АНО ВО
«Российский новый университет»
Тамбовский филиал

392002, г. Тамбов, ул. Пензенская, д. 61/175, к. 3, тел. (4752)77-10-65

С.И. Молчанова

ОСОБЕННОСТИ РАБОТЫ С ЭЛЕКТРОННЫМИ НОСИТЕЛЯМИ В ПРОЦЕССЕ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ

Учебное пособие для студентов, обучающихся по направлению подготовки «Юриспруденция», уголовно-правовой профиль

Тамбов
2022

УДК 343
ББК 67.52
М 76

Автор-составитель:
Молчанова С.И., к.ф.н., доцент кафедры уголовно-правовых дисциплин Тамбовского филиала АНО ВО «Российский новый университет», эксперт АНКО «Тамбовский Центр судебных экспертиз»

Рецензент:
Иванов Сергей Александрович - к.ю.н., преподаватель АНО СПО «Колледж права и безопасности».

М76*.Молчанова С.И. Особенности работы с электронными носителями в процессе раскрытия и расследования преступлений. Учебно-методическое пособие для студентов, обучающихся по направлению подготовки 40.03.01 «Юриспруденция» /Молчанова С.И. –2022 г. –57 с.*

Учебное пособие составлено в соответствии с требованиями ФГОС ВО и предназначено для студентов, обучающихся по образовательной программе бакалавриата 40.03.01 Юриспруденция для получения ими практических умений и навыков по освоению дисциплины «Криминалистика», «Уголовный процесс», а также при подготовке к зачетам и экзаменам по данным учебным дисциплинам.

В пособии представлены ситуации из практической деятельности при которых требуется принятие решения по тактике проведения следственных действий, использовании специальных приемов и методов их проведения, а также по выдвижению версий и планированию расследования.

Пособие может представлять интерес для студентов юридических вузов, практикующих юристов, особенно начинающих, а также для более широкого круга читателей, не имеющих специальной юридической подготовки и опыта работы в проведении расследования преступлений.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Анализ состояния дел в отраслях хозяйства и управления страны свидетельствует о том, что за последние 15-20 лет в числе выявленных корыстных преступлений широкое распространение получили преступные посягательства, связанные с использованием разнообразных средств электронно-вычислительной техники (СВТ) во многих технологических процессах. Например, массовый характер приобрели хищения наличных и безналичных денежных средств в крупных и особо крупных размерах в учреждениях, организациях и на предприятиях всех форм собственности, применяющих автоматизированные компьютерные системы для обработки и электронной передачи данных первичных бухгалтерских документов, отражающих кассовые операции, движение материальных ценностей и другие разделы учета.

Приходится констатировать, что процесс компьютеризации общества привел к возникновению новых видов преступных посягательств, ранее не известных отечественной юридической науке и практике, связанных с использованием средств электронно-вычислительной техники и информационно-обрабатывающих технологий. Данные преступления стали называться *компьютерными*, исходя из аналогов и терминологии зарубежной юридической практики. Как свидетельствует статистика, в последнее время количество компьютерных преступлений неуклонно увеличивается, возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от обычных видов преступлений.

Анализируя нынешнее развитие ситуации с точки зрения будущего, специалисты прогнозируют рост организованной преступности, связанной с использованием в корыстных целях электронных средств, одним из которых является персональный компьютер. Предполагается, что в ближайшее время различные учреждения и организации все больше будут полагаться на обработку данных с помощью ЭВМ и новых информационных технологий. По мере развития техники все большее число стран будет подключаться к существующим и вновь образуемым компьютерным информационным сетям, на которых в настоящее время базируется вся мировая экономика, что неизбежно приведет к появлению у преступных групп и сообществ еще большего желания обогатиться. По данным ФБР США, российские специалисты - компьютерщики, входящие в состав отечественных преступных групп и сообществ, осуществляющих свою преступную деятельность на территориях США и западноевропейских стран и обладающих достаточным финансовым и кадровым потенциалом, без особого труда могут «взломать» почти любые коды и получить

неправомерный доступ к коммерческим секретам крупнейших многонациональных корпораций. В результате таких действий десятки миллионов долларов в считанные минуты незаконно снимаются со счетов корпораций и переводятся на оффшорные счета, используемые преступниками. Согласно оценкам специалистов, ежемесячно совершается около тысячи подобных «операций», проследить за которыми ни отечественные, ни зарубежные правоохранительные органы пока не могут.

Расследование подобных преступлений вызывает серьезные затруднения в документировании преступной деятельности, выявлении преступников, требует привлечения специалистов в области вычислительной техники, новейших средств электросвязи и защиты конфиденциальной информации. В настоящее время по данным делам работает созданное в 1999 году отдельное управление по борьбе с преступлениями в сфере высоких технологий.

1. ОСОБЕННОСТИ ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ В ЦЕЛЯХ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

К следственным действиям, которые по делам о преступлениях, совершаемых с использованием средств электронно-вычислительной техники, отличаются наибольшей спецификой, относятся:

- осмотр места происшествия;
- осмотр средства вычислительной техники;
- осмотр машинного носителя информации (МНИ);
- осмотр машинного документа;
- обыск и выемка;
- назначение экспертиз.

Проводятся они в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом некоторых особенностей.

Осмотр места происшествия

При осмотре места происшествия в ***состав следственно - оперативной группы*** (СОГ) в зависимости от конкретной следственной ситуации должны входить следующие лица:

- следователь, специализирующийся на расследовании уголовных дел рассматриваемой категории - руководитель СОГ;

- специалист-криминалист, знающий особенности работы со следами преступлений данной категории;

- специалист по СВТ;

-сотрудник Гостехкомиссии России (в случае совершения преступления в отношении юридического лица и/или наличия специальных средств защиты информации и СВТ) или оперативно-технического подразделения правоохранительного органа;

- специалист по сетевым технологиям СВТ (в случае наличия на месте происшествия периферийного оборудования удаленного доступа или локальной компьютерной сети);

- специалист по системам связи (при использовании для дистанционной передачи данных каналов электросвязи);

- оперативные сотрудники (ОУР, ОБЭП, налоговой полиции, ФСБ);

- участковый инспектор, обслуживающий данную территорию;

- инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, являются охраняемыми объектами).

При необходимости для участия в осмотре места происшествия могут быть приглашены и другие незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, бухгалтеры со знанием СВТ, специалисты спутниковых систем связи, операторы компьютерных систем и сетей - сотовых, пейджинговых, Интернет и др. - и т.д.).

Рассматриваемое следственное действие должно быть заблаговременно подготовлено и детально спланировано, ***необходимо предварительно провести следующую работу:***

1. С учетом сложившейся следственной ситуации, наметить круг лиц, участвующих в осмотре;

2. Определить последовательность действия лиц при осмотре места происшествия;

3. Пригласить соответствующих квалифицированных специалистов;

4. Перед началом осмотра разъяснить цели проведения следственного действия и задачи, стоящие перед специалистами, а также их права и обязанности;

5. 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.

Цель осмотра места происшествия - установление конкретного СВТ, выступающего в качестве предмета и/или орудия совершения преступления и имеющего следы преступной деятельности. При производстве следственного действия целесообразно использовать тактический прием «от центра - к периферии», где «центром» (отправной точкой осмотра места происшествия) являются СВТ, находящиеся на месте осмотра.

По прибытию на место происшествия, следователь должен проделать следующую работу:

1. Удалить с места происшествия всех посторонних лиц и организовать его охрану, если этого не было сделано. Обязательной охране подлежат такие объекты:

- территория места происшествия;

- все СВТ, находящиеся на территории (в помещении);

- пункты отключения электропитания СВТ, находящиеся в здании (учреждении, организации, на территории).

Следователю необходимо знать, что к изменению или уничтожению информации (следов) может привести не только работа за пультом управления СВТ (клавиатурой), но и включение-выключение СВТ или разрыв соединения между ними. Поэтому, если на момент производства следственного действия какие-либо СВТ и иные электротехнические приборы

и оборудование были включены или выключены, то они должны оставаться в таком состоянии до момента окончания осмотра их специалистом.

2. 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.

В протоколе осмотра следует отразить следующие фактические данные:

- 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, коробов, потерн и 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 фактическое состояние устройств электропитания 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, тепло-, 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 или флюса; 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.

Осмотр средства вычислительной техники

Осмотр СВТ, участвовавшего в преступлении, ***производят для достижения следующих целей*:**

1. Обнаружения следов, образовавшихся в результате происшествия или совершения преступления, и других вещественных доказательств для установления, кем, с какой целью и при каких обстоятельствах было совершено преступление;

2. Выяснения обстановки происшествия для восстановления механизма совершения преступления;

3. Установления технического состояния СВТ.

При 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);

- операторы СВТ - ЭВМ, пейджинговой и сотовой связи, контрольно-кассовых аппаратов, бухгалтер по приему и отправке электронных платежей и т. д. (для наружного осмотра СВТ);

- сотрудник Гостехкомиссии России (для осмотра специальных технических средств защиты выделенных помещений, СВТ и информации от несанкционированного доступа, утечки и съема, а также обнаруженной специальной разведывательной аппаратуры негласного получения информации);

- инженер-программист (для осмотра программного обеспечения СВТ, определения принципа его функционирования, установления следов преступной деятельности в среде машинной информации).

Отметим, что во избежание уничтожения (повреждения) СВТ и следов преступления при работе специалиста - криминалиста по осмотру СВТ недопустимо использование магнитосодержащих материалов, инструментов, приборов и оборудования, направленных

источников электромагнитного излучения (магнитного порошка, магнитной кисточки, электромагнита, металлодетектора, мощных ламп освещения, мощных УФ и ИК излучателей, и т.д.), а также кислотно-щелочных материалов и нагревательных приборов. При осмотре места происшествия и при производстве других следственных действий вышеуказанными материалами и оборудованием можно пользоваться с особой осторожностью на расстоянии более 1 метра от СВТ и их соединительных проводов.

***В протоколе осмотра СВТ фиксируются следующие данные*:**

- тип, марка, конфигурация, цвет и заводской номер (или 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 (привести к возникновению происшествия);

- 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;

- категорию информации, циркулирующей в СВТ (общедоступная или конфиденциальная);

- наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нем информации от несанкционированного доступа, съема и утечки (особенно тех из них, которые автоматически уничтожают информацию и МНИ при нарушении процедуры доступа к СВТ, порядка их использования и/или правил работы с информацией) определяется специалистом Гостехкомиссии России;

- 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, корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения или соединения СВТ и ее составляющих, отсоединения коммуникационных и электропитающих проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.).

Осмотр машинного носителя информации

Осмотр машинного носителя информации 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 относятся:

- магнитные диски (гибкие дискеты, жесткие «винчестеры», «банки» и «Zip»);

- оптические и магнитооптические компакт-диски (CD - «лазерные диски»);

- бумажные перфоленты и магнитные ленты (в бобинах и кассетах);

- бумажные перфокарты и магнитные карты (поштучно и в «колодах», комплектах);

- пластиковые карты (карточки);

- интегральные микросхемы (ИМС) в виде оперативной памяти (ОЗУ) и/или постоянного запоминающего устройства (ПЗУ), в т. ч. находящиеся в различных СВТ (персональных компьютерах, пейджерах, 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 протоколе осмотра должны быть зафиксированы следующие фактические данные*:**

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

2. Наличие, индивидуальные признаки и техническое состояние футляра (коробки, упаковки, специального технического устройства) - тип, размеры, цвет, материал, физические повреждения, наклейки, принцип функционирования, емкость и т.д.

3. 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, нарушения несущего слоя 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).

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

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

6. Наличие, индивидуальные признаки защиты носителя от несанкционированного использования (тип - голография, штрихкод, эмбосинг, флуоресцирование, перфорация, ламинирование, вплавление личной подписи пользователя и т. д.; размеры, цвет, вид).

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

8. Работоспособность и внутренняя спецификация - серийный номер и/или 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).

9. Результат осмотра содержимого файлов (программ, компьютерной информации), записанных на МНИ или находящихся в оперативной памяти СВТ и имеющих значение для дела.

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

11. Индивидуальные признаки СВТ, используемых в процессе осмотра, - тип, вид, марка, название, заводской или регистрационный (учетный) номер и т.п.

12. 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.

