МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное казенное образовательное учреждение
высшего образования «Казанский юридический институт
Министерства внутренних дел Российской Федерации»

Кафедра экономики, финансового права и информационных
технологий в деятельности ОВД

Шевко Н.Р., Панченко В.В., Каримов А.М.

«Методические рекомендации по предупреждению, пресечению, раскрытию и расследованию преступлений, совершенных с использованием высоких технологий и коммуникаций»

Казань – 2016

Оглавление

Глава 1. Уголовно-правовая и криминологическая характеристика преступлений, совершаемых с использованием высоких технологий.

1.1. Понятие и виды преступлений, совершаемых с использованием высоких технологий.

Вопросы противодействия преступлениям в сфере высоких технологий невозможно рассматривать, предварительно не выделив объект и предмет исследования.

Компьютерное преступление как уголовно-правовое понятие — это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

Первое преступление подобного рода в СССР было зарегистрировано в 1979 г. в Вильнюсе. Ущерб государству от хищения составил 78584 руб. Данный факт занесен в международный реестр правонарушений подобного рода и явился своеобразной отправной точкой в развитии нового вида преступлений в нашей стране.

На данный момент не существует общепризнанного определения таких преступлений, а сам термин «компьютерное преступление» носит операционный характер.

Вместе с тем исследователи выделяют три категории явлений, относимых к этому понятию:

– злоупотребление компьютером — ряд мероприятий с использованием компьютера для извлечения выгоды, которые нанесли или могли нанести ущерб;

– прямое незаконное использование компьютеров в совершении преступления;

– любое незаконное действие, для успешного осуществления которого необходимо знание компьютерной техники.

Наряду с этим в практический оборот введен термин «киберпреступность», охватывающий любое преступление, которое может совершаться с помощью компьютерной системы (сети) или в рамках компьютерной системы (сети). В принципе он охватывает любое преступление, которое может быть совершено в электронной среде. Существуют две категории киберпреступлений:

а) киберпреступление в узком смысле — любое противоправное деяние, осуществляемое посредством электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;

б) киберпреступление в широком смысле — любое противоправное деяние, совершаемое посредством или в связи с компьютерной системой или сетью, включая такие преступления, как незаконное хранение, предложение или распространение информации посредством компьютерной системы или сети.

Интересы преступных деяний, за исключением патологических проявлений, всегда связаны с сырьем и путями его реализации. Э. Тоффлер давно предположил, что «для цивилизации Третьей волны одним из главных видов сырья, причем неисчерпаемым, будет информация, включая воображение»[1], ну а сырье, технологии переработки, конечный продукт и способы не контролируемой (со стороны владельца) реализации всегда интересовали преступников в плане извлечения корыстного интереса, в том числе и сфере высоких технологий.

Широко распространенное понятие «высокие технологии» (англ. high technology, high tech, hi-tech) на самом деле собирательное понятие, и отсутствие четкого и официального определения предполагает, что это — наиболее новые и прогрессивные технологии современности. К высоким технологиям в настоящее время относят самые наукоемкие отрасли промышленности. При этом интегрирующим свойством по отношению как к научному знанию в целом, так и ко всем остальным технологиям обладают

[1] Тоффлер Э. Третья волна. — М.: ИЛ, 1999.

информационные технологии (ИТ). Исключительно важную роль ИТ оказывают на развитие радиоэлектронных средств (РЭС), которые в свою очередь не только обеспечивают все виды связи, вычислительные средства, продукцию оборонных промышленных комплексов и других отраслей промышленности, но и являются фундаментом существования ИТ.

Особо следует подчеркнуть, что в любой технический объект в настоящее время входит как обязательная составная часть специально разработанное математическое обеспечение, а в ряде случаев и банки данных, специально созданные для проектирования, модификации и эксплуатации объектов.[2]

Однако компьютерные системы не всегда являются частью информационных технологий. Термин «информационные технологии» означает процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов. Законодательно данное утверждение закреплено в Федеральном законе от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации».

Отождествление информационных систем с компьютерными системами уже привело к подмене понятия «формализованной (т. е. заключенной в некую форму) информации», обрабатываемой с помощью технических средств обработки, на «компьютерную информацию», как, например, в гл. 28 Уголовного кодекса РФ.

Сужение понятия информации в технических системах обработки информации (ТСОИ) до термина «компьютерная информация», с одной стороны, вынуждает подгонять факты незаконного манипулирования (использования) информации (в любой форме) к обозначенным в гл. 28 УК РФ составам преступлений, с другой – ограничивают область применения уголовной ответственности за их совершение.

[2] Россинская Е. Р. Проблемы становления компьютерно-технической экспертизы как нового рода инженерно-технических экспертиз // Криминалистика в XXI веке: материалы международной научно-практической конференции. — М.: Академия управления МВД России, 2001.

Здесь хотелось бы отметить общую тенденцию в развитии законодательных правовых норм — высокую бланкетность отдельных положений законодательства, что не позволяет однозначно трактовать понятия в столь специфичной сфере как информационные технологии. Так, например, вследствие того, что средства и методы в Федеральном законе «Об информации, информационных технологиях и о защите информации» объединены, информационная система определена как «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств», но при этом, из трех составляющих компонентов два — базы данных и технические средства — никак не определены.

Существующая на сегодняшний день законодательная (широкая) трактовка понятия информации как «сведений (сообщений, данных) независимо от формы их представления», наряду с отсутствием пояснений относительно определений «технических средств» обработки, «данных» и тем более «баз данных», позволяет отнести к информационным системам огромный перечень технологий обработки информации. Вместе с тем указанный Закон, кроме гарантий защиты информации, не несет никакой правоустанавливающей нормы, кроме как опосредованно обязывает собственника или ее «оператора» самостоятельно заботиться о ее защите.

Несоблюдение собственником ИС требований Закон определяет как препятствие в гарантированном возмещении возможных убытков лицу, не принимавшему мер по соблюдению конфиденциальности информации.

Таким образом, из положений Закона следует, что защита информации является заботой самого собственника. Между тем существующие расценки на сертифицированные средства защиты информации, услуги по специальным исследованиям на предмет информационной безопасности и ограниченный круг лицензиатов, оказывающих подобные услуги, практически оставляют собственника со своими проблемами один на один с

рекомендациями по созданию системы информационной защиты. Логично предположить, что представители защиты в делах по успешно совершенным компьютерным преступлениям смогут доказать отсутствие у потерпевшей стороны средств и методов защиты информации и потребовать от суда отклонения требований возмещения ущерба.

1.2. Классификация преступлений, совершаемых с использованием высоких технологий.

Исследователи, занимающиеся проблемой киберпреступности, предлагают различные классификации киберпреступлений. Киберпреступления подразделяют на виды в зависимости от объекта и предмета посягательства и т.д.

Самый распространенный вариант – это подразделение на компьютерные преступления и преступления, совершаемые с помощью или посредством компьютеров, компьютерных сетей и иных устройств доступа к киберпространству. Эту классификацию использует Организация Объединенных Наций, подразделяя этот вид преступной деятельности на киберпреступления в «широком» и «узком» смысле. В данном контексте компьютерные преступления – это преступления, основным объектом посягательства которых является конфиденциальность, целостность, доступность и безопасное функционирование компьютерных данных и систем. Остальные киберпреступления, помимо компьютерных систем, посягают на другие объекты (в качестве основных): безопасность общества и человека (кибертерроризм), имущество и имущественные права (кражи, мошенничества, совершенные посредством компьютерных систем или в киберпространстве), авторские права (плагиат и пиратство).

Конвенция Совета Европы о киберпреступности изначально подразделяла киберпреступления на четыре группы (потом был принят дополнительный протокол, и теперь групп – пять), выделяя в первую группу

«компьютерные преступления», называя их преступлениями против конфиденциальности, целостности и доступности компьютерных данных и систем. К ним относятся, в частности, незаконный доступ, незаконный перехват, вмешательство в данные, вмешательство в систему и т.д.

Во вторую группу входят преступления, связанные с использованием компьютерных средств. К ним относятся подлог с использованием компьютерных технологий, мошенничество в целях неправомерного извлечения экономической выгоды для себя или третьих лиц.

Третью группу составляют преступления, связанные с контентом (содержанием данных). Речь идет о детской порнографии, причем в Конвенции достаточно подробно разъясняется, какие именно действия по распространению детской порнографии должны преследоваться (производство, предложение или предоставление в пользование, распространение или передача, приобретение, владение).

В четвертую группу вошли преступления, связанные с нарушением авторского права и смежных прав. Виды таких преступлений в Конвенции не выделяются: установление таких правонарушений отнесено документом к компетенции национальных законодательств государств.

В начале 2002 г. к Конвенции был принят протокол, добавляющий в перечень преступлений пятую группу - распространение информации расистского и другого характера, подстрекающего к насильственным действиям, ненависти или дискриминации отдельного лица или группы лиц, основывающимся на расовой, национальной, религиозной или этнической принадлежности.

