**КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

Уголовное наказание за совершение преступлений в сфере компьютерной информации предусмотрено главой 28-ой УК РФ. Преступными являются следующие виды деяний:

• неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК);

• создание, использование и распространение вредоносных программ для ЭВМ или машинных носителей с такими программами (ст. 273 УК);

• нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК).

Однако, в «чистом» - обособленном виде эти деяния встречаются очень редко. Как правило, они совершаются в совокупности с иными общественно опасными деяниями и имеют факультативный характер. Это обусловлено тем, что при использовании компьютерной информации в качестве средства совершения другого преступления, она сама становится предметом общественно опасного деяния. Невозможно противоправно воспользоваться компьютерной информацией не нарушив при этом ее правовой защиты, т. е. не совершив хотя бы одного из действий, перечисленных в ст. 20 Закона “Об информации, информатизации и защиты информации” РФ, а именно: утечки, хищения, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования.

Чаще всего компьютерная информация используется для совершения следующих преступлений, расположенных по ранжиру: нарушение авторских и смежных прав (ст. 146 УК); мошенничество (ст. 159 УК); подделка, изготовление или сбыт поддельных документов, штампов, печатей и бланков (ст. 327 УК); изготовление или сбыт поддельных кредитных либо расчетных карт и иных платежных документов (ст. 187 УК); изготовление или сбыт поддельных денег или ценных бумаг (ст. 186 УК); уклонение от уплаты налогов с организаций (ст. 199 УК); нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК); незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК). При раскрытии и расследовании данных преступных посягательств необходимо использовать методические рекомендации, относящиеся к расследованию преступлений в сфере компьютерной информации.

В действующем законодательстве Российской Федерации указан ряд терминов и определений, используемых для описания основных элементов криминалистической характеристики рассматриваемых преступных деяний.

Компьютерная информация – это сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, находящиеся на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Иными словами, это сведения, циркулирующие в вычислительной среде, зафиксированные на физическом носителе в форме, доступной восприятию ЭВМ, или передающиеся по каналам электросвязи посредством электромагнитных сигналов из одной ЭВМ в другую, из ЭВМ на периферийное устройство, либо на управляющий датчик оборудования.

Компьютерная информация всегда опосредована через физический (машинный) носитель, вне которого она не может существовать. Машинный носитель информации – это любое техническое устройство либо физическое поле, предназначенное для фиксации, хранения, накопления, преобразования и передачи компьютерной информации. Наиболее распространены следующие виды машинных носителей информации:

• внутренний накопитель на жестком магнитном или магнито – оптическом диске (НЖМД или НМОД – винчестер);

• внешний накопитель на жестком магнитном диске (ЗИП-драйвер);

• внешнее устройство накопления информации (стриммер);

• накопитель на магнитной ленте или специальной металлической нити (в кассетах или бобинах);

• гибкий магнитный диск (ГМД – дискета);

• оптический или магнитооптический диск (лазерный или компакт - диск);

• бумажная (картонная), пластиковая или металлическая карта;

• интегральная микросхема памяти (ИМСП) – микроэлектронное изделие окончательной или промежуточной формы, предназначенное для выполнения функций электронной схемы памяти ЭВМ и других компьютерных устройств, элементы и связи которого неразрывно сформированы в объеме и (или) на поверхности материала, на основе которого изготовлено изделие;

• листинг – распечатка компьютерной информации на твердом физическом носителе (бумаге или пленке);

• физическое поле – материальный носитель физических взаимодействий искусственного или естественного происхождения;

• электромагнитный сигнал – средство переноса информации в пространстве и во времени с помощью электромагнитных колебаний (волн).

Основные криминалистические особенности компьютерной информации заключаются в следующем:

1) она достаточно просто и быстро преобразуется из одной объектной формы в другую, копируется (размножается) на различные виды машинных носителей и пересылается на любые расстояния, ограниченные только радиусом действия современных средств электросвязи;

2) при изъятии компьютерной информации, в отличие от изъятия материального предмета (вещи), она сохраняется в первоисточнике, т.к. доступ к ней могут одновременно иметь несколько лиц, например, при работе с информацией, содержащейся в одном файле, доступ к которому одновременно имеют несколько пользователей сети ЭВМ.

Выделяется два основных вида компьютерной информации – общего пользования (общедоступная) и охраняемая законом (конфиденциальная).

К конфиденциальной относится та компьютерная информация, которая удовлетворяет двум обязательным условиям:

• информация должна быть документированной (документом) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;

• доступ к такой информации должен ограничиваться в соответствии с законодательством Российской Федерации.

Последнему условию удовлетворяют сведения, отнесенные к различным видам тайн (государственная, служебная, коммерческая, банковская, следственная, медицинская, адвокатская, личная, семейная и др.); передаваемые путем переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений; являющиеся объектом авторских и смежных прав; имеющие статус персональных данных – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность.

Конфиденциальная компьютерная информация всегда будет чужой для лица, не имеющего к ней доступа на законных основаниях, либо получившего его в нарушении установленного порядка, с нарушением правил ее защиты.

Вместе с этим, защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

В соответствии с Концепцией правовой информатизации России, утвержденной Указом Президента РФ от 28.06.93 г. № 966, использование информации сопровождается строгим соблюдением требований ее защиты, а нарушение требований защиты информации расценивается как несанкционированный доступ (НСД) к информации.

Под доступом к компьютерной информации понимается всякая форма проникновения к ней с использованием средств электронно - вычислительной техники, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать и копировать).