Осмотр машинного документа

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.).

Цели осмотра - выявление и анализ внешних признаков и реквизитов документа, анализ его содержания, обнаружение возможных признаков его подделки (фальсификации).

При подготовке к проведению данного следственного действия следователю необходимо ознакомиться с требованиями *ГОСТ 6.10.4-84 от 01.07.87 г. «УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения».* Этим нормативным актом определяются требования к составу и содержанию реквизитов, придающих юридическую силу документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники; порядок внесения изменений в эти документы; транспортирования (передачи, пересылки и т.д.) машинных документов, их записи на МНИ; система приема по каналам электросвязи, воспроизведения машинного документа на машинограмму, создания копий и дубликатов машинных документов.

Документы, используемые в документообороте юридических лиц (учреждений, организаций, предприятий и т.д.) могут создаваться как для внешнего, так и внутреннего пользования. Однако в соответствии с требованиями *ГОСТ 6.38-72 «Система организационно - распорядительной документации. Основные положения»,* рассматриваемые документы должны всегда иметь следующие реквизиты: наименование

юридического лица, выдавшего (или создавшего) документ; номер документа и дата его составления; заголовок; адресат; содержание; подпись и печать на документах, требующих особого удостоверения их подлинности (или код лица, утвердившего документ).

В соответствии со статьей *160 Гражданского кодекса Российской Федерации* допускается использование для удостоверения подлинности юридических документов факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи (ЭЦП) либо иного аналога собственноручной подписи физического лица.

В частности, порядок использования ЭЦП определяется *ГОСТ Р 34.10.94 «Электронная цифровая подпись (ЭЦП)».* Электронная подпись дает возможность не только гарантировать аутентичность документа в части его авторства путем электронно-цифровой фиксации основного текста и личностных характеристик подписи физического лица, утвердившего документ, но и установить факт неискаженности (целостности) содержащейся в нем информации, а также зафиксировать попытки подобного искажения. Электронная подпись, состав которой непосредственно зависит от заверяемого текста, соответствует только этому тексту при условии, что его никто не изменял. Проверочная сумма (хэш-функция) измененного (фальсифицированного) электронного документа отличается от проверочной функции, которая получается в результате обработанного преобразования электронной подписи. Алгоритм криптографического преобразования данных в ЭВМ, системе ЭВМ или их сети с помощью ЭЦП определяется *ГОСТ Р 34.11.94 «Функция криптографического преобразования данных (хэш-функция)».* Переданный получателю подписанный документ состоит из текста, электронной подписи и сертификата пользователя, который содержит в себе гарантированно подлинные данные пользователя, в том числе его отличительное имя и открытый ключ расшифрования для проверки подписи получателем либо третьим лицом, осуществившим регистрацию сертификата.

На документы, создаваемые СВТ, распространяется также *ГОСТ 13.002-79 «Микрофильм на правах подлинника. Основные положения».*

Порядок работы с некоторыми видами документов, создаваемых СВТ, может регулироваться, кроме вышеуказанных, межотраслевыми, внутриотраслевыми и другими нормативными актами (например, приказом по объединению, учреждению, организации, предприятию, возлагающим обязанности по удостоверению документов определенной категории на конкретное должностное лицо или работника).

В протоколе осмотра документа должны быть отражены следующие данные:

1. Наименование (назначение) документа (например, идентификационный код и наименование формы документа по классификатору ОКУД).

2. Тип используемого машинного носителя, его индивидуальные признаки и техническое состояние.

3. Тип, марка, конфигурация и техническое состояние аппаратного и программного оборудования, других технических устройств, применявшихся при осмотре.

4. Наличие сопроводительного письма или документа, его заменяющего (например, договора на использование пластиковой карточки или регистрационного сертификата на использование ЭЦП).

5. Форма записи содержания документа (человекочитаемая, закодированная в машинном формате, смешанная).

6. Реквизиты организации (лица) создателя документа (наименование и юридический адрес).

7. Наличие грифа ограничения доступа к документу на машинном носителе или машинограмме («конфиденциально», «для служебного пользования», «секретно», «совершенно секретно»).

8. Регистрационный номер документа и/или машинного носителя (заводской номер, серийный номер тома, метка тома).

9. Дата изготовления (создания) или выдачи документа (с указанием времени записи документа на МНИ, позволяющим идентифицировать ее с машинным протоколом).

10. Размер документа (линейный или объемный - по количеству символов или общему объему символов в документе в байтах) и/или количество страниц.

11. На чье имя выдан (реквизиты адресата-получателя).

12. Какими реквизитами заверен (ЭЦП; 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).

13. 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.).

14. Выявленные при осмотре признаки подлога и материальной подделки документа и его носителя.

Изъятие средств вычислительной техники, машинных носителей информации, компьютерной информации как элемент отдельных следственных действий

Изъятие СВТ, машинных носителей информации и компьютерной информации должно происходить при непосредственном участие соответствующих специалистов. При этом следователь должен обеспечить строгое соблюдение требований уголовно-процессуального законодательства, иначе изъятые при производстве следственного действия СВТ, материалы и документы впоследствии не смогут выступать в качестве доказательств по делу.

Для успешного осуществления вышеуказанного требования ***необходимо придерживаться следующих рекомендаций:***

1. По ходу проведения следственного действия необходимо постоянно акцентировать внимание понятых на все производимые специалистами манипуляции и их результаты.

2. Фактическое изъятие СВТ, находящихся на момент их осмотра во включенном состоянии, производится только после того, как будут выполнены и отражены в протоколе следственного действия такие мероприятия:

- определено и корректно приостановлено выполнение вычислительной операции;

- информация, находящаяся в оперативной памяти СВТ, записана на его постоянный МНИ, либо на специально подготовленный и тестированный для этих целей внешний МНИ;

- определены и корректно закрыты все исполняемые программы (в некоторых случаях некорректное отключение СВТ, путем его перезагрузки или выключения электропитания, без предварительного выхода из исполняемой программы приводит к потере информации, нарушению конфигурации вычислительной системы, стиранию всех информационных ресурсов на данном СВТ);

- выключено электропитание СВТ и всех его периферийных устройств;

- все электропитающие и соединительные провода и кабели, имеющие разъемное соединение, отсоединены от СВТ, источника питания и периферийного оборудования с обязательным указанием в протоколе порядка их соединения (принципиальная схема), отсоединения и индивидуальных признаков каждого элемента.

3. Изымаемые СВТ и их составляющие следует опечатывать так, чтобы исключить возможность непроцессуальной работы с ними, разукомплектовки и физического повреждения. Для достижения данной цели необходимо сделать следующее:

- опечатать аппаратуру и технические устройства путем наложения листа бумаги на разъёмы электропитания и подключения периферийного оборудования (порты) с захлестом на боковые панели корпуса изымаемого устройства и закреплением их краев густым клеем;

- в случае отсутствия у СВТ электропитающего и соединительного (портового) разъемов наложить лист бумаги или бумажный конверт (колпак) на штепсельную и/или соединительную вилку, зафиксировать его клеем или бечевой на корпусе провода у основания вилки;

- лист (полоску) бумаги-пломбы следует также наложить на все разъемные детали корпуса СВТ и его составляющих, скрепив их между собой, и зафиксировать клеем (на прорезь дисковода, щель приемного устройства, лицевой и боковой панелях, тыльной панели и корпусе и т.п.);

- при наличии картонных коробок, ящиков, бумажных канцелярских или почтовых мешков и больших конвертов изымаемые СВТ можно запаковать в них без соблюдения требований, отмеченных в вышеприведенных пунктах, но обязательно опломбировать все соединительные швы и сделать опись вложения;

- на листах пломбирующей бумаги, на пломбах или упаковке должны быть подписи следователя, понятых и специалиста, участвующего в изъятии;

- МНИ, документы, технические устройства, соединительные (или электропитающие) провода и кабели вместе с разъемными устройствами надо упаковать отдельно друг от друга, сделать точное описание каждого в протоколе индивидуальных признаков и опись вложения для каждой единицы тары;

- при отсутствии четких внешних признаков изымаемый предмет следует запечатать в отдельную коробку (ящик, конверт), сделать об этом обязательную отметку в протоколе проведения следственного действия.

4. При изъятии магнитного носителя машинной информации нужно помнить, что он должен перемещаться в пространстве и храниться исключительно в специальном экранированном контейнере или алюминиевом футляре (оболочке), исключающем разрушающее воздействие различных электромагнитных и магнитных полей и направленных излучений. Для этого магнитные носители информации сначала упаковывают в пакет из обычной фольги (бытового или технического назначения), а затем опечатывают обычным способом, вкладывая в коробку или конверт. В качестве контейнера можно использовать цельноалюминиевую коробку с крышкой (например, алюминиевую посуду с крышкой из того же материала). Если в коробку упаковывается несколько носителей информации, то всегда составляется опись вложения с указанием индивидуальных признаков каждого носителя.

5. Недопустимо приклеивать что-либо непосредственно к МНИ и документам, пропускать через них бечеву, пробивать стиплером, делать пометки или маркировки,

накалывать твердым предметом знаки, использовать пластилиновые или сургучовые печати и т. д.

6. При изъятии печатающих устройств (принтеров), особенно матричного (игольчатого) типа, их необходимо упаковывать в отдельные коробки (мешки, конверты) вместе с расходными материалами (красящими лентами, картриджами, бумагой), зафиксировав в том положении, в котором они находились на момент производства следственного действия.

7. В случае невозможности изъятия и приобщения к делу в качестве вещественного доказательства средства вычислительной техники (например, если СВТ является элементом компьютерной сети или системы дистанционной обработки информации), необходимо с помощью специалиста отключать его от источников удаленного доступа или, в крайнем случае, создать условия лишь для приема информации, полностью исключив возможность ее передачи (отправки). Идеальным вариантом изъятия СВТ в подобной ситуации является включение в телекоммуникационную сеть дублирующего СВТ с программно - аппаратными характеристиками, аналогичными изымаемому, после чего требуемое устройство отключается от сети и изымается. Такую технически сложную операцию может выполнить только квалифицированный специалист или группа специалистов, задействованных в следственном действии.

8. Если же возникла необходимость изъятия информации из оперативной памяти СВТ (непосредственно из оперативного запоминающего устройства - ОЗУ или из виртуального диска СВТ), то сделать это можно только путем копирования соответствующей информации на МНИ с использованием стандартных, специально подготовленных и тестированных программных и аппаратных СВТ, тактико-технические характеристики и индивидуальные признаки которых обязательно должны быть отражены в протоколе проведения следственного действия. Процесс изъятия должен быть зафиксирован с использованием видеозаписи.

9. Как показывает практика, при изъятии СВТ у следователя могут возникать конфликты с пользователем. При их разрешении необходимо руководствоваться следующими рекомендациями:

- 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 неизъятые 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, желание сохранить от изъятия определенные СВТ 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.).[1]

Стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных со СВТ, средствами и системами их защиты, необходимо в обязательном порядке получать и анализировать с участием специалистов информацию о технологических особенностях функционирования вышеприведенных технических устройств, уровня их соподчиненности и используемых средств связи и телекоммуникации во избежание их разрушения, нарушения заданного технологического ритма и режима функционирования причинения крупного материального ущерба пользователям и собственникам, уничтожения доказательств.

Осмотр места происшествия, средства вычислительной техники, машинного носителя информации и документа необходимо проводить в строгой последовательности, уделяя особое внимание тем частям предметов, на которых имеются повреждения и следы, и с обязательным использованием фото- и/или видеосъемки. Важно сфотографировать или произвести видеозапись не только места происшествия, отдельных объектов, СВТ и их соединений, но и все действия специалистов, участвующих в осмотре.

К протоколу осмотра прилагаются план или схема места происшествия, принципиальная схема соединения СВТ между собой и с каналами электросвязи (со спецификацией и расшифровкой условных обозначений), фото- видеопленка или магнитный носитель информации (лента, дискета или жесткий диск), распечатка информации.

Обыск и выемка

Обыск по делам о преступлениях, совершаемых с использованием СВТ, в большинстве случаев является неотложным следственным действием и требует тщательной подготовки.

На подготовительном этапе обыска следователю необходимо осуществить следующие мероприятия:

---

[1] ***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.