Приведенная в Конвенции классификация, по мнению ряда западных и отечественных исследователей, не является всеобъемлющей: по мере развития научно-технического потенциала и общественных отношений в киберпространстве этот список будет, к сожалению, расширяться. Более того,

преступления, указанные в Конвенции, связаны с некоторыми, но не со всеми действиями, которые создают общественную опасность.

Способы совершения преступлений в сфере информационных технологий:

a. Спаминг - рассылка незапрашиваемых массовых сообщений по электронной почте. В рассылаемое сообщение входит рекламный текст или иное нежелательное содержимое – «нигерийское» письмо о призах в вымышленных лотереях, фишинг-письма для выманивания PIN-кодов, программы-вирусы для «зомбирования» компьютера.

b. Кардинг – жаргонное название преступлений с банковскими картами – в них незаконно используются сами карты или информация о них. Различают «кардинг-он-лайн», включающий применение скомпрометированных карт в Интернет-магазинах, «кардинг-офф-лайн» – использование карт для расчета в традиционных торгово-сервисных предприятиях (ТСП) и «кэшинг» – съем денег в банкомате (АТМ) по скомпрометированным картам

c. Фишинг (англ. *phishing* – производное от *phone* и *fishing*), результатом которого нередко становится доступ преступников к важной конфиденциальной информации владельца платежной карты. Для выведывания используются различныеприемы: отправка электронных сообщений, подделанных под официальные письма, совершение ложных телефонных звонков от имени банка и т. д. Сравнительно новым приемом сбора мошенниками конфиденциальной информации является так называемый вишинг (англ. *vishing – voice phishing*) – голосовой фишинг, реализуемый посредством мобильной телефонной связи.

Широкое общественное информирование о ставших известными способах выведывания мошенниками конфиденциальной информации снизило эффективность фишинговых атак, что привело к изобретению преступниками так называемого фарминга (англ. *pharming* – производное от

phishing и *farming*). Этот вид интернет-мошенничества представляет собой процедуру скрытого перенаправления потенциальных жертв мошенничества на ложные IP-адреса в сети Интернет. Для фарминга может быть использован компьютер владельца платежной карты, на который незаметно для пользователя размещается специальная про-грамма («троян»). Фарминг может быть осуществлен и непосредственно на DNS сервере интернет-провайдера владельца карты. Для получения конфиденциальной информации мошенники делают все возможное, чтобы потенциальная жертва была в полной уверенности, что пользуется услугами банка. После того как владелец карты выполнит стандартную процедуру ввода платежных реквизитов, он перенаправляется на официальный сайт банка.

d. Бот-сети (botnets) – сети в Интернет зомбированных (инфицированных) компьютеров. Зараженный компьютер-бот в дальнейшем используется для рассылки спама, проведения «атак на отказ в обслуживании» (Distributed Denial of Service - DDoS), организации клик-фрода. Необходимая для инфицирования программа-вирус скрытно устанавливается на каждый компьютер бот-сети.

e. Скимминг – вид мошенничества с банковскими картами, который предусматривает использование различных устройств типа – скиммер.

Скиммеры (от англ. *skimming* – снятие сливок) – приборы, монтируемые на банкомат для несанкционирован-ного считывания конфиденциальной информации непосредственно с карты; накладные клавиатуры, размещаемые на клавиатуре банкомата и используемые для копирования вводимых на настоящую клавиатуру данных; миниатюрные видеокамеры, установленные таким образом, что в их объектив попадает информация, которая вводится в банкомат посредством клавишного набора[3].

[3] Антонов И.О., Шалимов А.Н. Способы мошенничества с использованием платежных карт как элемент криминалистической характеристики данного вида преступлений // Ученые записки Казанского университета. Гуманитарные науки. Казань, 2013. Том 155. Книга 4. С. 196-203

Существуют по крайней мере три способа снятия денежных средств с пластиковой карты.

Способ первый. Зачастую мошенники используют устройства, которые, будучи установлены на банкомате, помогают им получить сведения о карточке. Это могут быть установленные на клавиатуры специальные "насадки", которые внешне повторяют оригинальные кнопки. В таком случае владелец карты снимает деньги со счета без всяких проблем, но при этом поддельная клавиатура запоминает все нажатые клавиши - естественно, в том числе и пин-код.

Способ второй. Технически сложно, но можно перехватить данные, которые банкомат отправляет в банк, дабы удостовериться в наличии запрашиваемой суммы денег на счету. Для этого мошенникам надо подключиться к соответствующему кабелю и считать необходимые данные.

Способ третий. Для того чтобы узнать пин-код, некоторые аферисты оставляют неподалеку миниатюрную видеокамеру. Сами же они в это время находятся в ближайшем автомобиле с ноутбуком, на экране которого видны вводимые владельцем карты цифры.

Новейшие технологии, взятые на вооружение преступниками, позволили им модернизировать устройства, используемые для скимминга. Речь идет о шимминге (англ. *shimming*) – использовании гибких, очень тонких плат, внедряемых преступниками в банкомат через щель приемника пластиковых карт. Плата при помощи специальной карты носителя присоединяется к контактам, считывающим данные с платежных карт. Толщина платы сопоставима с толщиной человеческого волоса (0.1 мм). Принципиальным отличием технологии шимминга от использования скимерских устройств является ее большая визуальная незаметность.

Специалисты из правоохранительных органов многих стран мира считают, что преступления, совершенные с использованием пластиковых платежных средств, можно отнести к одним из наиболее опасных

экономических преступлений. Причем совершаются они не только в компьютерной банковской системе, но и через Интернет.

По некоторым данным, на сегодняшний день насчитывается около 30 видов незаконных операций с карточками через Всемирную паутину. Наиболее распространенные из них - оплата несуществующими картами, создание фальшивых виртуальных магазинов, электронное воровство, фальшивая оплата в игорных заведениях.

Кардинг - это незаконное использование банковских карточек для покупки товаров или услуг через Интернет. Занимаясь кардингом, можно либо получить информацию о реальной карте, либо сгенерировать все эти данные. Интересующиеся могут свободно найти ссылки на сайты, которые открыто торгуют сведениями о банковских картах.

По данным Национального агентства финансовых исследований, в 2015 г. в среднем у каждого пользователя банковской карты имеется 2,3 карты, при этом 85% держателей карт имеют зарплатную карту, 71% - дебетовую карту, 65% - кредитную карту[4]. Согласно данным правоохранительных органов РФ, среди преступлений с использованием высоких технологий наибольшие темпы роста имеют показатели количества противоправных деяний с использованием платежных карт[5].

Неизбежным следствием расширения сферы применения банковских карт выступают новые виды преступных посягательств на собственность, что предполагает необходимость изменения уголовного законодательства. Федеральным законом от 29 ноября 2012 г. N 207-ФЗ в УК РФ введена ст. 159.3, предусматривающая ответственность за мошенничество с

[4] Безопасность банковских карт: взгляд потребителя и активность игроков рынка. Отчет по результатам исследования. М.: Национального агентства финансовых исследований, 2016. [Электронный ресурс] URL: http://nacfin.ru/wp-content/uploads/2015/01/moshennichestvo_bankovskie_karty.pdf. Проверено на 30.10.2016.

[5] Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 ноября. URL: http://www.rg.ru/2012/11/29/karti-site.html, свободный.

использованием платежных карт, что обусловлено стремлением законодателя решить проблему квалификации хищения с использованием карт.

Пластиковая карта — обобщающий термин, который обозначает все виды карточек, различающихся по назначению, по набору оказываемых с их помощью услуг, по своим техническим возможностям и организациям, их выпускающим. Важнейшая особенность всех пластиковых карт, независимо от степени их совершенства, состоит в том, что на них хранится определенный набор информации, используемый в различных прикладных программах.

При осуществлении платежей при помощи электронного средства платежа нет необходимости в заведении отдельного банковского счета. Перемещение электронных денежных средств происходит не по банковским информационным системам, а по специально предназначенным для этой карты сетям, где они хранятся на консолидированном счете. Электронные денежные средства представляют собой определенную информацию, которая была конвертирована в эквивалент, выраженный в стоимостной или натуральной единице (деньги, минуты, количество поездок, литры и т.д.). В зависимости от территории действия различают карты локального характера, использование которых возможно в офисах, банкоматах банка эмитента, как правило, в пределах одной страны (Оперативная российская платежная система Сберкарт), и международного характера, используемые в качестве универсального средства платежа на территории стран-участников, где принимаются данные карты (Visa, Master Card, Diners Club, American Express, JCB и China Unionpay).