Для защиты компьютерной информации от несанкционированного доступа используются разнообразные средства защиты. Под средствами защиты компьютерной информации понимаются - технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих информацию, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Средства защиты конфиденциальной компьютерной информации, обрабатываемой в государственных информационных системах и системах Центрального Банка России, подлежат обязательной сертификации. Деятельность юридических и физических лиц, связанная с разработкой, производством, реализацией и эксплуатацией средств защиты информации, а также предоставлением услуг в этой области, осуществляется исключительно на основании лицензии.

Уничтожение компьютерной информации – ликвидация компьютерной информации любыми способами без возможности ее восстановления

Блокирование компьютерной информации – физическое воздействие на компьютерную информацию, ее машинный носитель и (или) программно - технические средства ее обработки и защиты, результатом которого явилась временная или постоянная невозможность осуществлять какие-либо операции над компьютерной информацией.

Модификация компьютерной информации – это внесение в нее любых несанкционированных собственником или владельцем изменений.

Копирование компьютерной информации – это повторение и устойчивое запечатление компьютерной информации любыми способами на отличном от оригинала машинном носителе при одновременной сохранности признаков, идентифицирующих ее.

Электронная вычислительная машина (ЭВМ) – программируемое электронное техническое устройство, состоящее из одного или нескольких взаимосвязанных центральных процессоров и периферийных устройств, управление которых осуществляется посредством программ, и предназначенное для автоматической обработки информации в процессе решения вычислительных и (или) информационных задач.

Система ЭВМ – совокупность ЭВМ, программного обеспечения и разнообразных технических устройств (периферийного оборудования, управляющих датчиков, исполнительных механизмов и др.), предназначенные для организации и/или осуществления информационных процессов.

Сеть ЭВМ – две и более ЭВМ, объединенные между собой с помощью средств электросвязи (электрических проводников, модемов, коммутирующих устройств и др.).

Нарушение работы ЭВМ, системы ЭВМ или их сети – это временное или устойчивое создание помех для их функционирования в соответствии с назначением.

Типичными орудиями подготовки, совершения и сокрытия преступлений в сфере компьютерной информации являются:

1. Средства электронно-вычислительной техники (СВТ):

- различные виды ЭВМ (персональная ЭВМ (ПЭВМ), сервер сети ЭВМ и электросвязи (пейджинговой, сотовой и др.), аппарат сотовой электросвязи с функцией работы в сети Интернет, банкомат, контрольно - кассовая машина с блоком фискальной памяти, электронная записная книжка, электронный переводчик, графическая станция, электронный издательский комплекс (типа “Ризограф”), супер смарт-карта и др.);

- периферийные устройства (видеоконтрольное устройство (дисплей, монитор), устройство управления ЭВМ (клавиатура, манипуляторы (“мышь”, джойстик, “шар” – трэк-болл, “световое перо”, “сенсорный экран”, Isopoint Control), печатающее устройство (принтер – матричный, струйный, термографический (“лазерный”), графопостроитель, плоттер), устройство видеоввода информации (сканер, цифровая фото- или видеокамера), устройство графического ввода информации (графический электронный планшет, диджитайзер), устройство работы с пластиковыми картами (импринтер, считыватель (ридер) - оптический, магнитный или электромагнитный, перкодер или программатор) и др.;

- некоторые аппаратные средства (соединительные провода, кабели, шины, шлейфы, разъемы, СОМ - порты, “шнурки”, устройства электропитания, аппаратные средства защиты компьютерной информации от несанкционированного доступа и т.д.);

- устройства приема и передачи компьютерной информации (модем - внутренний или внешний, другие средства телекоммуникации);

- вредоносная программа для ЭВМ (компьютерный вирус, « троянский конь» для негласного получения и копирования конфиденциальной компьютерной информации, крэк-программа («взломщик» кодов защиты, генератор паролей доступа, дешифратор криптографической защиты) и др.).

2. Специальные технические средства (СТС), предназначенные (разработанные, приспособленные, запрограммированные) для негласного получения (изменения, уничтожения, блокирования) информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

3. Разнообразные магнитные материалы и технические устройства, генерирующие направленное электромагнитное излучение.

4. Электромонтажный инструмент и материалы.

5. Контрольно-измерительные приборы и устройства.

6. Средства систем электросвязи и их компоненты.

Наиболее широко применяемым универсальным орудием совершения преступления в сфере компьютерной информации является ПЭВМ или ПК - персональный компьютер с соответствующим программным обеспечением и периферийным оборудованием.

При совершении преступления в сфере компьютерной информации с использованием новых телекоммуникационных технологий и средств электросвязи место совершения общественно опасного деяния, как правило, не совпадает с местом реального наступления общественно опасных последствий. Таких мест может быть несколько. Они могут быть удалены друг от друга на значительные расстояния, находиться в транспортных средствах, различных учреждениях, на участках местности, в том числе в различных странах и на континентах. Последнее возможно по причине неограниченного радиуса действия, мобильности и доступности современных средств электросвязи, неотъемлемой частью которых является компьютерная информация. Поэтому, местом совершения преступления рассматриваемой категории целесообразнее всего считать то транспортное средство, тот участок местности или территорию того учреждения, организации, государства, где были совершены общественно опасные деяния независимо от места наступления преступных последствий.