- выяснить, какие СВТ находятся в помещении, намеченном для проведения обыска (по возможности установить их тактико-технические характеристики);

- установить, какие средства защиты информации и СВТ от несанкционированного доступа находятся по месту обыска (по возможности - выяснить ключи доступа и тактико-технические характеристики средств защиты);

- определить режим и технические системы охраны объекта, СВТ и категорию обрабатываемой информации (общедоступная или конфиденциальная);

- выяснить, какие средства связи и телекоммуникаций используются для работы СВТ и информационного обмена - установить их тип, тактико-технические характеристики, категорию (общедоступные или конфиденциальные), абонентские номера, позывные, ключи (коды) доступа и т.п.;

- установить тип источников электропитания вышеперечисленных технических средств (электросеть, автономные, бесперебойные - комбинированные) и расположение пунктов обесточивания помещения и аппаратуры, подлежащих обыску;

- пригласить соответствующих специалистов для подготовки и участия в следственном действии;

- подготовить соответствующие СВТ, специальную аппаратуру и материалы для поиска, просмотра, распаковки, расшифровки, изъятия и последующего хранения машинной информации, СВТ и специальных технических устройств;

- определить дату, время и границы проведения обыска, время поиска и меры, обеспечивающие его конфиденциальность (важно, чтобы пользователь, владелец или оператор СВТ не подозревал о предстоящем следственном действии и не работал в момент проведения обыска на СВТ);

- проинструктировать оперативных сотрудников и видеооператора о специфике проводимого следственного действия;

- по возможности изучить личность обыскиваемого, пользователя (владельца) СВТ, вид его деятельности, профессиональные навыки по владению СВТ;

- пригласить понятых, обладающих специальными познаниями в области автоматизированной обработки информации.

По прибытии к месту проведения обыска необходимо вести себя следующим образом:

- быстро и внезапно войти в обыскиваемый объект (или одновременно в несколько помещений);

- при оказании сопротивления со стороны лиц, находящихся на объекте обыска, - обыскиваемого, его родственников, охранников (сторожей), сотрудников организации и т.п. -

принять срочные меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение;

- организовать охрану места обыска и наблюдение за ним; охране подлежат периметр обыскиваемых площадей, СВТ, хранилища МНИ, все пункты (пульты) связи, охраны и электропитания, находящиеся на объекте обыска (в здании, помещении, на производственной площади), специальные средства защиты от несанкционированного доступа, хранилища ключей аварийного и регламентного доступа к СВТ, помещениям и другим объектам (пульты, пункты, стенды, сейфы и т.п.).

Следователю необходимо знать, что к изменению или уничтожению машинной информации, ее носителей и СВТ, которые впоследствии могут выступать в качестве доказательств по делу, приводят не только манипуляции с самими СВТ, но и включение или выключение их электропитания. Поэтому все электротехническое оборудование и средства электротехнических систем, имеющиеся на месте обыска, должны находиться до момента их осмотра специалистом в том пространственном положении и техническом состоянии, в котором они были в момент начала обыска. *Для этого необходимо соблюдать следующие условия*:

- не разрешать кому бы то ни было из находящихся на объекте обыска лиц (за исключением приглашенных специалистов), прикасаться к СВТ и источникам питания электрооборудования с любой целью, даже в случае согласия обыскиваемого добровольно выдать искомый предмет, документ или информацию;

- не разрешать кому бы то ни было без разрешения специалиста выключать-включать электроснабжение объекта;

- в случае если на момент начала обыска электроснабжение объекта выключено, то до его восстановления следует отключить от электросети все СВТ, предварительно зафиксировав в протоколе схему их подключения к источникам электропитания, расположение, тактико-технические характеристики и порядок отсоединения от них СВТ;

- не производить самостоятельно никаких манипуляций с электрооборудованием и СВТ, если результат их заранее неизвестен;

- при настойчивых попытках обыскиваемого или других лиц, находящихся на месте обыска, получить доступ к СВТ, пунктам связи, управления и энергоснабжения, к другим техническим средствам и оборудованию следует принять меры для удаления этих лиц в другое помещение (не подлежащее обыску) с одновременной фиксацией в протоколе данного события.

***На обзорной стадии обыска необходимо*:**

1. Определить и отключить специальные средства защиты информации и СВТ от несанкционированного доступа, особенно те, которые автоматически уничтожают информацию и МНИ при нарушении процедуры доступа к СВТ и машинной информации, порядка их использования и/или установленных правил работы с ними; принять меры к установлению пароля, ключа санкционированного доступа и шифрования-дешифрования информации.

2. Установить наличие телекоммуникационной связи между СВТ, СВТ и каналами электросвязи по схемам «компьютер - компьютер», «компьютер - управляющий компьютер», «компьютер - периферийное устройство», «компьютер - средство электросвязи», «компьютер - канал электросвязи», «периферийное устройство - периферийное устройство», «периферийное устройство - канал (средство) электросвязи» и наоборот.

При наличии компьютерной сети любого уровня технической организации в первую очередь должен быть осмотрен и подвергнут обыску центральный управляющий компьютер (сервер сети, компьютер процессингового центра, узла связи, охранной системы и т.п.). Данное СВТ хранит в своей оперативной и постоянной памяти наибольшую часть машинной информации, управляет другими СВТ, имеет с ними прямую и обратную связь и, как правило, имеет программу автоматической фиксации доступа СВТ друг к другу (своеобразный «электронный журнал» учета работы всех СВТ сети - их индивидуальные номера (позывные, абонентские и т.п.), точные даты и время каждого соединения при обмене информацией, длительность и вид сеанса связи, характеристику передаваемой и получаемой информации, аварийные ситуации, сбои в работе отдельных СВТ (рабочих станций, периферийного оборудования), идентификационные коды и пароли операторов, попытки несанкционированного или нештатного доступа и т.д.).

Следователь должен знать, что при наличии соединения СВТ с другим оборудованием и электронно-вычислительной техникой, находящимися вне периметра обыскиваемой зоны (в другом помещении, здании, населенном пункте и т.д.), существует реальная возможность непосредственного доступа к машинной информации и совершения любых действий с ней и СВТ (стирание, уничтожение, модификация, копирование, блокирование, нарушение работы). *Для предотвращения этого необходимо*, в зависимости от ситуации и рекомендаций специалиста, временно или на длительный срок, частично или полностью отключить СВТ или локальную вычислительную сеть целиком от технических устройств, находящихся за периметром обыскиваемой зоны. Отключение может быть произведено как на программном, так и аппаратном уровне. Если СВТ работает в режиме «электронной почты», то предпочтительнее оставить его до конца обыска в работающем состоянии в режиме «приема почты», исключив возможность какой-либо обработки и

передачи информации. Эту работу может сделать только квалифицированный специалист. Все выполняемые им действия должны быть зафиксированы с помощью видеозаписи и отражены в протоколе обыска.

3. Определить СВТ, находящиеся во включенном состоянии, и характер выполняемых ими операций и/или программ. Особое внимание необходимо уделить терминальным печатающим и видеоотображающим устройствам (принтерам и мониторам). Распечатки информации (листинги) при необходимости должны быть изъяты и приобщены к протоколу следственного действия; изображение на экране монитора изучено и детально описано в протоколе (можно также зафиксировать его на видеопленку, либо сделать распечатку на бумаге с использованием специальных сканирующих программ).

Если специалисту удастся установить, что на момент обыска на каком-либо СВТ происходит уничтожение информации, либо уничтожается машинный носитель информации, необходимо всеми возможными способами приостановить этот процесс и начать обследование с данного места или СВТ.

4. При обследовании персонального компьютера необходимо:

- установить последнюю исполненную программу и/или операцию, а при возможности все, начиная с момента включения компьютера;

- произвести экспресс-анализ машинной информации, содержащейся на жестком диске и в оперативной памяти компьютера с целью получения информации, имеющей значение для следствия (интерес могут представлять файлы с текстовой и графической информацией).

Детальный этап обыска является очень трудоемким и требует высокой квалификации как специалиста в области СВТ, так и всей следственно-оперативной группы.

Необходимо четко организовать поисковые мероприятия, направленные на поиск тайников, в которых могут находиться предметы, устройства и документы. Ими может служить и само СВТ - аппаратные и программные оболочки модулей его составляющих.

***Следователю стоит придерживаться следующих рекомендаций*:**

- При невозможности вскрытия корпуса СВТ (если это может привести к утрате информации, физическому повреждению ее носителя либо приведению к неисправному состоянию) необходимо изъять СВТ целиком для лабораторного исследования.

- Все обнаруженные машинные носители информации (дискеты, пластиковые карточки, ленты, в т.ч. аудио-, видеокассеты и оптические компакт-диски) следует изъять для последующего анализа содержащихся на них данных на *аттестованном* исследовательском *оборудовании*, при отсутствии которого осмотр информации недопустим.

- Нельзя использовать специальную поисковую и досмотровую технику, один из элементов которой - источник электромагнитных или магнитных излучений (металлодетекторы, магниты, электронные стетоскопы, рентгеновские установки и т.п.).

- При необходимости изъятия жесткого диска персонального компьютера целесообразно изъять весь процессорный (системный) блок.

- В случае изъятия печатающего устройства (принтера) необходимо помнить, что в настоящее время возможна идентификация печатной продукции, изготовленной лишь на матричном (игольчатом) принтере. Для лазерного (электрографического) и струйного типов принтеров данный анализ практически невозможен.

На заключительном этапе обыска составляются: протокол следственного действия и описи к нему; вычерчиваются планы обыскиваемых помещений, схемы расположения СВТ относительно друг друга, строительных проемов, инженерно - технических коммуникаций, оконечных устройств электронесущей арматуры, а также принципиальная схема соединения СВТ между собой и с другими техническими устройствами; проводятся дополнительная фотосъемка и видеозапись.

Предметом выемки в абсолютном большинстве случаев *служат* средства вычислительной техники, машинные носители информации, машинная информация, всевозможные документы, средства защиты информации, специальная разведывательная и контрразведывательная аппаратура, а также свободные образцы почерка, машинописных текстов и готовой продукции для сравнительного исследования.

Помимо вышеуказанного могут быть изъяты материалы, предметы, приспособления, устройства и инструменты, которые могли быть использованы преступником при изготовлении орудий преступления, поддельных документов, машинных носителей информации и самой информации; черновики, на которых отрабатывалась поддельная подпись или другие реквизиты документа; копии и бланки регистрационно-учетных документов и расчетно-кассовых операций; техническая и справочная литература, косвенно связанная с технологией обращения и изготовления электронных документов и машинных носителей информации, орудий преступления; фотографии, аудио-, видеокассеты соответствующего содержания, в том числе с зарубежными художественными видеофильмами, содержащими эпизоды преступной деятельности, способы подготовки, совершения и сокрытия преступлений, изготовления спецтехники; оргтехника - копировальные и печатные аппараты (ксероксы, печатные машинки, телефонные аппараты с расширенными функциями, факсы, пейджеры, сотовые и радиотелефонные аппараты и т.д.); штампы, печати и маркираторы; ламинаторы; средства эмбосирования машинных носителей, нанесения защитных знаков и т.д.

Назначение экспертиз

По делам рассматриваемой категории существует постоянная необходимость использования в процессе расследования специальных познаний в области новых информационных технологий. Данные познания необходимы как для получения доказательств, так и для процессуального оформления документов, подготовленных средствами компьютерной техники, которые впоследствии могут играть роль доказательств.

С начала 90-ых годов в России появился новый вид криминалистических экспертиз, получивших название ***компьютерно - технических***.