Каждая карта подлежит процедуре персонализации, в соответствии с которой ей присваивается определенный номер, имя держателя, срок действия. При этом все необходимые данные, связанные с информацией о держателе карты, наносятся на магнитную полосу и (или) в память микропроцессора карты, при наличии чипа. При совершении каких-либо

операций с картой денежные средства могут поступать как с одного счета, к которому привязана карта (кредитная или расчетная), так и с нескольких счетов клиента, к которым эта карта также привязана. Для удобства клиента допускается также использование нескольких карт по одному счету, например, для членов семьи. Для юридических лиц и индивидуальных предпринимателей предусматриваются определенные ограничения на снятие наличных денежных средств в течение одного операционного дня. Для физических лиц банки и иные кредитные организации устанавливают собственные денежные лимиты.

Организованные преступные группы кардеров нередко совершают несколько эпизодов мошенничества. Так, в городе Ухта были задержаны участники преступной группы, состоящей из трех человек, занимавшихся мошенничеством с использованием поддельных платежных карт (23 эпизода хищений). Члены организованной преступной группы по фальшивой банковской карте приобрели на одной АЗС 900 л бензина на 22140 руб., а на другой – 3658 л дизельного топлива на 100960 руб. Эмитентами пластиковых карт, которые были задействованы при совершении преступления, являлись банки США, Испании, Франции и Швейцарии. Для совершения мошенничества преступники использовали специальное оборудование по изготовлению поддельных пластиковых карт[6]

Специалисты отмечают, что, как и другие киберспреступления, преступления с использованием платежных карт нередко совершаются членами разветвленных, хорошо организованных преступных групп, участники которых имеют свою преступную специализацию[7]. Криминальная специализация в группе может выглядеть следующим образом: одни члены группы осуществляют сбор информации по платежным картам, другие – обрабатывают собранную информацию и передают их тем, кто занимается

[6] Попова Н. Российские банкоматы оказались в ливанской петле // АН-online. – 2012. – 11 фев. – URL: http://argumenti.ru/crime/2012/02/156477, свободный.

[7] Козловский В. Масштабы кибермошенничества растут // Российская газета. 2012. 29 нояб. URL: http://www.rg.ru/2012/11/29/karti-site.html, свободный

изготовлением поддельных карт. Подготовленное таким образом хищение осуществляют лица, специализирующиеся на «вещевом» кардинге – именно они используют платежную карту для обмана работников торговой организации.

Еще одним основанием для классификации способов мошенничества с использованием платежных карт является технологическое решение, задействованное преступниками при совершении преступления. В статье 159.3 УК РФ указано два способа совершения такого мошенничества: с использованием поддельной (1) или принадлежащей другому лицу (2) платежной карты (УК РФ). Примером последнего является дело, в ходе расследования которого было установлено, что К., совершив тайное хищение имущества, завладел платежной картой потерпевшего и решил использовать ее для осуществления мошенничества. С целью реализации своего умысла К. неоднократно использовал похищенную платежную карту для приобретения различных товаров[8].

Сегодня до 80 % обращений через интернет-сайт МВД РФ посвящены мошенничеству при покупке товаров через социальные сети и интернет-магазины. Также продолжает расти разнообразие вредоносных программ для мобильных устройств.

Целью злоумышленников может быть получение доступа к мобильному банку жертвы и к конфиденциальным сведениям.

В 2014 г. зафиксировало увеличение числа программ, используемых для реализации мошеннических схем. Они имеют широкий функционал – от получения данных банковских карт до снятия наличных денег и несанкционированного проникновения во внутреннюю сеть банка. Не теряет популярность и «классический» скимминг. Обобщенные данные в области разработки безопасных приложений и оценки уязвимостей показывают следующую статистику:

[8] Приговор Верхнепышминского городского от 7 июня 2011 г. по уголовному делу № 1-152/11 http://docs.pravo.ru/document/view/18392970/.

1. В 2015 году злоумышленник оказался способен получить доступ к узлам внутренней сети субъекта национальной платежной системы в 9 случаях из 10, а в 2012 году аналогичное соотношение составляло 7 из 10;

2. Для проведения атаки в 82 % случаев достаточно иметь среднюю или низкую квалификацию;

3. Факторы уязвимости web-приложений обнаружены в 93 % исследованных систем;

4. Причинами возникновения уязвимостей в АБС являются ошибки (недостатки) разработки (23 %) и отсутствие эффективных защитных механизмов (43 %);

5. Уязвимости приложений – один из распространенных факторов, способствующих проникновению в корпоративные сети[9].

Рассмотрим основные приемы мошеннических действий, следующие из российской специфики. Самый распространенный способ – халатность и правовой нигилизм клиентов, которые разглашают PIN-код путем его записи на карту или путем так называемого «дружественного мошенничества» – разглашения PIN-кода членам семьи, близким друзьям, коллегам.

Еще пример – когда из-за фактора технической неграмотности клиенты впадают в панику при получении SMS-сообщения «Ваша банковская карта заблокирована» со всеми вытекающими для них последствиями.

Всего же разделяют 9 основных видов киберпреступлений.

1. Операции с поддельными картами.
2. Снятие денежных средств с помощью средств электронного банкинга.
3. Операции с украденными/утерянными картами.
4. Многократная оплата услуг и товаров.
5. Мошенничество с интернет заказами и магазинами.
6. Многократное снятие со счета.
7. Мошенничество с использованием подложных слипов.

[9] Выборнов А. Устранение уязвимостей // BIS journal. 2014. № 4.

8. Мошенническое использование банкоматов при выдаче наличных денег.

9. Подключение электронного записывающего устройства к POS-терминалу/банкомату (Skimming).

10. Другие виды мошенничества.

1.3. Криминологическая характеристика компьютерных преступлений

Обстановка совершения преступлений в сфере компьютерной информации характеризуется рядом существенных факторов. Для нее характерно несовпадение между местом совершения противоправных действий и местом наступления общественно опасных последствий. Рассматриваемые преступления совершаются, как правило, в специфически интеллектуальной области профессиональной деятельности и с использованием специализированного оборудования. Все эти преступления обычно совершаются в условиях различных нарушений установленного порядка работы с компьютером, о которых лицам становится известно в ходе их соответствующей профессиональной подготовки. Для правонарушителей в данной области обычно достаточно ясен механизм возможных нарушений правил пользования информационными ресурсами и связь с событиями, повлекшими наступление криминального результата.

Следовательно, относительно **объекта преступного посягательства** двух мнений быть не может — им, естественно, является информация, а **действия преступника** следует рассматривать как **покушение на информационные отношения общества.**

Субъекты данных преступлений нередко владеют специальными навыками не только в области управления компьютера и устройствами, но и специальными знаниями в области обработки информации в информационных системах в целом. При этом для корыстных преступлений, связанных с использованием информационных систем, характерны и специальные познания в соответствующих финансовых и иных

информационных технологиях. Для нарушений правил эксплуатации компьютера и действий с ВЦ характерны специальные познания в узкой предметной профессиональной области устройств компьютера и программного обеспечения.

Лица, совершающие компьютерные преступления, могут быть объединены в три большие группы:

а) лица, не связанные трудовыми отношениями с организацией-жертвой, но имеющие некоторые связи с нею;

б) сотрудники организации, занимающие ответственные посты;

в) сотрудники — пользователи ПК, злоупотребляющие своим положением.

Кроме того, субъекты компьютерных преступлений могут различаться как по уровню их профессиональной подготовки, так и по социальному положению.

Что касается источников киберпреступлений, то специалисты подразделяют лиц и организации, осуществляющие атаки, на несколько категорий. Однако, между этими категориями не существует достаточно четких границ. Таким образом, деление на группы можно считать в каком-то смысле условным[10][11].

1. Хакеры — лица, рассматривающие защиту компьютерных систем как личный вызов и взламывающие их для получения полного доступа к системе и удовлетворения собственных амбиций.

Лица, имеющие высокий уровень знаний в области компьютерных технологий, и проводящие много времени за компьютером в поисках уязвимостей компьютерных систем. Существуют мифы о «белых хакерах» и «черных хакерах». «Белые» занимаются поиском брешей в программном обеспечении для последующего их исправления, «черные»

[10] Яблоков Н. П. Криминалистика: Учебник. — М.: ЛексЭст, 2006.

[11] Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Электронный ресурс. Режим доступа: http://www.crime.vl.ru/index.php?p=3626&more=1&c=1&tb=1&pb=1

несанкционированно проникают в компьютерные системы с целью причинения ущерба данным, кражи информации, или нанесения иного вреда.

Некоторые хакеры не только получают доступ к информации или программному обеспечению, но и перепродают ставшие им доступными сведения. В ноябре 1998 года, по сообщениям прессы, член пакистанской военной группировки Харкат-уль-Ансар пытался приобрести военное программное обеспечение, украденное хакерами с компьютеров Министерства обороны США .

2. Хактивисты. Термин «хактивизм» введен впервые специалистом по компьютерной преступность Д.Деннинг. Он возник из соединения двух слов «hack» и «activism» и используется для обозначения явления социального протеста, которое представляет собой своеобразный синтез социальной активности, преследующей цель протеста против чего-либо, и хакерства (использования Интернет-технологий с целью причинения ущерба компьютерным сетям и их пользователям).

