечению. Если на начальной стадии осмотра не удалось установить пароли и коды используемых программ, то компьютер подлежит опечатыванию и выемке, с тем чтобы в условиях лаборатории с привлечением специалистов-программистов выявить существующие пароли и коды доступа, осуществить надлежащий осмотр компьютера и содержащихся на нем файлов. В таких случаях достаточно изъять только системный блок, в который входят процессор и накопители на магнитных дисках. Остальную часть компьютера (монитор, клавиатуру, принтер) следует опечатать.

Недопустимо производить изъятие в несколько приемов. В том случае, если следователь не располагает необходимым транспортом, следует сделать несколько рейсов от объекта до места хранения изъятых материалов с выставлением охраны на объекте изъятия (охране подлежат СВТ и помещение, в котором они находятся).

Изъятые предметы и материалы не могут быть оставлены на ответственное хранение на самом объекте или в другом месте, где к ним могут иметь доступ посторонние лица.

Недопустимо оставлять на объекте части СВТ по причине их «абсолютной необходимости» в деятельности данного пользователя, как правило, такое желание указывает на наличие в них важной для следствия информации.

Следует изымать все СВТ, находящиеся в помещении объекта и несущие следы преступной деятельности.

В протоколе следственного действия должны обязательно фиксироваться конкретные признаки изымаемых СВТ (марка, быстродействие, марка процессора, объем памяти и т. д.)[4].

Изъятие средств компьютерной техники производится только в выключенном состоянии. При этом должны быть выполнены и отражены в протоколе следующие действия:

- установлено включенное состояние оборудования и зафиксирован порядок его отключения;
- описано точное местонахождение изымаемых предметов и их расположение относительно друг друга и окружающих предметов (с приложением необходимых схем и планов);
- описан порядок соединения между собой всех устройств с указанием особенностей соединения (цвет, количество, размеры, характерные индивидуальные признаки соединительных проводов, кабелей, шлейфов, разъемов, штекеров и их спецификация);
- определено отсутствие либо наличие компьютерной сети, используемый канал (каналы) связи и телекоммуникаций. В последнем случае

установлен тип связи, используемая аппаратура, абонентский номер, позывной либо рабочая частота;

- произведено разъединение (с соблюдением всех необходимых мер предосторожности) аппаратных частей (устройств) с одновременным опломбированием их технических входов и выходов;
- определен вид упаковки и транспортировки изъятых предметов.

Транспортировка и хранение компьютерной техники и информации должны осуществляться в условиях, исключающих ее повреждение, в том числе в результате воздействия металлодетекторов, используемых для проверки багажа в аэропортах. Хранят компьютеры и их комплектующие в сухом, отапливаемом помещении. Следует удостовериться, что в нем нет грызунов, которые часто являются причиной неисправности аппаратуры. Учитывая нестандартность обстановки, в которой может производиться осмотр места происшествия, вопрос о возможности изъятия компьютерной техники и информации, способе упаковки, транспортировки и хранении изъятых объектов решается следователем в каждом конкретно случае совместно со специалистом. Процессуальный порядок изъятия объектов определяется общими требованиями Уголовно-процессуального кодекса РК.

Осмотр машинного носителя информации (МНИ) может быть произведен в ходе осмотра места происшествия или как самостоятельное следственное действие.

Осмотр МНИ производится с участием специалиста и начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием. *К машинным носителям информации*, как правило, *относятся* магнитные диски (гибкие — дискеты, жесткие — «винчестеры», «банки» и «Zip»); оптические и магнитооптические компакт-диски (CD — «лазерные диски»); пластиковые карты (карточки); интегральные микросхемы (ИМС), в т. ч. находящиеся в различных СВТ в виде оперативной памяти (ОЗУ) и/или постоянного запоминающего устройства (ПЗУ) — персональных компьютерах, сотовых и иных аппаратах электросвязи, электронных записных книжках, электронных переносных справочниках и переводчиках, контрольно-кассовых аппаратах, банкоматах, контрольно-пропускных устройствах, смарт-картах и т. д.).

В ходе осмотра МНИ подлежит изучению и фиксации следующая информация.

Тип, вид, марка, назначение, цвет и заводской номер (или учетный номер носителя).

Наличие индивидуальных признаков и техническое состояние футляра (коробки, упаковки, специального технического устройства) — тип, разме-

ры, цвет, материал, физические повреждения, наклейки, принцип функционирования, емкость и т. д.

Техническое состояние — размеры носителя, внешний вид, материал каркаса носителя, его целостность и индивидуальные признаки, материал основного информационно-несущего слоя и его целостность (механические повреждения — царапины, деформации и т. д.), наличие и положение (сохранность) приспособлений от несанкционированного уничтожения (перезаписи) информации (ключей, пломб, заглушек, маркеров), наличие и техническое состояние механизмов защиты информационно-несущего материала (отверстий окон для считывания и записи информации).

Наличие, размеры, цвет, марка и техническое состояние разъемов для подключения к специальному считывающему устройству.

Присутствие внешней спецификации, ее цвет и размеры (заводские или пользовательские наклейки с текстом или специальными пометками).

Наличие индивидуальных признаков защиты носителя от несанкционированного использования (тип — голография, штрихкод, флюоресцирование, перфорация, ламинирование, вплавление личной подписи пользователя и т. д.; размеры, цвет, вид).

Признаки материальной подделки МНИ и их защиты: подчистки, травления, следы термического воздействия, переклеивания (склеивания, наклеивания, заклеивания), дописки, замены, перепайки и т. д.