В настоящее время с их помощью можно решать следующие задачи:

- воспроизводить и распечатывать всю или часть компьютерной информации (по определенным темам, ключевым словам и т.п.), содержащейся на машинных носителях, в том числе находящейся в нетекстовой форме (в сложных форматах - в форме языков программирования, электронных таблиц, баз данных и т.д.);

- восстанавливать компьютерную информацию, ранее содержавшуюся на машинных носителях, но впоследствии стертую или измененную (модифицированную) по различным причинам;

- устанавливать дату и время создания, изменения (модификации), стирания, уничтожения, либо копирования той или иной информации (документов, файлов, программ и т.д.);

- расшифровывать закодированную информацию, подбирать пароли и раскрывать систему защиты СВТ;

- исследовать СВТ на предмет наличия в них программно-аппаратных модулей и модификаций, приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети (вредоносных средств - компьютерных вирусов, «закладок», «жуков» и т.п.);

- определять авторство, место (средство) подготовки и способ изготовления документов (файлов, программ), находящихся на машинном носителе информации;

- выяснять возможные каналы утечки конфиденциальной информации из компьютерной сети, конкретных СВТ и помещений; устанавливать возможные несанкционированные способы доступа к охраняемой законом компьютерной информации и ее носителям;

- выяснять техническое состояние, исправность СВТ, оценивать их износ, а также индивидуальные признаки адаптации СВТ к конкретному пользователю;

- устанавливать уровень профессиональной подготовки отдельных лиц, проходящих по делу, в области программирования и в качестве пользователя;

- определять конкретных лиц, нарушивших правила эксплуатации ЭВМ, системы ЭВМ или их сети;

- выяснять причины и условия, способствующие совершению правонарушения, связанному с использованием СВТ.[2]

Исходя из этих задач, ***следователь может поставить на разрешение эксперта следующие основные вопросы***:

1. Является ли представленное на исследование техническое устройство средством электронно-вычислительной техники? Если да, то укажите тип, вид, назначение, техническое состояние и тактико-технические характеристики.

2. Каковы тип, вид, марка, изготовитель, техническое состояние, тактико-технические характеристики (исправность, процент износа, и т.п.) средств вычислительной техники, представленных на исследование?

3. Какая информация содержится на машинных носителях, представленных на исследование?

4. Возможна ли раскодировка информации, записанной в сложных форматах? Если да, то каково ее содержание в человекочитаемой форме?

5. Какие документы находятся на представленных на исследование машинных носителях информации? По возможности представьте их в человекочитаемой форме путем распечатки на бумажном носителе.

6. Какая компьютерная информация и в какой форме (файл, программа, документ) была стерта, скопирована, изменена (модифицирована), уничтожена?

7. Каковы индивидуальные признаки компьютерной информации, представленной на исследование, - название, размер, дата и время создания, изменения (модификации)?

8. Когда и в какое время был создан файл (документ), представленный на исследование?

9. Как изменялось содержание обнаруженных документов (конкретных файлов, программ) на представленных на исследование машинных носителях информации - по названию, размеру, дате, времени создания (стирания, изменения)?

10. Возможно ли получение скрытой информации, касающейся проходящих по делу лиц (предметов, документов, событий)? Если да, то распечатайте ее в человекочитаемой форме.

---

[2] ***Катков С.А., Собецкий И.В., Фёдоров А.Л.*** Подготовка и назначение программно-технической экспертизы // Информ. бюллетень СК МВД России. 1995. № 4 (85). С. 93-94.

11. Изготовлены ли представленные документы с использованием печатающих средств компьютерной техники?

12. Какого типа (вида, класса) печатающее устройство (принтер) использовалось при изготовлении представленных на исследование документов?

13. Изготовлены ли представленные документы на одном или на разных печатающих устройствах (принтерах)?

14. Не производилась ли допечатка в представленном на исследование документе с использованием печатающего устройства (принтера)?

15. Подготовлены ли предъявленные на исследование документы на представленных на исследование печатающих устройствах (принтерах)?

16. Какого рода программное обеспечение могло использоваться при подготовке и распечатке представленных на исследование документов?

17. С помощью каких программно-аппаратных средств вычислительной техники был подготовлен документ (машинный носитель), представленный на исследование?

18. Содержатся ли на представленных на исследование средствах вычислительной техники программно-аппаратные модули и модификации, способные уничтожать, блокировать, модифицировать либо копировать информацию, нарушать работу ЭВМ, системы ЭВМ или их сети без предварительного предупреждения пользователя о характере действия или не запрашивающие разрешение пользователя на реализацию программой своего назначения? Если да, то какие? Каков характер их воздействия на ЭВМ и ее программное обеспечение?

19. Содержатся ли на представленных на исследование средствах вычислительной техники программно-аппаратные модификации, влияющие на конечные результаты работы конкретного технического устройства либо программного продукта? Если да, то какие? Каков характер и последствия их воздействия на конкретное устройство и его программное обеспечение?

20. Нарушение каких правил эксплуатации ЭВМ, системы ЭВМ, их сети, а также систем их безопасности привело к образованию ущерба (наступлению иных тяжких последствий)? Определите конкретные должностные лица, ответственные за нарушение указанных правил.

21. Какой материальный ущерб причинен потерпевшему?

22. Каким паролем (кодом) осуществляется доступ к ЭВМ (системе ЭВМ, компьютерной сети, программе, файлу, периферийному устройству и т.п.), представленной на исследование?

23. Каковы тип, вид, марка, изготовитель, техническое состояние и основные тактико-технические характеристики средства защиты ЭВМ (компьютерной информации), представленной на исследование?

24. Каков уровень профессиональной подготовки конкретного лица, проходящего по делу, в области программирования (в качестве пользователя ЭВМ, системы ЭВМ, компьютерной сети, программиста, оператора, администратора баз данных и т.п.) либо защиты компьютерной информации?

25. Каковы каналы утечки компьютерной информации из ЭВМ, системы ЭВМ, компьютерной сети, иного средства электронно-вычислительной техники, помещения, проходящих по делу?

26. С помощью каких технических устройств было осуществлено копирование (стирание, уничтожение, модификация) охраняемой законом компьютерной информации? По возможности укажите тип, вид и основные тактико-технические характеристики устройства.

27. Какие причины и условия, способствовали совершению правонарушения в сфере компьютерной информации? Представьте их подробное описание.

28. Возможно ли сопряжение (соединение) представленной на исследование ЭВМ (средства электронно-вычислительной техники) с каналами электросвязи? Укажите конкретно, с какими (вид, тип, модификация канала электросвязи) и с помощью каких устройств?

29. Возможно ли сопряжение (соединение) представленного на исследование технического устройства с ЭВМ, системой ЭВМ или компьютерной сетью? Укажите тактико-технические характеристики аппаратуры.

Этот список вопросов не является исчерпывающим и может быть расширен, исходя из обстоятельств конкретного уголовного дела. В затруднительных случаях при постановке вопросов следует консультироваться у самого эксперта.

Постановление о назначении компьютерно-технической экспертизы должно содержать максимально полную описательную часть, в которой следует отразить:

- обстоятельства уголовного дела;

- сведения о лицах, причастных к совершению преступления;

- документы, сведения о которых могут содержаться на машинных носителях, представляемых на исследование;

- сведения, которые могут быть использованы в качестве «ключевых» слов при восстановлении и/или поиске экспертом информации (например, названия фирм, учреждений и организаций, фамилии клиентов, предполагаемые номера счетов и т.д.).

В резолютивной части объем задания эксперту должен быть определен конкретно. Современные СВТ имеют большие объемы постоянной памяти в виде жестких дисков (до нескольких гигабайт), поэтому следователь физически не сможет изучить и оценить содержание всего машинного носителя в течение приемлемого для этого времени. Для оптимизации данного процесса темы интересующей следователя информации должны быть точно обозначены при постановке вопросов, а сами они - сформулированы кратко и информативно.

При назначении компьютерно-технической экспертизы следователь должен четко представлять ее возможности и ограничения, не ставить перед экспертами вопросы и задания, выходящие за рамки их компетенции.

Нередко в процессе расследования компьютерного преступления возникает необходимость в установлении этапов обработки бухгалтерских данных с использованием СВТ, на которых вносились те или иные изменения, а также признаков интеллектуального подлога в первичных и сводных бухгалтерских документах, составленных на ЭВМ; в определении фактов уменьшения облагаемой налогом прибыли, выявлении счетных работников, причастных к совершению компьютерного преступления, путем исследования носителей оперативной информации, а также лиц, вводивших соответствующие данные в ЭВМ, и т.д. Для этих целей необходимо использовать ***возможности судебно - бухгалтерской экспертизы***, позволяющей при проведении исследований установить, насколько соблюдены те или иные требования положений о документах и документообороте в бухгалтерском учете при оформлении различных хозяйственных и иных операций первичными документами и отображении их в регистрах бухгалтерского учета и отчетности, в том числе выраженных в форме, зафиксированной на машинном носителе и машинограмме, созданных средствами компьютерной техники.

В случаях выявления нарушения этих нормативных документов, эксперт-бухгалтер может установить их причины (не сделаны ли они с целью совершения преступления - злоупотребления, сокрытия недостачи материальных ценностей, уменьшения их размера и т.д.) и сделать вывод о том, насколько эти нарушения положений повлияли на состояние бухгалтерского учета и выполнение функций лицами, ответственными за это в управлении хозяйственной или иной деятельностью. При этом возможно установление лиц, ответственных за созданные или допущенные нарушения правил составления первичных документов и учетных регистров.[3]

Наиболее оптимальным вариантом в некоторых случаях является назначение ***комплексной компьютерно-технической и судебно-бухгалтерской экспертизы***. Как

[3] См.: ***Белуха Н.Т.*** Судебно-бухгалтерская экспертиза. – М.: Дело. 1993. С. 107.

правило, необходимость такой экспертизы возникает в процессе расследования многоэпизодных уголовных дел о преступлениях в сфере экономики, совершенных с использованием компьютерной информации.

По делам рассматриваемой категории назначаются также: *технологические, электроакустические, фоноскопические, видеофоноскопические, радиотехнические, электротехнические и иные технические экспертизы*; в зависимости от отрасли хозяйства или характера нарушений - *товароведческие, финансово-экономические, криминалистические*, в частности, *технико-криминалистические экспертизы документов, созданных с использованием СВТ и новых репрографических технологий*, *и т.д.*

Например, ***при назначении радиотехнической экспертизы перед экспертом можно поставить следующие вопросы***:

1. Является ли представленное на исследование устройство (само или в комплекте) радиопередающей (радиоприемной) аппаратурой (установкой)?

2. В каком диапазоне радиочастот работает данное устройство и какова его мощность в антенне? Укажите дальность и другие тактико-технические характеристики радиоприема (или передачи).

3. В работе какого канала электросвязи используется данное устройство?

4. Является ли данное устройство самодельным, заводского изготовления или частью промышленной аппаратуры (ее отдельными блоками)?

5. Возможно ли использование данного устройства для проведения специальных технических мероприятий (разведывательных или контрразведывательных)?

6. Создает ли данное устройство помехи в каналах электросвязи, в частности, для радио- и телеприема (телефонной, телеграфной, факсимильной, связи ЭВМ и др. видов электросвязи)? Если да, то насколько превышены допустимые нормы и к каким вредным последствиям может привести эксплуатация данного устройства?

Таким образом, наряду со штатными экспертами соответствующих учреждений правоохранительных органов к подготовке и участию в следственных действиях необходимо шире привлекать специалистов профильных предприятий и учреждений, научно-исследовательских и учебных заведений, а также отдельных специалистов, имеющих опыт практической работы в определенной области знаний.

Следователь, правильно оценив и тщательно изучив заключения экспертов и прилагаемые к ним материалы, может широко использовать полученные данные как при назначении и производстве других экспертиз и следственных действий, так и в качестве самостоятельных доказательств по делу.

2. ОСОБЕННОСТИ ИССЛЕДОВАНИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ В ЦЕЛЯХ ПОЛУЧЕНИЯ ДОКАЗАТЕЛЬСТВЕННОЙ ИНФОРМАЦИИ ПРИ РАСКРЫТИИ И РАССЛЕДОВАНИИ ПРЕСТУПЛЕНИЙ

Подготовка материалов для проведения экспертных исследований должна предусматривать мероприятия, обеспечивающие исключение доступа (удаленного и местного, физического или технического) к электронному оборудованию. В общем виде процесс подготовки материалов для аппаратной экспертизы включает в себя три последовательных стадии, обеспечивающие получение процессуально-корректных доказательств.