На жаргонном языке компьютерных преступников называют “хэкерами”, “крэкерами” и “фрикерами”. Данные лица, как правило, обладают специальными познаниями и практическими навыками в области компьютерных технологий и, как минимум, являются пользователями ЭВМ. Как правило, в случае совершения преступления в сфере компьютерной информации в отношении юридического лица, преступником или сообщником (пособником) является сотрудник данного учреждения, организации. Это - операторы ЭВМ, периферийных устройств и средств связи; программисты; инженеры-системотехники; инженеры-электроники; администраторы баз данных; должностные и иные лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети.

Ведя речь о личности преступников, важно подчеркнуть, что данному типу людей присущи высокий уровень интеллектуального развития, нестандартность мышления, профессионализм, фанатичное отношение к новым компьютерным технологиям, изобретательность, богатая фантазия и скрытность. Преступник из числа сотрудников организации, как правило, является образцовым служащим, имеющим соответствующее образование. Указанные лица, как правило, ранее не совершали никаких преступлений. Нередко - это руководители различного ранга, обладающие распорядительными функциями, но непосредственно не отвечающие за конкретные участки работы с компьютерной информацией и ЭВМ.

Чаще всего преступления в сфере компьютерной информации совершаются устойчивыми преступными группами, для которых характерны мобильность, высокая техническая оснащенность, четкое распределение ролей, ярко выраженная корыстная мотивация, хорошо продуманная система сокрытия следов преступных деяний. Наибольшую опасность и сложность для выявления и раскрытия представляют преступные группы, имеющие в своем составе высококвалифицированных специалистов, обладающих специальными познаниями в области негласного получения и защиты компьютерной информации. Большая часть преступлений, совершенных указанными субъектами, остаются латентными.

Мотивы и цели совершения преступления в сфере компьютерной информации различны. В рейтинговом порядке их можно расположить следующим образом: корысть, месть, личные неприязненные отношения с сослуживцами и руководством по месту работы, стремление скрыть другое преступление, хулиганские побуждения и озорство, исследовательские цели, демонстрация личных интеллектуальных способностей или превосходства.

Практически невозможно привести исчерпывающий перечень способов совершения преступления в сфере компьютерной информации, так как их содержание могут составлять самые разнообразные действия, в зависимости от изобретательности, преступной квалификации и интеллектуальности преступника. Однако, несмотря на многообразие способов совершения преступления рассматриваемого вида их можно сгруппировать следующим образом:

1) использование либо распространение вредоносных программ для ЭВМ или машинных носителей с такими программами;

2) перехват компьютерной информации;

3) несанкционированный доступ к компьютерной информации;

4) манипуляции данными и управляющими командами;

5) нарушения правил эксплуатации средств электронно - вычислительной техники, электросвязи, защиты компьютерной информации, а также обработки, хранения и передачи конфиденциальной компьютерной информации;

6) комплексные методы.

Наиболее часто используются следующие способы подготовки, совершения и сокрытия преступления в сфере компьютерной информации: хищение (изъятие) машинных носителей информации, в т.ч. путем их подмены; копирование конфиденциальной компьютерной информации; создание вредоносных программ для ЭВМ; распространение вредоносных программ; распространение машинных носителей, содержащих вредоносные программы для ЭВМ; внесение изменений в существующие программы; фальсификация входных и/или выходных электронных документов; изготовление дубликатов документов и их носителей; использование недостатков программ для ЭВМ; дезактивация либо обход защиты компьютерной информации и СВТ от несанкционированного доступа (путем подбора пароля, кода доступа и др.); перехват компьютерной информации из канала электросвязи; неправомерный доступ к СВТ и машинным носителям; блокирование, модификация, копирование, уничтожение, повреждение компьютерной информации с использованием специально приспособленных, разработанных, запрограммированных технических средств негласного получения информации.

При выявлении и расследовании преступлений в сфере компьютерной информации подлежат установлению: факт совершения преступления (не является ли событие следствием непреодолимых факторов - погодных условий, природных катастроф, самопроизвольных технических аварий, поломок и неполадок); непосредственная причина нарушения безопасности компьютерной информации и орудий ее обработки; предмет преступного посягательства; категория компьютерной информации (общего пользования или конфиденциальная); место и время совершения преступления; способ совершения преступления; совершено ли преступление дистанционно извне помещения (по каналам электросвязи и локальной сети ЭВМ); режим работы с компьютерной информацией, орудиями ее обработки и средствами их защиты; с помощью каких конкретно СВТ совершено преступление (тип, вид, модификация, функциональное назначение, техническое состояние и другие признаки); конкретный терминал или участок сети (абонентский (регистрационный) номер, код, шифр, рабочая частота), режим их работы и ответственное лицо; имела ли место утечка конфиденциальной информации (какой именно, откуда, при каких обстоятельствах); размер материального ущерба, из чего он складывается; с какими служебными действиями, с операциями технологического процесса связано преступление, кто из должностных лиц или работников несет ответственность и имеет непосредственное отношение к ним в силу технологии производства, должностных инструкций (обязанностей) или командно - административного управления; личность подозреваемого и основные ее характеристики (обладает ли специальными познаниями, в какой области и каков их уровень); не совершено ли преступление группой лиц, каковы роль и характер каждого участника преступления; мотив преступления; кто является потерпевшим (физическое или юридическое лицо); кому было известно о намерениях преступников, кто участвовал в сокрытии преступления и его следов; причины и условия, способствовавшие совершению и сокрытию преступления, что усугубило их проявление - не обусловлено ли это нарушениями нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам.