3. Киберпреступники, «корыстные преступники» — лица, вторгающиеся в информационные системы для получения личных имущественных или неимущественных выгод.

С тех пор, как корыстная преступность открыла для себя сеть Интернет, кибервымогательство стало одним из основных способов эксплуатации компьютерных сетей для незаконного извлечения прибыли.

4. Лица, занимающиеся шпионажем, «шпионы» — лица, взламывающие компьютеры для получения информации, которую можно использовать в политических, военных и экономических целях.

5. Террористы— лица, взламывающие информационные системы для создания эффекта опасности, который можно использовать в целях политического воздействия.

6. Вандалы — лица, взламывающие информационные системы для их разрушения.

7. Психически больные лица, страдающие новым видом психических заболеваний — информационными болезнями или компьютерными фобиями.

Профили киберпреступников:

a. Кодеры - квалифицированные программисты, изготавливающие преступные инструменты - программы-вирусы, пользовательские боты, программы для рассылки спама и др. Часто кодеры предлагают сами преступные услуги. Поставляя программы, кодер минимизирует риск быть наказанным.

b. Дропы - играют важную роль в киберпреступлениях, именно они превращают похищенные логины и PIN-коды в реальные деньги. Работа дропа наиболее опасна - дроп снимает деньги в банкомате и затем передает их заказчику.

c. Подростковая преступность. Киберпреступность, увы, молодая, и ее основанная рабочая сила - подростки в возрасте 15+. Именно они посещают многочисленные чаты, посвященных кардингу и другим подобным темам. Большинство подростков пытаются создавать самодельные почтовые программы-мейлеры, создают фишинг-страницы и др. Заработки подростков невелики, однако из них вырастают взрослые кардеры.

На многочисленных форумах и сайтах в Интернет злоумышленники готовят преступления, сбывают краденное, обмениваются опытом. Форумы обеспечивают обучение молодых кардеров, на них можно найти инструментарий для взлома, предложения услуг по проведению атак DDOS и др.

d. Провайдеры, обслуживающие мошенников – в Интернете организованы AntiAbuseHosting сети («абузоустойчивые» хостинги - на сленге), позволяющие размещать любые противоправные сайты и при этом защищать владельцев этих сайтов от действий правоохранительных органов. В целях «шифровки» своих клиентов недобросовестные провайдеры

используют промежуточные прокси-серверы и VPN-серверы – это позволяет удлинить цепочку, ведущую к преступникам.

1.4. Глобальная картина киберпреступности

Во многих странах резкий всплеск в количестве подключений к глобальной сети совпал по времени с экономическими и демографическими преобразованиями, ростом разрыва в доходах, сокращением расходов в частном секторе и снижением финансовой ликвидности. На общемировом уровне правоохранительные органы в своих ответах на вопросник отмечают рост уровня киберпреступности в связи с тем, что и частные лица, и организованные преступные группы используют новые возможности для совершения преступлений, руководствуясь стремлением к извлечению прибыли и получению личной выгоды. По оценкам, свыше 80% киберпреступлений совершаются в той или иной форме организованной деятельности. Для совершения киберпреступлений более не требуется обладание сложными навыками или знание сложных методов. Преимущественно в развивающихся странах возникли субкультуры молодых людей, занимающихся финансовым мошенничеством при помощи компьютеров, многие из которых вовлечены в киберпреступления, начиная с позднего подросткового возраста.

В глобальном плане наблюдается широкий диапазон киберпреступлений, которые включают преступления, совершаемые в целях получения финансовой выгоды, преступления, связанные с использованием содержащейся в компьютере информации, а также преступления, направленные против конфиденциальности, целостности и доступности компьютерных систем. Однако государственные органы и предприятия частного сектора по-разному воспринимают относительный риск и угрозу.

Более надежную основу для сравнения представляют собой обследования виктимизации. Они свидетельствуют о том, что виктимизация

частных лиц в результате киберпреступности значительно выше, чем в случае «обычных» форм преступности. Показатели виктимизации от мошенничества с кредитными картами в режиме онлайн, кражи персональных данных, ответов на попытку фишинга и несанкционированного доступа к учетным записям электронной почты составляют от 1 до 17% среди пользователей Интернета в 21 стране мира, в отличие от типичных показателей в отношении краж со взломом, грабежа и краж автомобилей, составляющих для этих же стран менее 5 процентов. Показатели виктимизации, связанной с киберпреступностью, выше в странах с низким уровнем развития, что подчеркивает необходимость укрепления профилактической работы в этих странах.

Основные тенденции в сфере киберпреступлений (по оценке полиции Евросоюза по состоянию на 2016 год):

1. Преступление в качестве услуги: «подпольные цифровые услуги» подкрепляются моделью «преступление в качестве услуги», которая становится все более популярной и востребованной. Она объединяет между собой специализированных поставщиков хакерских утилит и организованные преступные группировки.

2. Программы-вымогатели: вымогательство и банковские «трояны» остаются главными угрозами среди вредоносного программного обеспечения. И эта тенденция вряд ли изменится в обозримом будущем.

3. Преступное использование данных: данные остаются ключевым товаром для киберпреступников. Во многих случаях они используются для получения немедленной финансовой выгоды, но все чаще применяются для реализации более сложных схем мошенничества, зашифровываются с целью получения выкупа, либо используется непосредственно для вымогательства.

4. Платежное мошенничество: EMV (чип и PIN-код), гео-блокировка и другие промышленные меры безопасности продолжают помогать в эффективной борьбе с карточным мошенничеством, но, тем не

менее, растет и число атак, направленных против банкоматов. Организованные преступные группы начинают компрометировать платежи, связанные с использованием бесконтактных карт (NFC).

5. Он-лайн сексуальное насилие над детьми: использование платформ со сквозным шифрованием для обмена медиа файлами, а также применение анонимных платежных систем способствует эскалации он-лайн трансляции жестокого обращения с детьми.

6. Социальная инженерия: правоохранительными органами был зарегистрирован рост числа фишинг-атак, направленных на цели, имеющие высокую значимость. Главной угрозой стали атаки против генеральных директоров предприятий и организаций.

7. Виртуальные валюты: Bitcoin остается той валютой, которую мошенники предпочитают для оплаты за приобретение незаконных товаров и услуг в «темной сети. Bitcoin также стал стандартным платежным решением при требовании выкупа и других форм вымогательства.

Глава 2. Особенности возбуждения уголовных дел, тактика производства отдельных следственных действий по уголовным делам о преступлениях, совершенных в сфере высоких технологий и компьютерной информации.

2.1. Возбуждение уголовных дел и планирование расследования преступлений в сфере высоких технологий. Типичные следственные ситуации и версии

На стадии возбуждения уголовных дел о преступлениях в сфере высоких технологий типично складываются следующие ситуации:

1. Правообладатель или собственник информационной системы выявил нарушения конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник информации самостоятельно выявил указанные нарушения в системе, однако не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Признаки преступления выявлены в результате оперативно-розыскной деятельности.

Типичными поводами для возбуждения уголовных дел по преступлениям в сфере компьютерной информации чаще всего служат:

1) заявление о преступлении, поступившее от потерпевшего (физического лица или представителя юридического лица);

2) непосредственное обнаружение органом дознания признаков преступления:

- в результате проверки сообщения о совершенном или готовящемся преступлении, поступившего из оперативных источников;

- в ходе проведения специальных оперативно-технических мероприятий;

- по результатам анализа материалов контрольно-ревизионных и иных документальных проверок;

- при задержании лица (лиц) на месте совершения преступления с поличным;

3) непосредственное обнаружение признаков преступления следователем при расследовании других преступлений;

4) сообщения в средствах массовой информации (статьи, заметки, письма, в том числе опубликованные в сети Интернет).

На основе анализа уголовных дел, связанных с неправомерным (несанкционированным) доступом к компьютерной информации, можно предложить некоторую обобщенную схему расследования подобных преступлений.

В ходе расследования основные следственные задачи целесообразно решать в такой последовательности:

1. Установление факта неправомерного доступа к информации в компьютерной системе или сети.

2. Установление места несанкционированного проникновения в компьютерную систему или сеть.

3. Установление времени совершения преступления.

4. Установление способа несанкционированного доступа.

5. Установление лиц, совершивших неправомерный доступ, их виновности и мотивов преступления.

6. Установление вредных последствий преступления.

7. Выявление обстоятельств, способствовавших преступлению, и в том числе установление надежности средств защиты компьютерной информации.

При расследовании компьютерных преступлений, связанных с созданием, использованием и распространением вредоносных программ для ПК, целесообразно применять следующую последовательность действий:

1. Установление факта использования и распространения вредоносной программы.

2. Установление факта и способа создания вредоносной программы.

3. Установление лиц, виновных в создании, использовании и распространении вредоносных программ.

4. Установление вреда, причиненного данным преступлением.

5. Установление обстоятельств, способствовавших совершению расследуемого преступления.