1. **Процессуально-корректное выключение аппаратуры, разборка конфигурации и подготовка к упаковке.** В эту стадию включаются этап завершения работы электронного средства с соблюдением методических и процессуальных норм, сбор торговой и технической документации об аппаратном средстве. Приведем пример. При подготовке аппаратных средств к изъятию для проведения экспертизы необходимо: путем опроса персонала или в ходе допросов выяснить сетевые имена пользователей и их пароли; изъять все оборудование, находящееся на компьютерных столах. При работе ПК произвести его «парковку». Необходимо изымать все оборудование независимо от того, работает оно или нет. Опечатать столы. Внимание следует уделять и упаковочной таре, на которой может быть информация, помогающая идентифицировать электронное устройство. При подготовке к изъятию и перед упаковкой компьютерных и радиоэлектронных средств должны быть установлены и зафиксированы: конфигурация компьютера; номера моделей и серийные номера каждого из устройств; инвентарные номера, присваиваемые бухгалтерией при постановке оборудования на баланс предприятия; прочая информация, имеющаяся на фабричных ярлыках и коробках. Изымается сопутствующая техническая, торговая и упаковочная документация и тара, относящиеся к данному аппарату. Например, уникальный IMEI-номер (международный идентификатор мобильного оборудования), позволяющий идентифицировать мобильный терминал, наносится как на упаковке под штрих - кодом, так и в аккумуляторном отсеке аппарата. Все изъятые системные блоки должны быть опечатаны таким образом, чтобы исключить возможность их включения в сеть или разборки.

К изъятым носителям информации необходимо приложить информацию о владельце и месте изъятия. При изъятии НЖМД необходимо произвести описание содержимого жесткого диска и побитовое (лучше двойное) копирование НЖМД на «зеркальную» копию или компакт-диск (640 Мб). Эти действия должны найти свое отражение и быть зафиксированы в протоколе следственного действия. При этом следует иметь в виду, что

«технически» подобную операцию можно осуществить только для компьютеров с файловой системой FAT16 или FAT32, не являющихся выделенными серверами в сети. Эти файловые системы используются в следующих операционных системах (ОС): MS-DOS и его клоны (FAT16); Windows и Windows for Workgroups (FAT16); Windows 95,98 (FAT16, FAT32); Windows 2000, NT, Windows NT Server.

Для опечатывания носителей информации (данных) необходимо:

1) упаковать их в жесткую коробку, опечатать ее;

2) на листе бумаги сделать описание упакованных носителей (тип каждого из них, их количество);

3) коробку с носителями и лист с описанием положить в полиэтиленовый пакет, который заклеить.

При опечатывании носителей информации недопустимо производить какие-либо действия с ними.

2. **Упаковка и консервация аппаратного средства для его транспортировки в экспертное учреждение.** В эту стадию следует включить мероприятия по упаковке, перевозке и сдаче образцов в экспертное учреждение. В частности, опыт ФБР (группа компьютерного анализа и исследований), в области работы с доказательствами показывает, что вопросам транспортировки изъятого оборудования уделяется очень серьезное внимание, так как некачественное выполнение этого мероприятия ведет к утрате вещественной доказательственной базы4. Перед транспортировкой образцов ВТ и РЭУ их следует упаковать, упаковку опечатать. Для этого следует использовать промышленную тару, коробки (пенопласт в качестве уплотнителя), мешки или ткань. НЖМД желательно упаковывать в устройства для безопасной перевозки носителей памяти типа «Mobile-Rack» и «Fleksi-Drive». Дискеты, компакт-диски, кассеты следует перевозить в плексигласовой упаковке. Аппаратуру необходимо плотно размещать в упаковочной таре, которую необходимо жестко закрепить в транспортном средстве. При транспортировке следует категорически избегать воздействия вибраций, взаимодействий с химически активными веществами; магнитных воздействий на аппаратуру и на магнитные носители информации, а также оградить изъятое от воздействия магнитосодержащих средств и криминалистической техники (например, магнитных подъемников, магнитных кисточек для выявления следов рук

[4] *Тушканова О.В.* Опыт экспертной работы ФБР США по исследованию компьютерных средств. Научно-практический семинар.Белгород. 28-31 мая 2000; *Айков Девид, Сейгер Карл, Фонстрох Уильям*. Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями. - М., 1999.

и проч.)5. Перевозку и хранение радиоустройств необходимо осуществлять в экранирующей таре. Например, перевозка сотовых телефонов на экспертизу должна проводиться в экранированной таре, т.е. металлических коробках с крышкой (если выяснены коды блокировок аппарата). После транспортировки в зимних условиях необходимо обеспечить прогрев объектов исследования в течение двух часов при комнатной температуре.

Если изъятые аппаратные средства оставлены на временное хранение на месте происшествия, следует организовать охрану выделенного для этих нужд помещения.

3. **Хранение аппаратных образцов до производства экспертизы**.

В эту стадию включаются обеспечивающие мероприятия по инструментальному хранению изъятых аппаратных образцов в соответствии со ст. 82 УПК РФ. Инструментальное хранение доставленных аппаратных средств необходимо обеспечить в соответствии с паспортными требованиями изготовителя. Аппаратные объекты представляются на экспертизу в неизмененном виде, соответствующем их фиксации и упаковке в ходе проведенного следственного действия. Получение аппаратных образцов и их выдача оформляются в соответствии с приложениями № 66, 67 к УПК РФ постановление и протокол о получении образцов для сравнительного исследования.

В общем виде экспертное исследование аппаратных средств также как и любое другое исследование в судебной экспертизе, имеет следующие основные стадии: подготовительную; проведения собственно экспертного исследования, в том числе экспертного эксперимента; анализа результатов и составление экспертного заключения САКЭ.

Подготовительный этап аппаратной экспертизы включает в себя осмотр экспертом объектов экспертизы еще на месте происшествия и далее в стационарных условиях. При этом эксперт уясняет взаимосвязь исследуемого аппарата с другими КЭС и на основании классификации использования преступниками аппаратных средств производит выдвижение экспертных гипотез (версий) о возможных путях решения вопросов и применяемых методах исследования. Продумывается составление плана экспертного исследования КЭС, планируются организационно-технические меры, необходимые для проведения исследования. Приведем краткое содержание описанных категорий.

Осмотр объектов САКЭ начинается с ознакомления с основаниями проведения экспертизы, предоставленными материалами следствия и аппаратными объектами и материалами, с которыми предстоит работать. Следующим действием эксперта является

---

[5]*Усов А.И., Зубаха В.С.* Направление разработки методического обеспечения производства компьютерных экспертиз и исследований. Сб.: Экспертная практика. №47.- М., 1999.

непосредственный осмотр представленных на экспертизу аппаратных объектов. При этом ему необходимо обратить внимание на целостность упаковки и печатей. При необходимости осуществляется предварительный просмотр данных, хранящейся на носителях. Экспертом должна учитываться, в соответствии с УПК РФ, возможность проведения повторного (ст.207 УПК РФ) комплексного (ст.201 УПК РФ) или комиссионного (ст.200 УПК РФ) экспертного исследования. После этого экспертом осуществляется планирование и логическое моделирование предстоящего экспертного исследования, включающего описание используемого аппаратно-программного (лицензированного) инструментального обеспечения, его подключение, планируемые промежуточные и конечные результаты. При этом следует зафиксировать следующие моменты:

- полный состав аппаратного обеспечения эксперта и режимы подключения всех плат (положения джемперов, используемые аппаратные настройки и т.п.);

- режимы подключения внешних носителей информации (на каком разъеме они установлены, как установлены джемперы и т.п.);

- полный состав общего (операционные системы, драйверы внешних устройств), общесистемного (системы управления базами данных, электронные таблицы, командные оболочки и т.п.) и специального программного обеспечения, установленного на компьютере эксперта, основные параметры установки, последовательность запуска при начальной загрузке операционной системы, а также степени соответствия, используемой при экспертизе конфигурации;

Значение такого подробного описания весьма велико, так как в ряде случаев из-за некорректного или нестандартного подключения исследуемых магнитных носителей данных (информации) могут быть получены неверные результаты или вообще поставлено под сомнение сама возможность проведения исследований6. Опыт проведения КТЭ в ОВД показал необходимость выполнения ряда обязательных первоочередных исследований (практически независимо от особенностей поставленных перед экспертом вопросов), а именно:

- проведение проверки на наличие программных вирусов и других вредоносных программ с использованием последней версии рекомендуемых антивирусных программ;

- определение системного времени, установленного на системной плате, а также соответствующих атрибутов файлов и директорий;

- определение используемого режима форматирования магнитного носителя, размера кластеров, количество дорожек и цилиндров. Выявление наличия поврежденных областей на

---

[6] *Зубаха В.С., Усов А.И., Саенко Г.В.* и др. Общие положения по назначению и производству КТЭ (методические рекомендации). - М., 2001.

НЖМД. Данная информации в исследовательской части заключения эксперта даст возможность решить впоследствии и при необходимости вопрос о проведении экспертизы последующих уровней.

По характеру выполняемых действий осмотр электронных объектов на месте происшествия или в экспертном учреждении, можно разделить на общий осмотр, осмотр вложений и внешний осмотр компьютерных средств (в частности, носителей данных).

При общем осмотре производятся следующие действия: изучение содержимого протоколов осмотра, обыска и др. (при их наличии) с целью учета в дальнейших исследованиях особенностей выполнявшихся ранее следственных действий; изучение оборудования и уяснение его связи с другими КЭС. В случае проведения экспертизы в экспертном учреждении - осмотр упаковки на целостность (коробок, пакетов, мешков и пр.), наличие и состояния печатей, подписей следователя и понятых, установление полного соответствия представленных материалов перечню приложения, сопроводительного письма и постановления о назначении экспертизы. Осмотр производится путем вскрытия упаковки и сверки содержимого вложений внутренней описи, составления описи объектов исследования по факту и фиксирования целостности упаковки, вложений и признаков механических повреждений.

Внешний осмотр КЭС и носителей информации производится: путем установления форм-факторов (фиксируются размеры корпуса, его особенности, наличие устройств для работы с носителями информации, наличие и состав разъемов, плат расширения, заглушек, наклеек, маркировок); конструктивных особенностей и параметров принтеров, сканеров клавиатур, мониторов, устройств-манипуляторов типа «мышь», шнуров питания и т.д.; определения типа носителей данных (информации) (НЖМД, ГМД, компакт-диск, стриммерная кассета, FLASH-карта, электронная записная книжка, магнитооптический диск, ZIP-диск и др.). Фиксирование признаков механических повреждений компьютерной техники и носителей информации, затрудняющих работу с ними в обычном (штатном) режиме, позволит впоследствии эксперту выяснить необходимость исследования нештатного состояния аппаратного средства, а также серийных и инвентарных номеров осматриваемых объектов.

Осмотр экспертом компьютерных или радиоэлектронных объектов должен заканчиваться подробным описанием признаков исследуемых объектов.

Для аппаратных объектов этими признаками являются: тип (вид, модель); форм-фактор и геометрические размеры; цвет; наличие или отсутствие серийного номера, кода и т.п.; отличительные признаки и особенности с полным их описанием и составом (кнопки, переключатели, наклейки, характерные надписи, повреждения) и т.д. Проведение осмотра

объектов экспертом рекомендуется сопровождать фиксированием на цифровую видео- и фотокамеру. Полученные изображения оформляются в виде фототаблицы, распечатываются и прикладываются к заключению эксперта в части, касающейся описания объектов.

Выдвижение экспертных гипотез. Экспертом выдвигается рабочая гипотеза (экспертная версия), в которой им формируется предположения о том, какими, по мнению эксперта, могут быть результат исследования и выводы, а также предполагаемые аппаратные методы, которые будут использованы для достижения предполагаемого результата. На основе этого предположения эксперт составляет план экспертного исследования, который представляет из себя логически проработанную последовательность действий, предпринимаемых экспертом с целью оптимального решения поставленной задачи. Логическая проработанность и обоснованность, с криминалистической точки зрения и придают впоследствии заключению статус доказательства.

Проведение организационно–технических мер. Эти экспертные действия необходимы для обеспечения технологической стороны исследований. Они включают в себя определение требуемого экспертного инструментария, который представляет собой аппаратное и программное обеспечение компьютеризированного рабочего места эксперта (КРМЭ) и организационно-методическое, в которое входят сертифицированные экспертные методики, рекомендации, справочное и каталоговое обеспечение, инструкции, техническая документация на аппараты и т.д. Эксперту необходимо также определить способ взаимодействия с другими экспертами в случае необходимости проведения комплексной комиссионной и дополнительной экспертизы.

Анализ результатов исследования и формулирование выводов.