Организация расследования на первоначальном этапе

Раскрывать преступления в сфере компьютерной информации, сложно, так как нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место (например, сбой в работе ЭВМ и программного обеспечения, средств электросвязи, энергообеспечивающего оборудования; замыкания в электропроводке и т.п.).

Перечень неотложных следственных действий и оперативных мероприятий, очередность их проведения будут определяться конкретной следственной ситуацией, в которой начинается расследование. Следственная ситуация характеризуется прежде всего объемом и достоверностью исходной криминалистически значимой информации, имеющейся в распоряжении следователя и оперативного работника.

Поводами и основаниями для возбуждения уголовных дел чаще всего служат: заявления граждан (конкретных потерпевших); сообщения руководителей предприятий, учреждений, организаций и должностных лиц (базирующиеся, как правило, на материалах контрольно - ревизионных проверок и сообщениях служб безопасности); сведения, полученные в результате проведения оперативно -розыскных мероприятий; непосредственное обнаружение следователем, прокурором или судом признаков преступления; статьи, заметки и письма, опубликованные в средствах массовой информации, а также в сети «Интернет».

Как правило, возбуждению уголовного дела предшествует предварительная проверка материалов, поступивших в правоохранительные органы. В связи с этим, следователь может заблаговременно ознакомиться с собранными по делу материалами, совместно с оперативным сотрудником выбрать в тактическом отношении наиболее оптимальный момент для возбуждения дела, а также определить характер и последовательность первоначальных следственных действий, организационных и иных мероприятий. **Успех расследования преступления в сфере компьютерной информации во многом обеспечивают:** быстрота и решительность действий следователя и оперативного сотрудника в самые первые часы производства по делу; организованное взаимодействие с различными подразделениями правоохранительных органов; наличие специалиста в области компьютерной обработки информации (возможно, пользователя ЭВМ).

В ходе предварительной проверки материалов **при решении вопроса о возбуждении уголовного дела** следователь должен прежде всего получить четкое и полное представление о предмете посягательства, месте его нахождения и условиях охраны; о характере деятельности и структуре объекта, где возможно было совершено преступление; об особенностях технологии производства; изучить конкретные условия деятельности данного объекта, существующий там порядок учета и отчетности, систему товаро- и документооборота, коммуникативные и иные тактико-технические характеристики используемой компьютерной техники, организацию охраны. Необходимо также хорошо знать служебные обязанности лиц, имеющих прямые или косвенные отношения к орудиям обработки и компьютерной информации, которые стали предметом преступного посягательства.

**К типичным признакам подготовки, совершения и сокрытия преступления в сфере компьютерной информации относятся:** появление в ЭВМ, системе ЭВМ или их сети фальшивых данных; несанкционированные изменения структуры файловой системы, программного обеспечения и конфигурации ЭВМ, системы ЭВМ или их сети; необычные (нестандартные) проявления в работе СВТ и их программного обеспечения; частые сбои в работе аппаратуры; жалобы клиентов на предоставление некачественного доступа к ЭВМ, системе ЭВМ, их сети или компьютерной информации; сверхурочная работа некоторых сотрудников на ЭВМ, в системе ЭВМ или их сети, нарушение установленного графика их эксплуатации; нерегламентированный доступ к ЭВМ, системе ЭВМ, их сети и к компьютерной информации отдельных субъектов; нарушение правил работы с компьютерной информацией и несанкционированные манипуляции с ней; чрезмерный интерес отдельных субъектов (клиентов, сотрудников) к содержанию чужих распечаток (листингов) и компьютерной информации определенной категории; случаи перезаписи отдельных данных и компьютерной информации без серьезных требуемых на то причин; применение на рабочем месте и вынос с работы личных машинных носителей информации под различными предлогами (записи игр и т.п.); исследование мусорных корзин (контейнеров) с технологическими отходами компьютерной обработки информации; случаи утечки конфиденциальной информации, либо обнаружение негласных устройств ее получения; нарушение установленных правил оформления документов при работе с ЭВМ, системой ЭВМ, их сетью или компьютерной информацией; создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом; несоответствие данных, содержащихся в первичных (исходных) документах, данным машинограмм и иным более поздним по времени создания документам; подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории.

Чтобы детально разобраться в **особенностях деятельности** **потерпевшего** (физического или юридического лица), следователю и оперативному сотруднику необходимо ознакомиться с соответствующей справочной литературой, изучить ведомственные нормативные акты. Исключительно важное значение имеют консультации со специалистами. Для этих целей могут быть привлечены любые лица, обладающие необходимыми знаниями и опытом для дачи консультаций по делу. Как правило, это квалифицированные сотрудники различных организаций, осуществляющих свою деятельность в сфере информации, информатизации и защиты информации. Наиболее предпочтительны сотрудники: Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России) и ее региональных структурных подразделений (Спеццентров); оперативно-технических подразделений правоохранительных органов; подразделений «К» при УСТМ МВД России; специалисты межрегиональных Центров защиты информации, функционирующих на базе гражданских высших учебных технических заведений; научные работники исследовательских институтов и лабораторий, а также учебных заведений.

**Для преступлений в сфере компьютерной информации** **типичны три ситуации первоначального этапа расследования:**

1. Сведения о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствуют.

2. Имеются сведения о причинах возникновения преступления, способе его совершения, но нет сведений о личности преступника.

3. Известны причины возникновения преступления, способы его совершения и сокрытия, личность преступника и другие обстоятельства.