К типичным признакам подготовки, совершения и сокрытия преступления в сфере компьютерной информации относятся:

- появление в системе ПК или их сети ложных данных (письма электронной почты от неизвестных и известных адресатов с прикрепленными файлами, не соответствующими описанию и т.п.);

- несанкционированные изменения, программного обеспечения и конфигурации ПК, системы ПК или их сети;

- частые сбои в работе аппаратуры;

- жалобы клиентов на предоставление некачественного доступа к ПК, системе ПК, их сети или компьютерной информации;

- нерегламентированный доступ к ПК, системе ПК, 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 компьютерной информации определенной категории;

- применение на рабочем месте и вынос с работы личных носителей информации под различными предлогами;

- случаи утечки конфиденциальной информации либо обнаружение негласных устройств ее получения; нарушение установленных правил оформления документов при работе с ПК, системой ПК, их сетью или компьютерной информацией;

- создание копий определенной категории данных и компьютерной информации, не предусмотренных технологическим процессом;

- несоответствие данных, содержащихся в первичных (исходных) документах, иным более поздним по времени создания документам;

- подозрительно частое обращение одного и того же пользователя к данным и компьютерной информации определенной категории.

- появление в компьютере недостоверных данных;

- не обновление в течение длительного времени в автоматизированной информационной системе кодов, паролей и других защитных средств;

- С учетом комплекса исходной информации, полученной при проведении проверочных действий, на первоначальном этапе расследования могут складываться следующие типичные следственные ситуации:

1. Установлен неправомерный доступ к компьютерной информации, есть следы, есть подозреваемый, который дает правдивые показания.

2. Установлен неправомерный доступ к компьютерной информации, имеются следы, прямо указывающие на конкретного подозреваемого, но он отрицает свою причастность к совершению преступления.

3. Установлен неправомерный доступ к компьютерной информации, известны лица, совершившие преступление, но обстоятельства доступа не установлены.

4. Установлен факт неправомерного доступа к компьютерной информации, совершить который и воспользоваться его результатами могли только лица из определенного круга (по своему положению, профессиональным навыкам и знаниям), либо известны лица (фирмы, организации), заинтересованные в получении данной информации.

Последняя из приведенных следственных ситуаций является наиболее сложной, так как отсутствуют сведения о виновном лице, следы преступления, неизвестен способ совершения преступления и др.

На основании вышеуказанных типичных следственных ситуаций на первоначальном этапе расследования преступлений рассматриваемого вида

можно выделить следующие общие версии:

1. Состав преступления отсутствует, поскольку происшедшее событие является следствием непреодолимых факторов (самопроизвольный сбой в работе программных или аппаратных составляющих средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, сетей электропитания и связи, средств защиты информации; выход из строя машинного носителя информации по причине естественного износа и старения; саморазрушение отдельных электронных компонентов компьютерных устройств и др.).

2. Совершено неумышленное преступление по причине халатности лица, ответственного за соблюдение режима конфиденциальности соответствующей компьютерной информации.

3. Преступление совершено с целью наживы лицом, имеющим доступ к конфиденциальной информации в силу исполнения им своих служебных обязанностей, – сотрудником потерпевшего.

4. Преступление совершено лицом, знакомым с условиями обработки и защиты конкретной конфиденциальной компьютерной информации потерпевшим.

5. Преступление совершено дистанционно с использованием специальных технических средств, предназначенных (приспособленных, разработанных, запрограммированных) для негласного получения конфиденциальной информации.

При выдвижении версий совершения преступлений в сфере компьютерной информации необходимо учитывать, что они совершаются обычно группой из двух и более человек, хотя не исключена возможность работы преступника – одиночки.

В случае возбуждения уголовного дела по фактам совершения преступлений в сфере компьютерной информации, исходя из содержания

уже имеющихся в материалах доследственной проверки документов, осуществляется планирование расследования на первоначальном этапе. План должен содержать ответы на следующие вопросы:

1. С производства каких следственных действий надо начать расследование, чтобы не утратить источники доказательственной информации?

2. Когда по тактическим соображениям целесообразнее всего осуществить задержание известного преступника?

3. Как обеспечить тактическую перспективу дела, в частности установить всех лиц, совершивших преступление, раскрыть их связи, выяснить причины и условия, способствовавшие совершению преступного посягательства?

4. Кто из свидетелей должен быть допрошен первым?

5. Кто из подозреваемых в совершении преступлений должен быть допрошен в первую очередь (по групповым делам), в какой последовательности это целесообразно сделать, чтобы обеспечить полноту и всесторонность расследования, исключить возможность влияния подозреваемых на соучастников, потерпевших и свидетелей?

6. У кого (где) и в какой тактической последовательности должны быть проведены обыски и выемки, когда (в какое время) и что следует искать (изымать) при их производстве, с участием каких специалистов и применением каких научно-технических методов и средств, чтобы обеспечить выявление и процессуально грамотное получение всех возможных доказательств?

7. Что необходимо предпринять для установления материального ущерба и обеспечения гражданского иска?

8. Каковы формы взаимодействия следователя с оперативным сотрудником, особенности их взаимодействия со специалистами (экспертами) и по каким вопросам (направлениям)?

9. Каковы приемы и допустимость использования в уголовном деле материалов, полученных в результате осуществления оперативно-розыскной деятельности?[12]

2.2. Тактика производства отдельных следственных действий по уголовным делам о преступлениях, совершенных в сфере высоких технологий и компьютерной информации.

1. Осмотр места происшествия.

Осмотр - самостоятельное следственное действие, заключающееся в обследовании следователем или иным полномочным лицом объектов, виды которых названы в законе, в установленном уголовно-процессуальным законом порядке для достижения определенных целей и специфических задач.

Под местом происшествия по делам о преступлениях в сфере компьютерной информации следует понимать не только территорию или помещение, где осуществлялось противоправное действие (бездействие) либо наступили вредные последствия содеянного, но и место, где обнаружены связанные с ним обстоятельства (вредные последствия).

Местом происшествия может быть, как одно помещение, где установлен компьютер и хранится информация, так и ряд помещений, в т.ч. в разных зданиях, соединенных компьютерной сетью или находящихся на различных территориях, связанных сетью Интернет. Очевидно, что в последнем случае осмотр каждого из указанных мест должен оформляться самостоятельным протоколом осмотра места происшествия.

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 СКТ и (или) компьютерная информация, обладающая

[12] Лузгин И.И. Технико-криминалистическое обеспечение как мегаинструментальная технология формирования единого криминалистического пространства // Эксперт-криминалист. 2010. N 1. С. 30 - 34.

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.

К участию в производстве осмотра места происшествия (ОМП) рекомендуется привлекать:

- специалиста по профилю сетевого средства вычислительной техники (ССВТ), которое нужно будет осмотреть в ходе следственного действия;

- специалиста, обладающего минимально необходимыми знаниями по тем операциям технологического процесса, при проведении которых были обнаружены признаки преступления;

- представителя администрации предприятия, учреждения или организации, на территории (в помещении) которых производится осмотр;

- лицо, несущее материальную ответственность за компьютерную информацию, подвергшуюся преступному воздействию, электронный носитель информации и СКТ;

- инспектора или ревизора, проводившего инвентаризацию, ревизию, аудиторскую или иную документальную проверку, вскрывшую признаки правонарушения.

Кроме того, необходимо отметить, что в качестве понятых рекомендуется привлекать лиц, обладающих необходимыми специальными знаниями в области обработки компьютерной информации (на уровне бытовых пользователей компьютерной техники).

На месте происшествия по делам о преступлениях в сфере компьютерной информации рекомендуется принимать следующие меры по сохранности обстановки и фиксации значимых обстоятельств:

1. Правильное количественное определение объектов осмотра компьютерных средств в качестве вещественных доказательств.

2. Использование специально разработанного компьютерного

оборудования и пакета служебного программного обеспечения.

3. Отражение в процессе осмотра не только количества выявленных компьютерных средств, но и описание их технических характеристик и состояния работоспособности.

4. Подробное описание графического интерфейса загруженной операционной системы данного компьютера с перечислением ярлыков установленных программ, что затруднит возможность их сокрытия или подмены после осмотра.

5. Закрепление виртуальных следов: более подробное описание файловой системы, прикладных программ, физических носителей информационных следов как электронных, так и бумажных с указанием места их обнаружения. Описание использованных при этом специальных программно-технических средств.

6. Фиксация последовательности проведения поисковых действий. Такое закрепление способствует более полному проведению следственного действия - «проверка показаний на месте»» (ст. 194 УПК РФ).

Особенно тщательно должны быть осмотрены и описаны в протоколе типичные вещественные доказательства: вредоносные программное обеспечение и носители на которых оно храниться; программы обеспечение, заведомо приводящие к несанкционированным пользователем действиям (влияющие на конечные результаты технологического процесса), а также их носители; обнаруженные специальные технические средства негласного получения (уничтожения, блокирования) компьютерной информации и носителей; специфические следы преступника и преступления.