Необходимо отметить, что ст.25 Закона «О государственной судебно-экспертной деятельности»7, ст. 204 УПК РФ указывают основания и принципы изложения экспертного заключения в самых общих чертах. Исходя из специфичности судебного аппаратно-компьютерного исследования, на основании вышеуказанных источников можно в целях систематизации и методических требований к изложению полученного экспертного материала предложить трехуровневую «условную» структуру заключения: вводный, исследовательский и заключительный разделы.

Во вводном разделе в соответствии со ст. 204 УПК РФ указываются формальные данные эксперта и его квалификация и экспертного учреждения, основания проведения экспертизы, вопросы, поставленные перед экспертом, предоставленные эксперту аппаратные

[7] См. Ст. 25 «Заключение эксперта или комиссии экспертов и его содержание» Закона «О государственной судебно-экспертной деятельности».

объекты и материалы, отмечаются лица, присутствующие при экспертизе (см. ст. 204 УПК РФ).

В исследовательском разделе также отмечаются лица, присутствующие при экспертизе, дается обоснование применяемым методикам исследования, их характеристикам. Производятся само исследование аппаратного объекта, содержание и результаты исследования.

В заключительном разделе даются выводы по поставленным перед экспертом вопросам и их обоснование с подборкой иллюстративного материала.

При экспертном исследовании аппаратного средства, в ходе которого решается задача его идентификации, подводится итоговая оценка совпадающих и различающихся признаков сравниваемых объектов, констатируется, что совпадающие признаки являются или не являются устойчивыми, существенными и образуют или не образуют индивидуальную, неповторимую их совокупность. Например, номер материнской платы совпадает с паспортными данными, указанными в техпаспорте на ПК; номер IMEI для мобильного терминала сотовой связи совпадает с номером на представленной коробке; выявленный номер кредитной ЧИП-карты соответствует PIN - коду названному лицом, держателем карты, и т.д.).

При исследовании КЭС, в ходе которого решается задача по его диагностике, выполняется итоговая оценка выявленных диагностических признаков, например, аппаратная конфигурация компьютерной системы и установленное на нем ПО позволяют выполнить распечатку представленного денежного знака; с исследуемой кредитной карты был прокатан данный слип; и т.д. Констатируются устойчивость, существенность и неповторимость установленной функциональной совокупности применительно к исследуемому аппаратному объекту (системе).

ЗАКЛЮЧЕНИЕ

Одним из приоритетных направлений внутренней политики Российской Федерации является активное развитие информационной инфраструктуры, создание

конкурентоспособных на международном уровне коммуникационных технологий*. Очевидно, что мировая экономика претерпевает существенные изменения под влиянием цифровизации. Это отражается на всех сферах жизнедеятельности человека: от бытовых и профессиональных до финансово-экономических и т.д. Однако процесс информатизации имеет и обратную сторону – криминализацию компьютерных и телекоммуникационных систем связи. Изменившиеся условия ставят перед правоприменителями концептуально новые задачи, требующие поиска современных путей их решения.

Одной из актуальных проблем уголовного процесса является юридическая неоднозначность понятия электронного информационного носителя как источника доказательной информации. В настоящее время ведутся активные научные дискуссии по определению, содержанию и порядку получения, оценки и использования информации на электронных носителях. Текущие проблемы включают юридическую неоднозначность концепции электронного носителя информации как источника доказательной информации. Недостатки правового регулирования порядка получения доказательной информации на электронных носителях зачастую негативно отражаются на качестве расследования уголовных дел, правильности сбора и исполнения доказательств в виде информации на электронных носителях.

На сегодняшний день проблема изъятия электронного носителя информации, как нового источника доказательств по уголовному делу, при производстве следственных действий является весьма актуальной. Безусловно, применение в преступной деятельности информационных технологий и активное использование сети Интернет привело к внесению соответствующих изменений в уголовно-процессуальное законодательство. В частности, Федеральный закон от 28.07.2012 № 143-ФЗ 1 внес изменения в ст.ст. 81, 82, 166, 182, 183 УПК РФ, дополнив их электронным носителем информации. Отметим, что участие специалиста при изъятии электронных носителей информации в ходе производства таких следственных действий, как обыск и выемка, является обязательным.

Сложность изъятия цифровых следов преступления зависит как от типа электронной информации, так и от вида электронного носителя, на котором она содержится. Наиболее простыми в работе являются технические объекты, которые чаще всего не имеют защиты в виде пароля, то есть доступ к хранящейся на них информации не ограничен. К таким объектам можно отнести флеш-карты, компактдиски, фотокамеры и т.п.

Кроме понятия и значения, достаточно остро на практике обсуждается сама процедура изъятия электронного носителя информации. Привлечение специалиста, обладающего знаниями в области информационных технологий, затруднительно ввиду их небольшого числа в экспертных учреждениях. Решается данная проблема путем привлечения к

производству следственных действий специалистов, которые не являются сотрудниками экспертно-криминалистических подразделений. Это могут быть сотрудники научно-исследовательских институтов (специализирующиеся на изучении, хранении, передаче, обработке, защите и воспроизведения информации с использованием компьютеров 1), технические специалисты коммерческих учреждений, в чьи функции входит установка компьютерных систем, программного обеспечения, ремонт компьютерной техники и т. д., а также преподаватели информатики.

Кроме изъятия электронных носителей информации специалист оказывает помощь в копировании информации. При этом законодатель запрещает осуществлять копирование информации, если это может воспрепятствовать расследованию преступления либо по заявлению специалиста повлечь утрату или изменение информации. Решение об удовлетворении ходатайства о копировании информации должен принимать исключительно следователь (дознаватель), т. к. именно он несет персональную ответственность за расследование уголовного дела, в том числе и за хранение доказательственной информации, полученной при производстве следственных действий.

В подавляющем большинстве следователи изымают электронные носители информации без их изучения. Ввиду того, что с информационным содержимым указанных носителей манипуляции не осуществляются, специалисты не привлекаются. По устоявшейся судебной практике в отдельных регионах подобная позиция признается допустимой, так как, по мнению судей, участие специалиста обязательно только при копировании информации, содержащейся на изъятых предметах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 24.03.2022) – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 24.09.2021).
2. Закон Российской Федерации «О федеральных органах правительственной связи и информации» // Вед. Верх. Сов. РФ. 1993. № 12.

3. О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 28 июля 2012 г. № 143-ФЗ. URL:http://www.consultant.ru/ document/ (дата обращения: 25.10.2021).

4. Государственный стандарт (ГОСТ) № 6.10.4-84 от 01.07.87 г. «УСД. Придание юридической силы документам на машинном носителе и машинограмме, создаваемым средствами вычислительной техники. Основные положения» // Постановление Госстандарта № 3549 от 09.10.84 г.

5. Балашова А.А. Электронные носители информации и их использование в уголовно-процессуальном доказывании: автореф. дис. ... канд. юрид. наук: 12.00.09. Москва, 2020. 216 с.

6. Бутенко О.С., Расчетов В.А. Актуальные вопросы изъятия электронных носителей информации // Наука, образование и культура. 2017. N 8 (23). С. 44-45.

7. Васюков В.Ф., Булыжкин А.В. Изъятие электронных носителей информации при расследовании преступлений: нерешенные проблемы правового регулирования и правоприменения // Российский следователь. 2016. N 6. С. 3-8.

8. Васюков В.Ф. Осмотр, выемка электронных сообщений и получение компьютерной информации // Уголовный процесс, 2016. № 10. С. 68-71.

9. Вехов В.Б. Электронные доказательства: проблемы теории и практики // Правопорядок: история, теория, практика. 2016. N 4 (11). С. 46-50.

10. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / Под ред. акад. Б.П. Смагоринского. – М.: Право и закон. 1996. 182 с.

11. Гаврилин Ю.В. Электронные носители информации в уголовном судопроизводстве // Труды Академии управления МВД России. 2017. N 4 (44). С. 46-50.

12. Григорьев В.Н. Тенденции и проблемы развития законодательства в области информационных технологий, регулирующего уголовное судопроизводство // Академическая мысль. 2019. № 3 (8). С. 57 – 61.

13. Григорьев В.Н., Максимов О.А. Понятие электронных носителей информации в уголовном судопроизводстве // Вестник Уфимского юридического института МВД России. 2019. N 2 (84). С. 33-44.

14. Зуев С.В. Электронная информация и ее носители в уголовно-процессуальном доказывании: развитие правового регулирования // Вестник Южно-Уральского государственного университета. Серия: «Право», 2017. Т. 17. № 1. С. 31-35.

15. Катков С.А., Собецкий И.В., Фёдоров А.Л. Подготовка и назначение программно-технической экспертизы // Информ. бюллетень СК МВД России. 1995. № 4(85). С. 87-96.

16. Ким А.В. Отдельные вопросы проведения осмотра и экспертизы электронных носителей информации // Ученые записки Крымского федерального университета имени В.И. Вернадского. Юридические науки. 2019. N 5 (71). С. 151-156.

17. Козловский П.В., Седельников П.В. Участие специалиста в изъятии электронных носителей // Научный вестник Омской академии МВД России. 2014. № 1 (52). С. 17 – 19.

18. Ларин Е. Г. Копирование информации с электронных носителей при производстве по уголовному делу // Законодательство и практика. 2012. № 2 (29). С. 52–53.

19. Лучин И.Н., Шурухнов Н.Г. Методические рекомендации по изъятию компьютерной информации при проведении обыска // Информ. бюллетень СК МВД России. 1996. № 4(89). С. 22-28.

20. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8-14.

21. Осипенко А. Л., Гайдин А. И. Правовое регулирование и тактические особенности изъятия электронных носителей информации // Вестник Воронежского института МВД России. 2014. № 1. С. 160.

22. Першин А. Н. Электронный носитель информации как новый источник доказательств по уголовному делу // Уголовный процесс. 2015. № 5. С. 50.

23. Тарабан Н.А. Информация о телефонных соединениях как доказательство в уголовном судопроизводстве и источник криминалистически значимой информации при раскрытии преступлений против личности // Российский следователь, 2014. № 17. С. 5-9.

24. Яковлева С.А., Шарова Д.В. Проблемы уголовно-процессуального регулирования изъятия электронных носителей информации // Вестник Марийского государственного университета. Сер.: Исторические науки. Юридические науки. 2020. N 3 (23). С. 292-300.

П Р И Л О Ж Е Н И Я

Образцы процессуальных документов, составляемых при оформлении отдельных следственных действий

Фрагмент протокола осмотра персонального компьютера

ОСМОТРОМ ОБНАРУЖЕНО:

Персональный компьютер импортного производства типа IBM PC/AT фирмы NEC заводской № 5673489 имеет металлический корпус типа MiniTower с передней пластмассовой панелью управления. На панели - два дисковода: для работы с гибкими магнитными дисками размером 3,5 дюйма и с оптическими компакт-дисками. На пластмассовой панели второго дисковода имеется эмбосированная надпись «compact DISC» и выполненная краской черного цвета надпись «Panasonic × 8». Дисковод для работы с оптическими компакт-дисками фирмы Panasonic восьмискоростной.

На передней панели процессорного блока находится световой индикатор частоты процессора с цифрами «133» зеленого цвета.

Внутренняя спецификация процессорного блока: система Plug and Play BIOS версии 1.1 27 июня 2018 г. выпуска; материнская плата типа ATC-1020 INTEL 430VX; процессор INTEL 486 DX5; сопроцессор установлен; рабочая частота 133 МГц; базовая память 640 KB; оперативная память 15360 KB; кэш память 256 KB; дисковод A: 1,44 MB, 3,5"(дюйма); жесткий диск: LBA, Индекс 4, объемом 1083 MB; дисковод D: CD-ROM, Индекс 3, типа ICD 1200 iT; терминал типа EGA/VGA; серийный порт: 3F8 2F8; параллельный порт: 378; операционная система Windows 95 с пакетом прикладных программ MS OFFICE и Norton Commander Версии 5.0, 6 февраля 2017 г. выпуска, фирмы Symantec Corporation.

Внутренняя спецификация жесткого диска: всего 655360 байт оперативной памяти, из них свободно 612304 байт; всего на жестком диске 1081540608 байт памяти, из них свободно 139591680 байт; на жестком диске файлов 13, каталогов 22, их названия занимают 230 байт памяти; *метка диска:* VITY; *серийный номер жесткого диска:* 416B:16A0; текущая дата: 12 марта 2019 года; текущее время: 16.30 ч.; *последняя исполняемая программа:* DrWeb.