**В первых двух следственных ситуациях** обычно планируют и осуществляют следующие неотложные следственные действия, оперативно - розыскные, организационные и иные мероприятия:

1) получение объяснения (допрос) заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей ( очевидцев);

2) вызов и инструктаж необходимых специалистов для участия в осмотре места происшествия;

3) осмотр места происшествия (с осмотром, предварительным исследованием и изъятием машинных носителей и компьютерной информации, СВТ, документов и т. п.);

4) проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, определения рабочего места преступника, обнаружения следов и других вещественных доказательств;

5) изучение справочной литературы, ведомственных нормативных актов, положений, инструкций, правил эксплуатации конкретного СВТ и порядка работы с компьютерной информацией, а также консультации с соответствующими специалистами;

6) наведение справок в контролирующих, инспектирующих и лицензирующих организациях и их структурных подразделениях (Гостехкомиссии, налоговой инспекции, Комитете по контролю за использованием радиочастот, Энергонадзоре, Госпожнадзоре, КРУ, торговой инспекции и т.п.);

7) истребование материалов контрольных проверок, инвентаризаций и ревизий (соблюдения правил обработки информации, системы защиты конфиденциальной информации, оборота электронных документов и др.) за интересующий следствие период, в случае необходимости - организовать их производство (в т.ч. повторно);

8) выемку и последующий осмотр недостающих документов (в том числе находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой по имеющимся данным совершены преступные действия, а также орудий (СВТ, программ для ЭВМ, компьютерной информации, предметов, материалов и др.), с помощью которых они, возможно, были изготовлены;

9) допросы подозреваемых и/или свидетелей, ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации;

10) обыски на рабочих местах и по месту проживания подозреваемых;

11) назначение экспертиз - программно-технической, радиотехнической, технической, бухгалтерской, полимерных материалов и изделий из них и иных.

Дальнейшие действия планируются с учетом дополнительной информации, полученной при производстве вышеуказанных действий.

**При наличии третьей следственной ситуации необходимо**:

1) изучить поступившие материалы с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка их передачи в органы предварительного следствия. При необходимости - принять меры к получению недостающей процессуальной информации;

2) решить вопрос о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях;

3) личный обыск задержанного;

4) осмотр места происшествия с участием соответствующих заранее приглашенных специалистов;

4) допрос задержанного;

5) обыски на рабочем месте и по месту проживания задержанного;

6) установление связей задержанного и лиц, причастных к совершению преступления;

7) допрос свидетелей (очевидцев);

8) допрос подозреваемого;

9) выемка и осмотр следующих вещественных доказательств и документов: подлинных документов, удостоверяющих личность преступника и наличие у него соответствующих специальных познаний, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в том числе документов, находящихся в электронной форме на машинных носителях информации); орудий подготовки, совершения и сокрытия преступления; предмета преступления;

10) допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за конкретный участок работы по фактам установленных нарушений;

11) истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении с конфиденциальной информацией, с бланками строгой отчетности, компьютерной информацией, ЭВМ, системой ЭВМ, их сетью и т. п.;

12) допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с преступником;

13) анализ полученной информации и решение вопроса о необходимости назначения судебных экспертиз, проведения ревизии, инвентаризации или контрольной проверки (в том числе повторной).

В очередность перечисленных следственных действий, оперативных и организационных мероприятий могут быть внесены коррективы в зависимости от изменения ситуации.

Особенности тактики производства отдельных следственных действий

Все следственные действия по делам о преступлениях в сфере компьютерной информации проводятся в строгом соответствии с правилами, регламентированными действующим уголовно-процессуальным законодательством, но с учетом следующих основных особенностей: следственное действие должно быть заблаговременно подготовлено и детально спланировано; в каждом следственном действии должны принимать участие специалисты четко представляющие свои задачи, права и обязанности; понятые должны обладать минимально необходимыми специальными познаниями в области обработки компьютерной информации (на уровне бытовых пользователей ПЭВМ), следователь и специалисты - познаниями в части полной сохранности (неизменяемости) компьютерной информации, содержащейся на осматриваемом (изымаемом) средстве электронно-вычислительной техники; для осмотра, обыска и выемки компьютерной информации и ее носителей заранее должны быть подготовлены необходимые СВТ и материалы.

При **осмотре места происшествия** в состав следственно - оперативной группы в зависимости от конкретной следственной ситуации, помимо следователя, должны входить: специалист-криминалист, знающий особенности работы со следами по преступлениям данной категории; специалист по СВТ; сотрудник Гостехкомиссии России, Центра защиты информации (при наличии на месте происшествия конфиденциальной компьютерной информации, машинных носителей с ней, специальных средств защиты от НСД и(или) СТС негласного получения (уничтожения, блокирования) компьютерной информации); специалист по сетевым технологиям (в случае наличия периферийного оборудования удаленного доступа или локальной компьютерной сети); специалист по системам электросвязи (при использовании для дистанционной передачи данных каналов электросвязи); оперативные сотрудники (отдела «К» или ОБЭП); участковый оперуполномоченный, обслуживающий данную территорию; инспектор отдела вневедомственной охраны (в случае, когда место происшествия или СВТ, находящееся на нем, одновременно является охраняемым объектом); специалист для проведения цветной фото- или видеосъемки следственного действия.

При необходимости в состав СОГ могут быть включены незаинтересованные в деле специалисты, знающие специфику работы осматриваемого объекта (инженеры-электрики, бухгалтеры со знанием СВТ, специалисты спутниковых систем связи, операторы компьютерных систем и сетей электросвязи, др.).