Для осмотра информации можно применить специальное компьютерное оборудование и программное обеспечение, имеющееся в распоряжении следственной группы, но исследовать информацию в компьютерах на месте происшествия с помощью программного обеспечения, установленного на самих осматриваемых компьютерах, крайне нежелательно

из-за опасности исказить или повредить данные. В современных компьютерах такой «осмотр» неизбежно сопровождается изменением информации на компьютерных носителях по сравнению с исходной[13].

При осмотре работающего ПК:

- расположение рабочих механизмов ПК и изображение на его экране (мониторе) или визуально-контрольном окне (для принтеров, контрольно-кассовых машин, контрольно-пропускных механизмов, цифровых аппаратов связи и т.д.);

- все действия, производимые специалистом при осмотре ПК (порядок нажатия на клавиши и запорные механизмы, корректного приостановления работы и закрытия исполняемой операции или программы, выключения ПК, отключения от источника электропитания, рассоединения или соединения ПК и его составляющих, отсоединения коммуникационных и электропитающих проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т.п.).

- установить, какая программа выполняется (для чего осмотреть изображение на экране дисплея и детально описать его, по возможности произвести фотографирование или видеозапись), тип программного обеспечения, загруженного в момент осмотра в компьютер, может свидетельствовать о задачах, для которых использовался данный компьютер;

- по мере необходимости и возможности остановить исполнение программы и установить, какая информация получена после окончания ее работы;

- установить наличие в компьютере накопителей информации (жесткие диски, дисководы для дискет, стримеры, оптические диски, флэш-карты и т. п.), их тип (вид) и количество;

---

[13] Пропастин С.В. Следственный осмотр: проблема определения целей и задач // Современное право. 2012. N 5. С. 133-135.

- при наличии технической возможности скопировать информацию, которая может иметь значение для дела (программы, файлы данных), и имеющуюся в компьютере (особенно это важно для информации, находящейся в оперативном запоминающем устройстве, поскольку после выключения компьютера она может быть уничтожена).

Целесообразно исследовать компьютер на наличие удаленных файлов. Некоторые операционные системы при недостаточности объема оперативной памяти создают так называемый «файл подкачки» (файл с расширением «swp») для хранения всей удаленной информации, которая при наличии специальной программы может быть восстановлена.

Рекомендуется также изучать не только подлинники изъятых машинных носителей, но и их копии, изготовленные средствами данной операционной системы. Следует обращать внимание и на поиск так называемых «скрытых» файлов (как правило, системных защищенных от записи файлов).

Отметим, что, во избежание уничтожения (повреждения) ПК и характерных следов преступления, при работе специалиста по осмотру ПК недопустимо использование магнитосодержащих материалов, инструментов, приборов и оборудования, направленных источников электромагнитного излучения.

Следователям не рекомендуется самостоятельно, без участия специалиста, выключать работающий в момент осмотра компьютер, поскольку это может создать сложности при повторном входе в систему, особенно защищенную.

Осмотр машинного носителя начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием.

В процессе осмотра места происшествия (или машинного носителя информации) необходимо указать в протоколе:

- место обнаружения носителя информации;

- наличие, индивидуальные признаки и техническое состояние футляра (коробки, упаковки, специального технического устройства);

- тип, вид, марку, назначение, цвет и заводской номер;

- техническое состояние - размеры носителя, внешний вид, материал каркаса носителя, его целостность и индивидуальные признаки, материал основного информационно-несущего слоя и его целостность;

- работоспособность и внутреннюю спецификацию - серийный номер и (или) метка тома, либо код; размер разметки, размер области носителя, свободной от записи и занятой под информацию; количество и номера сбойных зон, секторов, участков, кластеров; 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);

- результат осмотра содержимого файлов (программ, компьютерной информации);

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

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). 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.

Недопустимо приклеивать что-либо непосредственно на магнитный

носитель информации и документам, пропускать через них бечеву, пробивать степлером, делать пометки или маркировки, накалывать твердым предметом знаки, использовать пластилиновые или сургучовые печати и т. д.

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 не изъятые ПК и помещение, в котором они находятся).

Стоит обратить особое внимание на то, что перед началом производства любых следственных действий, непосредственно связанных с ПК, 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.

2. Тактика проведения допроса

Особенности тактики допроса участников уголовного дела о преступлении в сфере компьютерной информации зависят от процессуального статуса допрашиваемого лица и ситуации производства следственного действия. Принимая решение о допросе конкретного лица в качестве свидетеля, следователь должен заранее прогнозировать, какую информацию (прежде всего технического характера) он может получить от допрашиваемого. Ориентируясь на это, необходимо заранее продумывать комплекс постановочных вопросов.

В процессе допроса свидетелей всякий раз необходимо выяснить:

- не было ли сбоев в работе программ, хищений носителей информации и отдельных компьютерных устройств;

- зафиксированы ли сбои в работе компьютерного оборудования, электронных сетей, средств зашиты компьютерной информации;

- зафиксированы ли в последнее время случаи срабатывания средств защиты компьютерной информации (антивирусные программы);

- как часто проверяются программы на наличие вирусов, каковы результаты последних проверок;

- как часто обновляется программное обеспечение, каким путем оно приобретается;

- каким путем приобретается компьютерная техника, как осуществляется ее ремонт и модернизация;

- как осуществляется защита компьютерной информации, каковы применяемые средства и методы защиты и др.

При расследовании неправомерного доступа к компьютерной информации на первоначальном этапе возникает необходимость допрашивать в качестве свидетелей граждан различных категорий, для каждой из которых существует своя специфика.

В процессе допроса системных администраторов и специалистов по информационной безопасности выясняется:

- перечень используемого программного обеспечения и его классификация (лицензионное, собственное);

- пароли защиты программ, отдельных устройств компьютера, частота их смен;

- технические характеристики компьютерной сети (при ее наличии), кто является администратором сети;

- порядок приобретения и сопровождения программного обеспечения;

- существование идентификационных программ, наличие в рабочих программах специальных файлов протоколов, регистрирующих вхождение в

компьютер пользователей, каково их содержание и др.

3. Тактика проведения обыска

Обыск по своим информационно-познавательным целям весьма близок к следственному осмотру.

Обыск по делам, связанным с НСД, в необходимых случаях производится на квартире подозреваемого, месте его работы, а также в других местах, где он имел доступ к компьютерной технике.

Целями проведения обыска при расследовании преступлений в сфере компьютерной информации являются обнаружение и изъятие (в случае возможности его осуществления) материальных объектов. способных по сбоим физико-техническим свойствам содержать информацию. имеющую отношение к расследуемому преступлению. К таким объектам могут быть отнесены:

1. компьютерная техника или устройства (смартфоны, планшеты и т.д.);
2. электронные носители информации;
4. вспомогательные системы, обеспечивающие нормальное функционирование автоматизированных информационных систем (линии электропитания, заземления и т.д.);
5. зафиксированные на бумаге алгоритмы, иди иные записи преступников;
6. справочная техническая литература, руководства по эксплуатации, технические журналы, блокноты и иные документы.

Существенной особенностью обыска при расследовании преступлении в сфере компьютерной информации является то, что следователь, проводящий данное следственное действие, как правило. не может оценить на месте значение обнаруживаемой информации. так как. во-первых, он сталкивается с огромными ее объемами и, во-вторых, она представлена в специальном виде, для восприятия которого необходимы определенные

специальные знания, иногда специальные аппаратные и программные средства.

В связи с этим, наиболее целесообразным действием следователя при проведении обыска является изъятие всех обнаруженных электронных носителей информации, или по возможности копирование такой информации.

В практике расследования встречаются случаи использования обыскиваемым лицом специальной техники, обеспечивающей практически мгновенное гарантированное невосстановимое уничтожение информации с любого носителя, выполняемые как в стационарной комплектации, так и в мобильной.

Для устранения препятствий подобного рода необходимо использовать комплекс организационно-тактических мероприятий, включающий:

1. четкое планирование действий членов СОГ;
2. блокирование активных действий ответственных операторов;
3. изъятие у операторов средств управления комплексами;
4. отключение линий связи (телефония, интернет);
5. использование блокираторов радиосвязи в различных диапазонах.
6. предотвращение отключения энергоснабжения, обеспечение охраны распределительного щита;
7. запрет производить какие-либо манипуляции с компьютерами и носителями информации;
8. обеспечение отключения беспроводных систем передачи данных

При наличии в осматриваемом помещении локальной сети необходимо точно установить местоположение серверов. Определить местоположение компьютеров при наличии локальной сети поможет проводка.

Следует обратить внимание на содержимое мусорных корзин, надписей и наклеек на мониторе и системных блоках, т.к. там могут содержаться данные о пароле и учетном имени (логине) пользователя.

Особое внимание нужно обратить на места хранения внешних носителей информации, данные о подключении таких носителей содержатся в служебных файлах и реестре операционной системы. Причем в качестве носителей информации могут выступать, например фоторамки, плееры, и другие мультимедийные устройства.