Работоспособность и внутренняя спецификация — серийный номер, метка тома, либо код; размер разметки (для дисков — по объему записи информации, для лент — по продолжительности записи); размер области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров, цилиндров; количество записанных программ, файлов, каталогов (подкаталогов), данных, их структура, название (имя и/или расширение), размер и объем, который занимают их названия, дата и время создания (или последнего изменения), а также специальная метка или флаг (системный, архивный, скрытый, только для чтения или записи и т. д.); наличие скрытых или ранее стертых файлов (программ) и их реквизиты (название, размер, дата и время создания или уничтожения).

Содержимое осмотренных файлов (программ, компьютерной информации), записанных на МНИ или находящихся в оперативной памяти СВТ и имеющих значение для дела.

В протоколе осмотра должны быть зафиксированы:

- все манипуляции (нажатия на клавиши и т. д.) со средствами вычислительной техники, совершенные в процессе осмотра.

- индивидуальные признаки СВТ, используемых в процессе осмотра, — тип, вид, марка, название, заводской или регистрационный (учетный) номер и т. п.
- ссылка на то, что используемые в процессе осмотра СВТ перед началом следственного действия были тестированы специалистом на предмет отсутствия в них вредоносных программных и аппаратных средств.

Цели осмотра машинного документа — выявление и анализ внешних признаков и реквизитов документа, снятие и анализ содержащейся информации, обнаружение возможных признаков его подделки (фальсификации).

В современных условиях электронная информация может иметь достаточно разнообразную форму. Электронные документы приобретают вид текста, звукозаписи, изображения. Кроме того, различны и целевые характеристики — передача во времени, в пространстве, хранение (запоминание), использование. Они отражены в содержании документа. В компьютерных (автоматизированных) системах документ — любой объект, находящийся в памяти компьютера. В условиях развития «высоких технологий» возникают принципиально новые носители информации, совершается постепенный переход к «бездокументарному управлению» — без традиционного бумажного документа. Эти явления могут использоваться в преступных целях. Возникает потребность совершенствования средств обнаружения новых документов, закрепленных на нетрадиционных носителях, и, в случае необходимости, их изъятия, прочтения и осмотра.

Осмотр документа на машинном носителе и машинограмме, создаваемым СВТ, производится с участием специалиста (или группы специалистов) в зависимости от сферы (области) деятельности, в которой используется осматриваемый документ (кредитно-финансовая, банковская, расчетно-кассовая, услуг, охраны и т. д.).

В ходе осмотра документа должны быть выявлены следующие данные:

- наименование (назначение) документа (например, идентификационный код и наименование формы документа по классификатору[5]);
- тип используемого машинного носителя, его индивидуальные признаки и техническое состояние;
- тип, марка, конфигурация и техническое состояние аппаратного и программного оборудования, других технических устройств, применявшихся при осмотре;
- наличие сопроводительного письма или документа, его заменяющего (например, договора на использование пластиковой карточки или регистрационного сертификата на использование электронно-цифровой подписи[6]);

- форма записи содержания документа (человекочитаемая, закодированная в машинном формате, смешанная);
- реквизиты организации (лица) создателя документа (наименование и юридический адрес);
- наличие грифа ограничения доступа к документу на машинном носителе или машинограмме («конфиденциально», «для служебного пользования», «секретно», «совершенно секретно»);
- регистрационный номер документа и/или машинного носителя (заводской номер, серийный номер тома, метка тома);
- дата изготовления (создания) или выдачи документа (с указанием времени записи документа на МНИ, позволяющим идентифицировать ее с машинным протоколом);
- размер документа (линейный или объемный — по количеству символов или общему объему символов в документе в байтах) и/или количество страниц;
- на чье имя выдан (реквизиты адресата-получателя);
- какими реквизитами заверен (электронно-цифровой подписью; кодом (позывным) лица, ответственного за правильность изготовления, копирования или передачу документа по телекоммуникационным каналам; собственноручной подписью уполномоченного лица; печатью; индивидуальным кодом абонента сети дистанционной передачи данных — «электронной почты»; специальным позывным кодом аппаратуры связи);
- индивидуальные признаки документа (название файла — программы); структура расположения символов; машинный формат текста (формат MS DOS, WORD for WINDOWS и т. д.); наличие маркеров страниц, выделений текста; тип и цвет печати (матричный, струйный, электрографический, смешанный) указать конкретно для каждого элемента; наличие защитных знаков и т. д.);
- признаки подлога и материальной подделки документа и его носителя.

---

[1] *Осипенко М.* Компьютеры и преступность // Информационный бюллетень НЦБ Интерпола в Российской Федерации. — 1994. — № 10. — С. 16.

[2] *Осипенко М.* Компьютеры и преступность // Информационный бюллетень НЦБ Интерпола в Российской Федерации. — 1994. — № 10. — С. 149.

[3] *Россинская Е. Р., Усов А. И.* Судебная компьютерно-техническая экспертиза. — М., 2001. — С. 399-411.

[4] *Катков С. А., Собецкий И. В., Фёдоров А. Л.* Подготовка и назначение программно-технической экспертизы // Информ. бюллетень СК МВД России. — 1995. — № 4 (85). — С. 92-96.

[5] Постановление Кабинета министров Республики Казахстан. «Об утверждении Основных правил документирования и управления документацией в объединениях (предприятиях),

учреждениях и организациях всех организационно-правовых форм Республики Казахстан» от 30 июня 1992 г — Алматы, 1992.

[6] Закон Республики Казахстан «Об электронном документе и электронной цифровой подписи» от 7 января 2003 г. // Каз. правда. 2003. 10 января.

Подписано в печать 26.04.2010.
Формат 64×80 $^{1}/_{16}$. Печать офсетная. Бумага офсетная.
Тираж 100 экз. Заказ № 400.

Отпечатано в типографии КарЮИ МВД РК им. Б. Бейсенова.
г. Караганда, ул. Ермекова, 124