**Целью осмотра места происшествия является** установление конкретного СВТ и компьютерной информации, выступающей в качестве предмета и(или) орудия совершения преступления и несущих в себе следы преступной деятельности. Поэтому при производстве следственного действия целесообразнее всего использовать тактический прием «от центра - к периферии», где в качестве «центра» (отправной точки осмотра места происшествия) будет выступать конкретное СВТ и(или) компьютерная информация, обладающая вышеуказанными свойствами. Детальное описание данных предметов, их соединений (физических и логических) должно сопровождаться видеосъемкой, фиксирующей последовательность действий следователя и специалистов, а также полученный при этом результат.

Если при проведении осмотра места происшествия используются СВТ и специальные поисковые технические устройства (материалы), об этом делается соответствующая отметка в протоколе следственного действия с указанием их индивидуальных признаков (тип, марка, название, заводской номер и т.д.). Кроме того, в обязательном порядке делается отметка о том, что данные СВТ перед началом следственного действия в присутствии понятых были тестированы специальным программным средством (указывают его тип, вид, название, версию, автора и другие реквизиты) на предмет отсутствия в них вредоносных программно - аппаратных средств и закладок.

Следователю необходимо знать, что к изменению или уничтожению компьютерной информации (следов преступника и преступления) может привести не только работа за пультом управления СВТ (клавиатурой), но и одноразовое кратковременное включение-выключение СВТ или разрыв соединения между ними. Поэтому, если на момент проведения следственного действия какие-либо СВТ и иные электротехнические приборы и оборудование были включены или выключены, то они должны оставаться в таком положении до момента окончания осмотра их специалистом. По этой же причине подлежат обязательной охране все пункты отключения электропитания, находящиеся на месте происшествия.

**Особенно тщательно должны быть описаны в протоколе следующие фактические данные**: технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ, включая расположение и основные характеристики токонесущих коммуникаций; расположение СВТ относительно друг друга и оконечных устройств токонесущих коммуникаций; отсутствие или наличие соединений между ними (видимых и дистанционных); наличие или отсутствие соединений СВТ с оборудованием, в том числе находящемся вне территории осмотра (на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границы места осмотра, либо к аппаратам электросвязи (в таком случае границы осмотра места происшествия значительно расширяются); наличие, внешнее состояние, расположение и вид охраны СВТ и компьютерной информации от НСД, их основные технические характеристики; расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также относительно других рабочих мест; наличие в одном помещении со СВТ других электрических устройств и приборов ( телефонных и иных аппаратов электросвязи, пейджеров, систем электрочасофикации, оргтехники - ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишуших машинок, приборов электроосвещения, громкоговорителей, телевизоров, радиоприемников и т.д.).

Особенно тщательно должны быть осмотрены и описаны в протоколе **типичные вещественные доказательства:** вредоносные программы для ЭВМ и машинные носители с ними; программы для ЭВМ, заведомо приводящие к несанкционированным пользователем действиям ( влияющие на конечные результаты технологического процесса), а также их носители; обнаруженные СТС негласного получения (уничтожения, блокирования) компьютерной информации и магнитных носителей; специфические следы преступника и преступления. **Типичными следами являются**: следы орудий взлома, повреждения, уничтожения и(или) модификации охранных и сигнальных устройств; показания регистрирующей аппаратуры (видеотехники, электронного журнала учета операций с компьютерной информацией, доступа к ней и СВТ, др.); показания специальных мониторинговых (тестовых) программно-аппаратных средств, в том числе **электронной цифровой подписи** (сокр. **ЭЦП**); следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсильных вилках, тумблерах, кнопках и рубильниках, включающих и отключающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов; капли припоя, канифоли или флюса; следы вдавливания, проплавления, прокола, надреза изоляции токонесущих и соединительных (управляющих) проводов, приклеивания к ним сторонних предметов и устройств.

Осмотру подлежат следующие документы и их носители, являющиеся доказательствами подготовки, совершения и сокрытия преступления:

а) учетно-справочная документация по работе с СВТ и компьютерной информацией (технический паспорт или документ его заменяющий; журнал оператора или протокол автоматической фиксации технологических операций, доступа к СВТ и конфиденциальной компьютерной информации; журналы (карточки) учета машинных носителей информации, машинных документов, заказов (заданий или запросов), выдачи МНИ и машинных документов, массивов (участков, зон), программ, записанных на МНИ; журналы учета уничтожения брака бумажных МНИ и машинных документов; акты на стирание конфиденциальной информации и уничтожение машинных носителей с ней);

б) документация, отражающая санкционированность доступа ( удостоверения личности, электронные ключи доступа, пароли, персональные идентификационные номера (ПИН-коды), ЭЦП и иные средства (предметы или устройства) идентификации и аутентификации санкционированного пользователя);

в) учетно-регистрационная и бухгалтерская документация (лицензии и лицензионные соглашения; сертификаты соответствия СВТ, программ для ЭВМ, средств защиты информации (в том числе и ЭЦП), протоколов обмена информацией и форматов электронных документов установленным требованиям; договора (соглашения) на пользование СВТ и доступ к компьютерной информации с соответствующим комплектом документов; расчетно-кассовые и иные бухгалтерские документы, отражающие факт оплаты пользователем предоставленной ему услуги, отпущенного товара или осуществленной им кредитно-банковской операции);

г) учетно-контрольная документация (журналы (акты) пуско - наладочных, ремонтных и регламентных работ по техническому обслуживанию СВТ, программ для ЭВМ и средств защиты информации; журналы аварий и сбойных (нештатных) ситуаций; акты сбоев и ложных сработок охранных сигнализаций; акты контрольных проверок соблюдения режима безопасности информации, ревизий, служебных и иных документальных проверок; сводные отчеты и контрольные показатели по отдельным участкам работы, операциям и временным интервалам);

д) документация, регламентирующая действия обслуживающего персонала ( должностные обязанности; инструкции по работе с СВТ, программами для ЭВМ, средствами защиты от НСД, действий оператора в нештатной ( аварийной) ситуации; черновая рабочая документация оператора СВТ).