Все изъятые системные блоки должны быть опечатаны таким образом, чтобы исключить возможность их включения и разборки.[14]

4. Осмотр мобильных телефонов, смартфонов и планшетных компьютеров с использованием программно-аппаратных комплексов.

В ходе осмотра мобильных устройств, смартфонов и планшетных компьютеров крайне рекомендуется использование специализированного программного обеспечения и (или) программно-аппаратных комплексов. Таких комплексов в настоящее время существует два - это UFED (производства фирмы Cellebrite, Израиль) и XRY (производства компании Micro Systemation, Швеция).

В соответствии с приказом Председателя Следственного комитета РФ в 2012 - 2013 годах все следственные управления Следственного комитета РФ были обеспечены аппаратно-программными комплексами UFED. Исходя из спецификации данного оборудования, UFED представляет собой средство для проведения оперативного исследования мобильных устройств. Аппаратно-программный комплекс позволяет провести упрощенное и быстрое логическое извлечение информации из обширного ряда мобильных устройств: мобильных телефонов, смартфонов, планшетов, телефонов

[14] Ю.М Баркалов «Актуальные проблемы информационной безопасности» Методические рекомендации для стран СНГ. Воронеж 2015 г.

китайской сборки на базе микропроцессора, некоторых моделей GPS-приемников, сим-карт мобильных устройств и карт памяти.

UFED использует несколько механизмов анализа мобильных устройств, а именно:

1) извлечение данных на физическом уровне;

2) логическое извлечение;

3) извлечение файловой системы.

Второй упомянутый нами программно-аппаратный комплекс, XRY, появился на рынке раньше UFED, и на сегодня его активно используют в правоохранительной системе Великобритании и США.

Комплекс работает в трех режимах, сходных с режимами UFED:

- XRY Logical предназначен для быстрого извлечения активных данных из мобильного устройства путем логического взаимодействия программного обеспечения с операционной системой устройства. Эффективен в 80% исследований. Обладает простым, интуитивно понятным и удобным интерфейсом;

- XRY Physical предназначен для физического извлечения (дампа) памяти мобильного устройства и ее последующего дешифрования. Обеспечивает глубокий анализ устройства с целью извлечения удаленных, защищенных или спрятанных данных;

- XRY Complete - полнофункциональное решение, объединяющее все инструменты и преимущества логического и физического извлечения данных. По информации производителя, программно-аппаратный комплекс предназначен для проведения защищенного извлечения цифровых данных из разнообразных мобильных устройств, таких, как смартфоны, GPS-навигаторы, 3G-модемы, портативные аудиоплееры и планшетные компьютеры. Благодаря функции "Мастер одновременного извлечения" комплекс позволяет пользователю исследовать до трех мобильных устройств одновременно, что достаточно существенно экономит время и ресурсы.

Аналогично с комплексом UFED в результате исследования телефонов создаются защищенные от несанкционированного доступа отчеты, которые можно вывести на печать или записать на компакт-диск. Функция экспорта XRY обеспечивает возможность создания отчетов в следующих форматах: html, xml, xlsx, xls, docx, doc и gpx.

В начале работы системы, после идентификации мобильного устройства, XRY подсказывает, какие данные можно извлечь из этой модели телефона, а какие нет.

После извлечения данных перед специалистом и следователем зачастую встает вопрос об анализе большого массива данных (особенно если речь идет о современных смартфонах), поэтому полезны инструменты приоритетной сортировки (Triage). Данная функция Списка особого контроля (Watch List Feature) помогает немедленно найти нужную следователю информацию для оперативного принятия решения.

Комплекс XRY позволяет извлекать данные из многочисленных программных приложений смартфонов. С его помощью можно извлечь данные вызовов IP-телефонии, картографическую информацию GPS и журналы средств оперативной пересылки сообщений.

Необходимо также отметить, что есть и новые технологии, позволяющие обойти защиту мобильного телефона и, как следствие, провести осмотр с максимальной степенью эффективности. Так, обойти защиту iPhone (начиная с версии 4) исключительно программными методами практически невозможно без риска повреждения данных, но устройство IP Box iPhone Password Unlock Tool (Китай), которое появилось в открытой продаже во втором квартале 2015 года, позволяет подключиться в iPhone или iPad и методом брутфорса (перебора) подобрать запрашиваемый при загрузке операционной системы iOS пароль[15].

[15] Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: "электронная почта" // Вестник Воронежского института МВД России. 2014. N 4. С. 46.

2.3. Особенности расследования краж и мошенничеств с использованием пластиковых карт и электронных платежных систем

Развитие банковских услуг в сфере электронных платежей привело к появлению нового направления преступной деятельности по совершению краж и мошенничеств сначала с использованием банковских карт и их реквизитов, а потом и в отношении средств, обращающихся в иных электронных платежных системах.

Типичные способы совершения краж и мошенничеств, совершенных с использованием банковских карт и их реквизитов, делятся на четыре группы:

1) использование подлинных карт;

2) использование конфиденциальной информации о реквизитах подлинных карт и их держателях;

3) использование поддельных карт;

4) использование несовершенства программно-аппаратного обеспечения технологии обращения пластиковых карт.

Важной особенностью механизма следообразования по кражам и мошенничествам, совершенным с использованием банковских карт и их реквизитов, является одновременное возникновение следов преступления в нескольких местах. Они возникают в рамках системы оборота банковских карт и их реквизитов, элементами которой являются: платежные системы; банки-эмитенты, банки-эквайреры; процессинговые центры; расчетные банки; торгово-сервисные предприятия; держатели карт; оборудование и коммуникации, связывающие финансовые организации между собой и с пунктами обслуживания карт. Во время проведения операций между участниками оборота банковских карт в автоматическом режиме осуществляется обмен информацией о проводимых транзакциях, что влечет за собой изменения на машинных носителях информации.

На стадии возбуждения уголовного дела при проверке сообщения о

краже и мошенничестве рассматриваемого вида необходимо устанавливать следующие обстоятельства:

1) факт проведения транзакции и ее характеристика (времени, места совершения транзакции, способа транзакции и др.);

2) наличие и характеристику ущерба;

3) сведения о пострадавшем лице;

4) характеристику банковской карты и ее связь с пострадавшим лицом;

5) сведения о возможном совершении держателем конкретной операции с использованием банковской карты, о ее передаче другому лицу, о поручении держателем другому лицу провести транзакцию с использованием банковской карты или ее реквизитов.

Основными методами проверки сообщений о кражах и мошенничествах, совершенных с использованием банковских карт и их реквизитов, являются:

1) запросы в банки-эмитенты, эквайреры, платежные системы с целью получения документов, отражающих факты совершения транзакций;

2) объяснения, взятые у держателей и лиц, совместно проживающих с ними;

3) осмотры мест происшествий;

4) осмотры предметов и документов: банковских карт; копий заявлений держателей об опротестовании конкретных транзакций; копий анкет держателей; копий договоров о кредитовании и выдаче банковских карт; копий выписок по карточным счетам за определенный период; копий электронных журналов банкоматов, POS-терминалов;

5) криминалистические и компьютерные исследования.

На первоначальном этапе расследования, в зависимости от места совершения кражи и мошенничества возникают следующие типичные ситуации:

1) имеются сведения о совершении кражи / мошенничества в месте,

оборудованном банкоматом;

2) имеются сведения о совершении кражи / мошенничества в месте, где используется POS-терминал;

3) имеются сведения о совершении кражи / мошенничества с использованием сети Интернет.

Общими для разрешения данных следственных ситуаций будут являться следующие действия:

1) осмотр места совершения транзакции с целью собирания и исследования следов совершения кражи или мошенничества;

2) допрос держателя банковской карты об обстоятельствах оспоренной транзакции;

3) допрос лиц, совместно проживающих с держателем карты, об обстоятельствах оспоренной транзакции;

4) допрос представителей банка об особенностях проведения транзакций, а также о факте совершения кражи или мошенничества;

5) выемка банковской карты у держателя и последующий ее осмотр с целью фиксации ее реквизитов и обнаружения на ней следов преступления;

6) выемка документов, подтверждающих договорные отношения между банком и держателем банковской карты, а также факт опротестования конкретных транзакций.

К тактическим особенностям осмотра места происшествия по делам о хищениях указанного вида относятся:

1) необходимость привлечения специалистов в области бухгалтерского учета и компьютерных технологий;

2) избирательность в применении тактических приемов;

3) наличие у понятых опыта использования банковских карт.

Глава 3. Использование специальных познаний при расследовании преступлений в сфере компьютерной информации и высоких технологий

3.1. Осмотр средств вычислительной техники (СВТ)

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.