Процессорный блок соединен белым управляющим электронесущим шнуром с монитором. На соединительном шнуре черной краской нанесена надпись «AWM E101344 Style 2969 VW1 30V 80`C SPACE SHUTTLE».

Монитор типа SVGA с размером экрана 14"(дюймов) фирмы SAMSUNG модификации SyncMaster 3Ne Low Radiation модель № CQB4147L серийный № HMBG401787; в пластмассовом корпусе; имеет следующие программно-заданные настроечные характеристики: по цветовой гамме - 256 цветов и оттенков; по разрешающей способности - 800×600 точек.

Процессорный блок и монитор подключены стандартным способом к бытовой электросети с переменным напряжением 220 вольт и частотой пульсации тока в 50 Гц через пятигнездовый удлинитель электропитания типа сетевой фильтр, марки «PILOT - GL» фирмы ZIS COMPANY, заводской № 2082GL с рабочими характеристиками: 220 вольт, 10 ампер, 50/60 Гц. Индикаторы включения фильтра в сеть электропитания и электроснабжения нагрузки горят красным светом, что свидетельствует о работе подключенного к нему электрооборудования.

К процессорному блоку с помощью стандартного соединительного шнура светло-серого цвета подключена клавиатура типа FCC ID:IZEOTCOK 100M фирмы MITSUMI, модели KPQ-E99ZC-13, заводской № 920306787.

При проверке системы компьютера на наличие вредоносных программ для ЭВМ (компьютерных вирусов) с использованием установленной на данном компьютере антивирусной программы DrWeb было **выявлено наличие** в его памяти и в загрузочном секторе жесткого диска **вируса** OneHalf.3544.

Составлена схема проводного соединения процессорного блока, монитора и клавиатуры между собой и с электропитающей арматурой.

Составлен план расположения процессорного блока, монитора, клавиатуры и электропитающей арматуры относительно друг друга, инженерно - технических коммуникаций, средств электросвязи, осветительных приборов, электрооборудования и окружающих предметов.

При осмотре ***применялась видеосъемка.***

Фрагмент протокола осмотра дискеты

Осмотр проводился с применением персонального компьютера типа IBM PC AT - 486 фирмы GLOBUS, заводской № 5673489, монитора SAMSUNG SyncMaster 3Ne Low Radiation, модель № CQB4147L, серийный № HMBG401787, матричного принтера типа EPSON LX-1050, модель № P10SA, серийный № 2QE7182404, операционной системы MS DOS Версии 6.22 и программы Norton Commander Версии 5.0, 6 февраля 2018 г. выпуска, фирмы Symantec Corporation.

Перед началом осмотра персональный компьютер и его программное обеспечение были тестированы специалистом на предмет отсутствия в них вредоносных программных и аппаратных средств.

ОСМОТРОМ ОБНАРУЖЕНО:

Персональный компьютер, монитор и принтер подключены стандартным способом к бытовой электросети с переменным напряжением 220 вольт и частотой 50 Гц.

В присутствии понятых и специалиста был вскрыт бумажный пакет № 1 размером 200×150 мм, заклеенный и опечатанный печатью № 23 для пакетов Следственного управления УМВД по Волгоградской области. На пакете имеется надпись: «Дискета размером 3,5 дюйма, изъята 30.08.2019 года в помещении Группы корреспондентских отношений ТРКЦ ГУ ЦБ России по Волгоградской области»; подписи следователя, специалиста и понятых. *Пакет повреждений и разрывов не имеет; целостность печатей не нарушена.* При вскрытии пакета в нем оказалась ***дискета с гибким магнитным диском диаметром 3,5 дюйма*** импортного производства фирмы BASF, ***упакованная в алюминиевую фольгу. Фольга с дискеты предварительно была удалена.***

Дискета имеет заводской номер F7055216E3, расположенный в нижнем правом углу тыльной стороны корпуса. Корпус дискеты неразборный, изготовлен из пластмассы черного цвета с защитным металлическим зашторивающим элементом. Данный элемент находится в положении полного закрытия рабочего окна. На лицевой стороне элемента имеются изготовленные типографским способом надписи: Verbatim, выполненная красителем черного цвета с полосой подчеркивания красного цвета; Data Life Plus - красителем черного цвета; MF 2HD - красителем красного цвета; IBM FORMAT - красителем черного цвета. На корпусе дискеты имеется заводская наклейка, изготовленная из бумаги. Основная ее часть - белого цвета размером 70×50 мм - находится на лицевой стороне дискеты и имеет следующие надписи, выполненные типографским способом: разлинована на семь горизонтальных линий желтого цвета длиной 50 мм с межстрочным интервалом 5 мм; с правой стороны - вертикальная надпись Verbatim с подчеркиванием, выполненные красителем красного цвета; в нижнем правом углу - знак в виде треугольника желтого цвета размером 10×10×10 мм. Нижняя часть наклейки красного цвета размером 70×15 мм, с захлестом на тыльную сторону дискеты имеет следующие надписи, выполненные типографским способом желтым красителем и расположенные в нижнем правом углу тыльной стороны дискеты: Write Protect и знак в виде треугольника размером 5×5×5 мм. На третьей линии основной части наклейки

по центру надпись «Диск № 3». На лицевой стороне корпуса дискеты заводским способом эмбосированы: в верхнем левом углу - знак «Стрелка вверх», в верхнем правом - «HD».

На тыльной стороне дискеты в центре находится круглое отверстие диаметром 25 мм, в котором механически подвижно расположен каркасный элемент осевого крепления гибкого магнитного диска, изготовленный из пластины тонколистового металла белого цвета. В нижнем левом и в нижнем правом углах тыльной стороны дискеты имеются сквозные прямоугольные отверстия размером 6×5 мм, изготовленные заводским способом. В последнем находится механически подвижный элемент защиты гибкого магнитного диска от записи (стирания) компьютерной информации, изготовленный из пластмассы черного цвета. Положение элемента свидетельствует о том, что ***гибкий магнитный диск закрыт для записи (стирания) компьютерной информации***.

При внешнем осмотре повреждений и следов вскрытия дискеты не обнаружено. Нажатием клавиш «Alt» «F1» (одновременно) и «Enter» на клавиатуре персонального компьютера в программе «Norton Commander» гибкий магнитный диск был открыт для визуального просмотра на мониторе. При просмотре содержания диска обнаружено, что на нем находятся четыре файла со следующими реквизитами:

Название файла (имя и расширение)	**Размер файла (байты)**	**Дата последнего изменения файла**	**Время последнего изменения файла**
dogovor	15312	24.01.2019	10:50
plat_inp.doc	15872	**29.08.2019**	**15:06**
platezka.frm	5515	30.04.2017	16:30
platezka.out ##	9062	**29.08.2019**	**15:32**

Последний *файл* **platezka.out** *имеет специальную метку* **##**, указывающую на то, что *файл скрыт от визуального просмотра*. **Содержимое каждого файла было осмотрено путем нажатия на клавишу «F3».** *При осмотре файла* **plat_inp.doc** дополнительно нажималась клавиша «F8» для выбора формата просмотра файла Word for Windows. При осмотре файла были **обнаружены электронные платежные поручения**. Путем нажатия на клавиши «Page Down», «PageUp», «↓» и «↑» **платежные поручения были осмотрены.** Обнаружено Платежное поручение № 13-946 от 29 августа 2019 г. на сумму 953 млн. 710 тыс. 845 рублей. Плательщик - ЗАО «Л-нефтепродукт»; Банк плательщика - Волгоградский филиал (*сокр. «ф-л»*) АКБ Сбербанка России, р/сч. № 345840, Код 241602/767; Получатель - АКБ «Империя»; Банк получателя - ГРКЦ ГУ ЦБ РФ в г. Москве МФО 54803218, Код 2840563041, р/сч. № 562402. Данное платежное поручение специалистом распечатано на

бумаге с использованием принтера, стандартного картриджа (красящая лента черного цвета) и программного обеспечения; прилагается к настоящему протоколу.

При осмотре файла **platezka.frm** *обнаружены электронные формы бланков платежных поручений.* При осмотре файла **platezka.out** *использовалась автоматизированная функция поиска по реквизиту номера платежного поручения 13-946* путем дополнительного нажатия на клавишу «F7», ввода реквизита поиска и нажатия на клавишу «Enter». При этом **обнаружено** Платежное поручение № 13-946 от 29 августа 2019 г. на сумму 953 млн. 710 тыс. 845 рублей. Плательщик - ЗАО «Л-нефтепродукт»; Банк плательщика - Волгоградский ф-л АКБ Сбербанка России, р/сч. № 345840, Код 241602/767; Получатель - ООО «Проба - Х»; Банк получателя - МКБ «Русский банк» в г. Москве МФО 54803218, Код 2813460012, р/сч. № 243712. Данное платежное поручение специалистом распечатано на бумаге с использованием принтера, стандартного картриджа (красящая лента черного цвета) и программного обеспечения; прилагается к настоящему протоколу.

Одновременным нажатием клавиш «Ctrl», «L» была получена внутренняя спецификация диска. Всего на диске 1457664 байта памяти, из них свободно 1411584 байта; на диске находится четыре файла, каталогов - нет; названия файлов занимают на диске 45761 байт памяти; метка тома диска - DIMA-136, серийный номер диска - 0FDE:1A74.

После осмотра дискета упакована в алюминиевую фольгу и вложена в бумажный пакет № 1 размером 200×150 мм, который заклеен и опечатан печатью № 23 для пакетов Следственного управления УМВД РФ по Волгоградской области. *На пакете сделана следующая надпись:* «Дискета размером 3,5 дюйма, изъятая 30.08.2019 года в помещении Группы корреспондентских отношений ТРКЦ ГУ ЦБ России по Волгоградской области, осмотренная 31.08.2019 г. в кабинете № 134 в помещении УВД Волгоградской области»; подписи следователя, специалиста и понятых.

Фрагмент постановления о назначении программно-технической экспертизы

Вариант № 1

УСТАНОВИЛ:

1 ноября 2019 г. неизвестные лица, используя компьютер АКБ «Волгобанк» г. Волгограда, по сети «Спринт» провели фиктивный платеж в адрес Московского филиала

АКБ «Т-банк» о перечислении с расчетного счета АООТ «Л-нефтепродукт» 423,5 млн. рублей на расчетный счет АОЗТ «П-Траст».

5 ноября 2019 г. при попытке получения указанных денежных средств в помещении Московского филиала АКБ «Т-банк» были задержаны предприниматель А.В. Васин и исполнительные директора филиалов АОЗТ «Планета-Траст» А.Н. Кожин и В.С. Алексеев.

Слагаемые указанной выше суммы снимались задержанными лицами с р/с АОЗТ «Планета-Траст» в счет оплаты ряда фиктивных контрактов, заключенных между АОЗТ «Планета-Траст» и его филиалами, между филиалом, руководимым А.Н. Кожиным, и предпринимателем А.В. Васиным. При проведении обыска в рабочем кабинете генерального директора АОЗТ «Планета-Траст» Б.М. Трегубова были **изъяты персональные компьютеры, печатающие устройства (принтеры), дискеты и документы**, в том числе письмо А.В. Васину от А.Н. Кожину, письмо А.Н. Кожину и В.С. Алексееву от Б.М. Трегубова с указанием на заключение ряда контрактов, а также сами контракты.

Принимая во внимание, что по настоящему уголовному делу для решения вопросов, связанных с компьютерной информацией, необходимо производство программно-технической экспертизы, руководствуясь ст. ст. 195 (196) и 199 УПК РФ,

ПОСТАНОВИЛ:

Назначить по настоящему уголовному делу программно - техническую экспертизу, производство которой поручить экспертам Информационного центра Главного управления внутренних дел УМВД РФ по Московской области.

На разрешение экспертов поставить следующие вопросы:

1. Какая информация содержится на жестких дисках персональных компьютеров, а также на изъятых дискетах?

2. Подготовлены ли предъявленные на исследование документы на представленных на исследование печатающих устройствах (принтерах)?

3. Возможно ли раскодировать информацию, записанную в сложных форматах? Если да, то каково ее содержание в человекочитаемой форме?