Их осмотр позволяет установить способ совершения преступления в сфере компьютерной информации, использованные для этого преступником материалы и средства, наличие у субъекта специальных навыков и познаний; выдвинуть версии о причинно-следственных связях.

**Осмотр средства электронно-вычислительной техники** в большинстве случаев является первоначальным следственным действием и проводится для обнаружения следов преступления; для решения вопросов о том, кем, с какой целью и при каких обстоятельствах было совершено преступление; выяснения обстановки происшедшего события; восстановления механизма совершения преступления. Проводить осмотр следует с участием специалиста.

**Прежде всего нужно** уяснить смысл и назначение СВТ; установить, включено оно или нет; проверить его работоспособность и наличие в его памяти компьютерной информации; установить наличие или отсутствие сопряжения с каналом электросвязи и другими техническими устройствами. После этого необходимо перейти к поиску материальных следов, содержащихся на его корпусе, отдельных деталях и проводных соединениях, в его постоянной и оперативной памяти (в виде компьютерной информации).

**При осмотре СВТ недопустимо использование:** магнитосодержащих материалов и инструментов; технических устройств, генерирующих и излучающих электромагнитные поля и наводки (магнитный порошок и кисточка, электромагнит, металлодетектор, мощные осветительные приборы, УФ и ИК излучатели и т.п.); кислотно-щелочных материалов и нагревательных приборов во избежании уничтожения (повреждения) СВТ и компьютерной информации, следов преступника и преступления. Вышеуказанными материалами и оборудованием можно пользоваться с особой осторожностью на расстоянии более 1 метра от СВТ и их соединительных проводов.

Осмотр СВТ обычно приводит к необходимости их изъятия для последующего экспертного исследования и(или) приобщения к делу в качестве вещественного доказательства.

**В протоколе осмотра СВТ фиксируют:** его тип (назначение), марку (название), конфигурацию, цвет и заводской номер (серийный, инвентарный или учетный номер изделия); тип (назначение), цвет и другие индивидуальные признаки соединительных и электропитающих проводов; состояние на момент осмотра (выключено или включено); техническое состояние - внешний вид, целостность корпуса, комплектность (наличие и работоспособность необходимых блоков, узлов, деталей, и правильность их соединения между собой), наличие расходных материалов, тип используемого машинного носителя информации; тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенного к нему электрооборудования, количество питающих электроразъемов-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; имеющиеся повреждения, непредусмотренные стандартом конструктивные изменения в архитектуре строения СВТ, его отдельных деталей (частей, блоков), особенно те, которые могли возникнуть в результате преступления, а равно могли спровоцировать возникновение происшествия; следы преступной деятельности (следы орудий взлома корпуса СВТ, проникновения внутрь корпуса, пальцев рук, несанкционированного подключения к СВТ сторонних технических устройств и др.); расположение СВТ в пространстве, относительно периферийного оборудования и других электротехнических устройств; точный порядок соединения СВТ с другими техническими устройствами; категорию обрабатываемой информации (общего пользования или конфиденциальная); наличие или отсутствие индивидуальных средств защиты осматриваемого СВТ и обрабатываемой на нем информации от несанкционированного доступа и манипулирования.

**Если на момент осмотра СВТ находится в рабочем состоянии необходимо детально описать:** расположение его рабочих механизмов и изображение на его видеоконтрольном устройстве (экране, мониторе, дисплее); основные действия, производимые специалистом при осмотре СВТ (порядок корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения (или соединения) СВТ, отсоединения проводов, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.).

Осмотр машинного носителя и компьютерной информации проводят по принципу «от общего к частному». Вначале описывают внешние индивидуальные признаки носителя: его цвет, размер, тип, вид, название, марка, заводской и индивидуальный номер, наличие наклейки и надписей на ней, наличие или отсутствие физических повреждений корпуса и следов на нем, положение элемента защиты от записи/стирания компьютерной информации. Затем переходят к осмотру компьютерной информации, содержащейся на МНИ. Перед началом ее осмотра необходимо указать в протоколе следственного действия: индивидуальные признаки используемого для осмотра средства электронно-вычислительной техники и основные реквизиты его программного обеспечения (тип, вид, марку, название, заводской или регистрационный номер, номер версии, юридический адрес и(или) автора программного продукта); юридические реквизиты программы, с помощью которой СВТ и его программное обеспечение в присутствии понятых было тестировано специалистом на предмет отсутствия вредоносных программно-аппаратных средств. После этого на указанный предмет проверяется и осматриваемая компьютерная информация.

Анализируя содержащуюся на осматриваемом носителе компьютерную информацию, надо установить сведения, имеющие отношение к расследуемому событию. Для оптимизации процесса осмотра большого объема информации можно применять функции автоматизированного поиска по конкретному слову (реквизиту), входящие в состав стандартного программного обеспечения ЭВМ. Ход осмотра должен дополнительно фиксироваться на цветной фото- или видеопленке. При обнаружении следов преступления, необходимо сделать распечатку всей или части компьютерной информации и приложить ее к протоколу следственного действия с указанием в протоколе индивидуальных признаков использованного для этого печатающего устройства (тип, вид, марку, название, номер).

**В протоколе осмотра, помимо вышеуказанного, необходимо отразить:** наличие, индивидуальные признаки защиты носителя от несанкционированного использования (голография, штрих-код, эмбоссинг, флуоресцирование, перфорация, ламинирование личной подписи и(или) фотографии владельца, их размеры, цвет, вид и т.п.); признаки материальной подделки МНИ и его защиты; внутреннюю спецификацию носителя - серийный номер и(или) метку 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 (структура их расположения на МНИ, название, имя и(или) расширение, размер (объем), в том числе тот, 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).

Готовясь к проведению **обыска**, следователь должен решить что и где он будет искать. Для этого необходимо тщательно изучить обстоятельства дела и собрать ориентирующую информацию о предмете обыска, месте его проведения и личности обыскиваемого. По делам о преступлениях в сфере компьютерной информации **предметом обыска могут быть** не только разнообразные СВТ, машинные носители и содержащаяся на них компьютерная информация, но и документы, средства электросвязи, разработанные и приспособленные специальные технические устройства, бытовые электротехнические устройства и оборудование, материалы и инструменты.

**В ходе обыска следует обращать внимание** на литературу, методические материалы и рекламные проспекты по компьютерной технике, обработке, защите, передаче и негласному получению компьютерной информации, а также на аудио-, видеокассеты, распечатки машинной информации и документы о соответствующем образовании. Особое внимание нужно уделять предметам, содержащим коды, пароли доступа, идентификационные номера, названия, электронные адреса пользователей конкретных компьютерных систем и сетей, алгоритмы входа и работы в системах и сетях. Необходимо также переиллюстрировать записные (телефонные) книжки, справочники и каталоги, в том числе электронные, находящиеся в памяти телефонных аппаратов, пейджеров и других компьютерных устройств.

Ценные доказательства могут быть обнаружены и при личных обысках подозреваемых (обвиняемых).

Предметом **выемки** в подавляющем большинстве случаев совершения преступления в сфере компьютерной информации являются персональные компьютеры, машинные носители информации (включая распечатки на бумаге, аудио- и видеокассеты, пластиковые карты) и всевозможные **документы** (в том числе и **электронные**), отражающие и регламентирующие различные операции, технологические процессы, связанные с обработкой, накоплением, созданием, передачей и защитой компьютерной информации, использования ЭВМ, системы ЭВМ и их сети. Последние находятся по месту работы (учебы) подозреваемого (обвиняемого), в рабочих кабинетах должностных лиц и других служебных (учебных) помещениях.

Помимо вышеуказанного **могут быть изъяты** специальные технические средства для негласного получения, модификации и уничтожения информации, свободные образцы почерка, бланки и фрагменты документов, заготовки машинных носителей информации, исходные тексты программ для ЭВМ, черновики и иные образцы для сравнительного исследования.

**Перед изъятием магнитных носителей информации** они должны быть в обязательном порядке упакованы в алюминиевый материал (алюминиевую фольгу или специальный контейнер), предохраняющий МНИ и его содержимое от внешнего электромагнитного и магнитного воздействия.

**Назначение экспертиз.** При расследовании преступления в сфере компьютерной информации наиболее характерна **компьютерно-техническая экспертиза***.* **Ее проводят в целях:** воспроизведения и распечатки всей или части компьютерной информации (по определенным темам, ключевым словам и т.д.), 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.); восстановления компьютерной информации, ранее содержавшейся на машинных носителях, но впоследствии стертой (уничтоженной) или измененной (модифицированной) по различным причинам; установления даты и времени создания, изменения (модификации), уничтожения, либо копирования информации (документов, файлов, программ); расшифровки закодированной информации, подбора паролей и раскрытия системы защиты от НСД; исследования СВТ и компьютерной информации на предмет наличия программно-аппаратных модулей и модификаций, приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; установления авторства, места (средства) подготовки и способа изготовления документов (файлов, программ), находящихся на МНИ; выяснения возможных каналов утечки информации из компьютерной сети, конкретных СВТ и помещений; установления возможных несанкционированных способов доступа к охраняемой законом компьютерной информации и ее носителям; выяснения технического состояния, исправности СВТ, оценки их износа, а также индивидуальных признаков адаптации СВТ под конкретного пользователя; установления уровня профессиональной подготовки отдельных лиц, проходящих по делу, в области программирования и в качестве пользователя конкретного СВТ; установления конкретных лиц, нарушивших правила эксплуатации ЭВМ, системы ЭВМ или их сети; установления причин и условий, способствующих совершению преступления в сфере компьютерной информации.

До вынесения постановления о назначении экспертизы рекомендуется проконсультироваться со специалистом по поводу ее целей, формулировки вопросов, характера предоставляемых материалов.

Может быть назначена идентификационная и не идентификационная компьютерно-техническая экспертиза.

По делам рассматриваемой категории из криминалистических экспертиз наиболее часто назначают дактилоскопическую, одорологическую, трасологическую, почерковедческую, фоноскопическую, автороведческую, радиотехническую и технико-криминалистическую экспертизу документов, экспертизу полимерных материалов и изделий из них.