4. Возможно ли получить скрытую информацию, касающуюся фирмы «Планета-Траст»? Если да, то распечатайте ее в человекочитаемой форме?

Для их разрешения **предоставить** в распоряжение экспертов следующие материалы:

- **персональные компьютеры** IBM PC AT 286 номер 06868 и IJF SUPER 286;

- **печатающие устройства** (принтеры) № 2911S96692 и № 8008661- 9Z;

- **дискеты** в количестве 34 штук, **упакованные в специальный алюминиевый футляр № 1;**

- **документы** на 9 листах, **упакованные в бумажный пакет № 2**. Вышеуказанные материалы опечатаны печатью для пакетов № 23 Главного управления внутренних дел г. Москвы.

Поручить начальнику ИЦ ГУВД Администрации Московской области разъяснить назначенным им экспертам их права и обязанности, предусмотренные ст. 57 УПК РФ, предупредить об уголовной ответственности за дачу заведомо ложного заключения в соответствии со ст. 307 УК РФ.

СЛОВАРЬ СПЕЦИАЛЬНЫХ ТЕРМИНОВ

Антивирусная программа - программа для ЭВМ, предназначенная для поиска, регистрации и уничтожения вредоносных программ для ЭВМ (компьютерных вирусов).

Аппаратура - физическое оборудование ЭВМ: механические, магнитные, электрические, электромагнитные, электронные, оптические и магнитооптические устройства.

Аттестованное средство вычислительной техники - средство вычислительной техники в отношении которого проведено специальное исследование на предмет отсутствия вредоносных программных и аппаратных средств с выдачей Аттестата соответствия требованиям по безопасности информации.

База данных - объективная форма представления и организации совокупности данных, систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

Базовая система ввода-вывода информации (BIOS) - один из модулей операционной системы (ОС) MS DOS, выполняющий автоматическое тестирование персональной ЭВМ при ее включении, вызов блока начальной загрузки ОС и обслуживание системных вызовов (прерываний).

Байт - единица измерения информации; наименьшая адресуемая единица данных или памяти ЭВМ. 1 байт - объем емкости памяти, необходимый для хранения в нем 1 символа.

Винчестер - малогабаритный пакет жестких магнитных дисков, герметизированных вместе с головками записи-чтения информации; является внешней несменной памятью ЭВМ.

Виртуальный диск - программное представление (имитация) несуществующего физического магнитного диска в виртуальной операционной системе.

Вычислительная сеть - сеть передачи данных, в одном или нескольких узлах которой размещены ЭВМ.

Гибкий магнитный диск (ГМД или флоппи-диск) - сменный магнитный диск на гибком физическом носителе, используемый в персональной ЭВМ в качестве внешней памяти прямого доступа. Выпускаются диски диаметром 200 мм (8 дюймов), 133 мм (5,25 дюйма) и 90 мм (3,5 дюйма).

Данные - информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека.

Диск - машинный носитель информации, представляющий собой круглую пластину, покрытую слоем материала, способного запоминать и воспроизводить информацию. Различают магнитные, магнитооптические и оптические диски.

Дискета - футляр с гибким магнитным диском, устанавливаемым в активный накопитель информации.

Дисковод - механизм для установления и работы с дисками; является одним из узлов накопителя на магнитных дисках.

Дисплей - устройство отображения информации, основанное на использовании электронно-лучевой трубки и снабженное клавиатурой для ввода данных в ЭВМ, контроля вычислительных процессов и управления ЭВМ.

Достоверность передачи информации - соответствие принятого сообщения переданному (вероятность отсутствия ошибок).

Жесткий диск - металлический диск, обе поверхности которого покрыты ферромагнитным слоем.

Интегральная микросхема (ИМС) - микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие.

Канал электросвязи - часть сети электросвязи, связывающая между собой источник и приемник сообщений. Под сетью электросвязи понимаются технологические системы, обеспечивающие один или несколько видов передач - телефонную, телеграфную, факсимильную, передачу данных и других видов документальных сообщений, включая обмен информацией между ЭВМ, телевизионное, звуковое и иные виды радио- и проводного вещания.

Каталог (директорий) - справочник файлов и библиотек программ со ссылками на их расположение. Используется операционной системой для определения местоположения файла (библиотеки программ). Система каталогов может включать главный (корневой) каталог и подкаталоги (поддиректории).

Код - программа для ЭВМ, находящаяся в формате машинного языка.

Компьютерный вирус - вредоносная программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

Конфигурация - компоновка системы с четким определением характера, количества, взаимосвязей и основных характеристик ее функциональных элементов; совокупность аппаратных средств и соединений между ними; перечень средств, включаемых в данный комплекс или систему.

Конфигурация операционной системы - разновидность версии операционной системы, адаптированной для конкретной ЭВМ.

Концентратор - функциональное устройство, позволяющее средству передачи данных обслуживать большее количество источников данных по меньшему числу каналов передачи данных.

Криптография - метод шифрования и дешифрования данных.

Локальная вычислительная сеть - вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования; сеть не использует средства электросвязи общего назначения и узлы ее расположены на небольшом расстоянии.

Магнитооптический диск - диск, в котором для хранения и поиска информации используется магнитооптический эффект: запись данных выполняется лазерным лучом и магнитным полем, считывание данных лазерным лучом, уничтожение данных лазерным лучом, размагничивающим соответствующие участки поверхности путем разогрева их до требуемой температуры.

Метка тома - физическая запись на внешнем машинном носителе информации, записываемая на том (диск) при его инициализации (разметке) и содержащая регистрационный номер тома (диска), адрес области меток файлов, идентификатор владельца тома (диска).

Модем - функциональное устройство, обеспечивающее модуляцию и демодуляцию сигналов; преобразующее цифровые сигналы в аналоговую форму и обратно для передачи их по каналам электросвязи.

Монитор - видеоконтрольное устройство.

Несанкционированный доступ (НСД) - преднамеренное обращение субъекта к данным и компьютерной информации, доступ к которым ему не разрешен, независимо от цели обращения.

Оперативная память - программно-адресуемая память, быстродействие которой соизмеримо с быстродействием центрального процессора; предназначена для хранения исполняемых в данный момент программ и оперативно необходимых для этого данных.

Операционная (мониторная) система (ОС) - комплекс программных средств, обеспечивающих управление выполнением программ для ЭВМ и способных реализовать функции планирования, управления вводом-выводом, управления данными и т. п.

Оптический диск - диск, предназначенный для одноразовой записи и многоразового считывания информации посредством лазерного луча. Стирание и изменение информации не предусмотрено. Известны диски типа CD-ROM (от Compact Disk - Read-Only Memory - компакт-диск-ПЗУ).

Пакет прикладных программ - система прикладных программ, предназначенных для решения задач определенного класса.

Перезагрузка - повторная начальная загрузка операционной системы, выполняемая, как правило, при остановке ("зависании") ЭВМ, когда другие способы восстановления ее нормального функционирования не дают результатов.

Периферийное устройство - устройство, имеющее подчиненный кибернетический статус в информационной системе: любое устройство, обеспечивающее передачу данных и команд между процессором и пользователем относительно определенного центрального процессора; комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора.

Персональная ЭВМ (персональный компьютер) - универсальная микрокомпьютерная система, предназначенная для использования в автономном режиме, системе ЭВМ или их сети для решения задач различной профессиональной ориентации, например, используемая в качестве рабочего места специалиста.

Перфорирование - способ записи информации на перфокарту или перфоленту путем пробивки кодовых комбинаций сквозных отверстий с помощью специального технического устройства - перфоратора.

Печать - вывод данных (текстово-графической информации) на печатающее устройство (принтер, графопостроитель-плоттер) и получение их распечатки на физическом носителе (листинге).

Программа для ЭВМ - объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

Программное обеспечение - совокупность управляющих и обрабатывающих программ, предназначенных для планирования и организации вычислительного процесса, автоматизации программирования и отладки программ решения прикладных задач, а также программных документов, необходимых для эксплуатации этих программ. В него входят: операционная система, программы технического обслуживания, система программирования.

Программный модуль - единица программного обеспечения.

Пластиковая карта (карточка) - машинный носитель информации в форме прямоугольной пластины, выполненной из поливинилхлорида (ПВХ), полихлорвинила (ПХВ) либо из композиционного материала, одним из компонентов которого являются

данные пластики. Пластиковая карта, как правило, имеет следующие линейные размеры - 85×54×0,76 мм.

Плата - сменная панель с электронными компонентами. «Материнская» плата - основная (базовая) плата, на которой находится центральный процессор, электрические проводники и разъемы для крепления остальных функциональных плат и электронных компонентов персональной ЭВМ.

Порт - многоразрядный вход или выход в техническом устройстве; точка взаимодействия двух технических устройств (например, ЭВМ с принтером или ЭВМ с адаптером канала связи - модемом); конец логического канала.

Принтер - алфавитно-цифровое печатающее устройство.

Протокол - **1.** Результат регистрации в хронологическом порядке информации о ходе вычислительного процесса. **2.** В вычислительных сетях - совокупность семантических и синтаксических правил, определяющих работу функциональных устройств в процессе связи.

Процессорный (системный) блок - основная часть базовой конфигурации ЭВМ с центральным процессором и периферийными устройствами.

Рабочая станция - узел локальной вычислительной сети, предназначенный для работы пользователя в интерактивном режиме.

Разметка (форматирование, инициализация) - подготовка машинного носителя информации к использованию путем записи служебной информации (например, первичная подготовка магнитного диска к работе включает разбиение дорожек диска на сектора, заполнение информационных полей определенным кодом, запись на нулевую дорожку программы начальной загрузки, загрузчика и некоторых системных данных).

Режим разграничения доступа - порядок доступа к данным и компьютерной информации в соответствии с установленными правилами.

Санкционированный доступ - доступ субъекта к данным и компьютерной информации, имеющего право (полномочия) на выполнение следующих действий: чтение (ознакомление), копирование (дублирование), изменение (обновление), модификация, стирание (частичное уничтожение), уничтожение и т.д.

Сектор - участок дорожки магнитного диска, являющийся минимальной физически адресуемой единицей памяти.

Сервер - ЭВМ, выполняющая определенные функции обслуживания пользователей; в вычислительных сетях - управляет использованием разделенных ресурсов (принтеров, внешней памяти, баз данных).

Спецификация - формализованное описание свойств, характеристик и функций объекта.

Средство вычислительной техники (СВТ) - техническое устройство, предназначенное для хранения, накопления, обработки, передачи данных и информации в процессе решения вычислительных и информационных задач.

Средство защиты информации (ограничения доступа) - совокупность аппаратных и программных средств, предотвращающих случайный или преднамеренный доступ к данным и охраняемой законом информации.

Стандартное программное обеспечение - программное обеспечение, поставляемое вместе с ЭВМ.

Стирание информации (данных) - частичное уничтожение данных и компьютерной информации, позволяющее при определенных условиях полностью или частично восстановить их оригинал с помощью специальных программ для ЭВМ.

Телекоммуникация - дистанционная связь; дистанционная передача данных.

Терминал - устройство для взаимодействия субъекта с вычислительной системой; в сетях ЭВМ - устройство, являющееся источником либо получателем данных.

Удаленный доступ - доступ к программам для ЭВМ и данным, осуществляемый с удаленного терминала.

Уничтожение информации (данных) - полное уничтожение данных и компьютерной информации без возможности их восстановления.

Устройство - конструктивно законченная техническая система, имеющая определенное функциональное назначение.

Утечка информации - неправомерный выход охраняемой законом информации за пределы пространства, контролируемого ее правообладателем.

Файл - поименованная область во внешней памяти ЭВМ.

Центральный процессор - большая интегральная микросхема, выполняющая в данной ЭВМ основные функции по обработке данных и управлению работой периферийных устройств.

ЭВМ - комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач.

Электронно-цифровая подпись - аппаратно-программное устройство криптографирования информации, данных и команд, позволяющее полностью гарантировать аутентичность сообщения, передаваемого по каналам электросвязи; зафиксировать попытки искажения передаваемого сообщения.

Электросвязь - всякая передача или прием знаков, сигналов, письменного текста, изображений, звуков по проводной, радио-, оптической и другим электромагнитным системам.