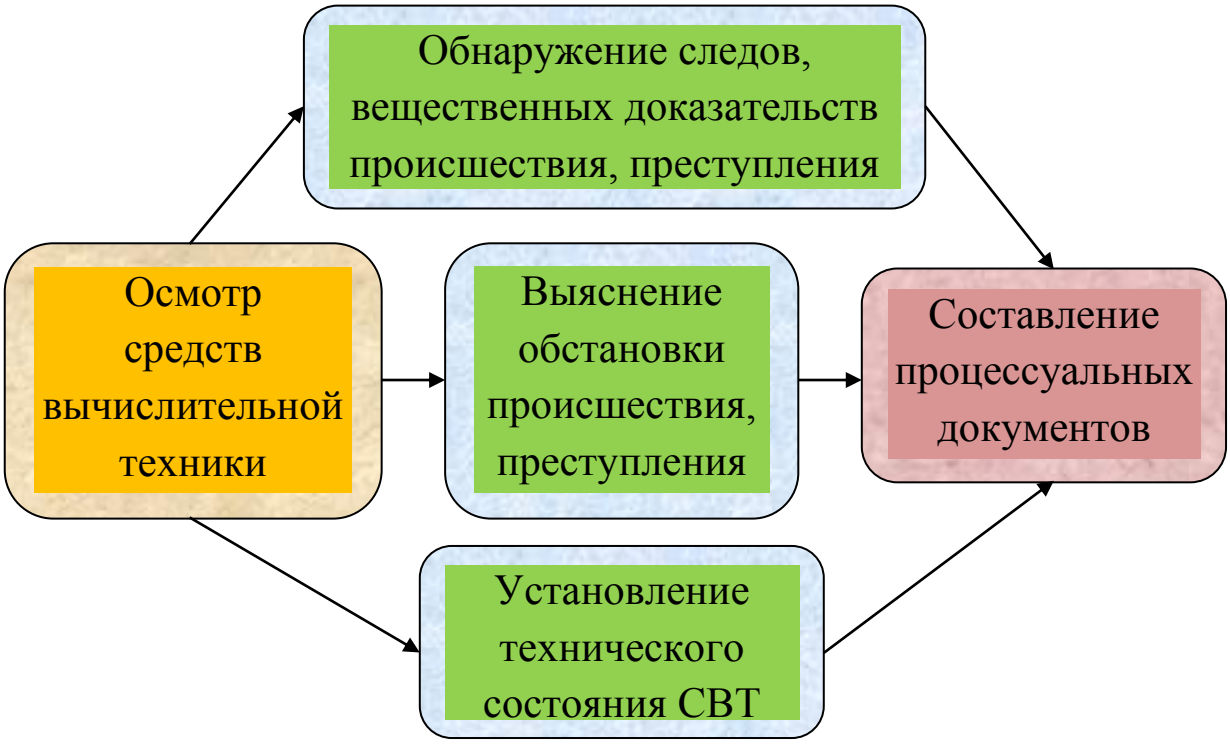


Рис. 1 Алгоритм расследования преступлений в сфере компьютерной информации и высоких технологий

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 ПК - 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 - ПК, 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 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 связи (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 находятся в рабочем состоянии;

- все 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 его составляющих, отсоединения коммуникационных и электропитающих проводов и кабелей, результаты измерения технических параметров контрольно-измерительной или тестовой аппаратурой и т. п.).

3.2. 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.

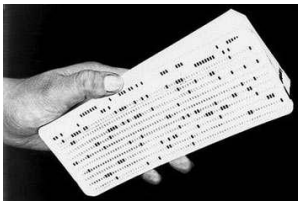
К машинным носителям информации относятся:

- магнитные диски (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. карты памяти, микрочипы).

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, плавления, 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.

Примечания:

1. Действия по пунктам 6 и 7 осуществляются соответствующим специалистом с использованием предназначенных для этого считывающих и осмотровых технических средств - осветителей, позволяющих просматривать носитель информации в бестеневом направленном освещении, на просвет, в ультрафиолетовых, инфракрасных, лазерных (оптических) лучах; электромагнитных, электронно-оптических, электромеханических считывающих (сканирующих) устройств; увеличительных приборов; измерительных инструментов и контрольно-измерительной аппаратуры.

Действия по пунктам 8 и 9 осуществляются специалистом в области компьютерной техники с использованием специально тестированных СВТ и соответствующего стандартного программного обеспечения (операционных систем, программ диагностики и контроля, в т. ч. антивирусных). Основные тактико-технические характеристики и индивидуальные признаки таких СВТ обязательно заносятся в протокол следственного действия - тип, марка, модификация, заводской или иной номер устройства (изделия) и т. д. При этом желательна распечатка всей информации, имеющейся на МНИ, в оперативной памяти, или полученной в результате использования программ

диагностики и контроля. Машинная информация, содержащаяся в ОЗУ, должна быть записана на постоянный носитель машинной информации, т. к. она автоматически уничтожается после выключения питания СВТ, выхода из тестирующей или прикладной пользовательской программы, при перезагрузке (смене) операционной системы или персонального компьютера.

3.3. 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, электронной подписи (ЭП)[16] либо иного аналога собственноручной подписи физического лица.

В частности, порядок использования ЭП 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 ПК, системе ПК или их сети с помощью ЭЦП определяется ГОСТ

[16] Об электронной подписи: Федеральный закон от 6 апреля 2011 г. № 63-ФЗ //Российская газета. 2011. №75.

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 ЭП).

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 (ЭП; 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.

Примечания:

1. Фактические данные по пунктам 10, 11 могут быть установлены по основным, автоматически фиксируемым СВТ реквизитам файла, в котором содержится документ, либо по электронно-цифровой подписи.

2. Запись документа на машинный носитель и создание машинограммы всегда должны производиться на основе данных, зафиксированных в исходных (первичных) документах, полученных по каналам электросвязи от автоматических регистрирующих устройств или в процессе автоматизированного решения задач.

3. Подлинники, дубликаты и копии документа на машинном носителе и машинограммы, полученные стандартными СВТ, имеют одинаковую юридическую силу, если оформлены в соответствии с требованиями ГОСТ 6.10.4-84.

4. Осмотр документа, как правило, приводит к необходимости следственной и оперативной проверки по существу данных и операций, которые отражает данный документ.

3.4. 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 участии 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 следующие 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 специального 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 степлером, 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 могут возникать конфликты между следователем и 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.).

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, фото- и видеопленка, магнитный носитель информации (лента, дискета или жесткий диск), распечатка информации.

3.5. 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:

- 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 выключать-включать электроснабжение объекта (указанные действия проводить только с разрешения специалиста);

- 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 электросвязи»; «канал электросвязи - периферийное устройство».

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 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 специалист установит, 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 находится предметы, устройства и документы. Ими могут быть и сами СВТ - аппаратные и программные оболочки модулей их 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 для лабораторного исследования;

- все обнаруженные машинные носители информации (дискеты, пластиковые карточки, ленты, оптические компакт-диски, аудио- и видеокассеты) следует изъять для последующего анализа содержащихся на них данных. Осмотр и анализ информации проводится только на аттестованном исследовательском оборудовании;

- 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 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 являются: средства вычислительной техники; машинные носители информации, машинная информация; всевозможные документы; средства защиты информации; специальная разведывательная и контрразведывательная аппаратура; 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.

3.6. Назначение экспертиз

В соответствии с УПК РФ[17] экспертиза назначается в случаях, когда при производстве дознания, предварительного следствия и при судебном разбирательстве необходимы специальные познания в науке, технике, искусстве или ремесле.

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-х годов в России появился новый вид криминалистических экспертиз, получивших название ***программно-технических*** (сокр. ПТЭ - программно-техническая экспертиза).

[17] "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 06.07.2016) (с изм. и доп., вступ. в силу с 01.09.2016).

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 ПК, системы ПК или их сети (вредоносных средств - компьютерных вирусов, «закладок», «жучков» 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 ПК, системы ПК или их сети;

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

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?

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

6. Какая компьютерная информация и в какой форме (файл, программа, документ) была стерта, скопирована, изменена (модифицирова-на), 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 представьте ее в виде распечатки на бумажном носителе.

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 ПК, системы ПК 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 ПК 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 ПК, системы ПК, 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 ПК (системе ПК, 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 ПК (компьютерной информации), представленной на исследование?

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

25. Каковы каналы утечки компьютерной информации из ПК, системы ПК, 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 ПК (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 ПК, системой ПК 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 программно-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, 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 программно-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 ПК; в определении фактов уменьшения облагаемой налогом прибыли; в выявлении счетных работников, причастных к совершению компьютерного преступления, путем исследования носителей оперативной информации, а также лиц, вводивших соответствующие данные в ПК, 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 с 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 нарушений в этих нормативных документах, 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 они 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.

Наиболее оптимальным вариантом в некоторых случаях является назначение комплексной программно-технической и судебно-бухгалтерской экспертизы. Как 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 экспертизы (в частности, технико - криминалистические экспертизы документов, по исследованию бумаги, чернил (красок), почерка и т. д.).

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

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

2. В каком диапазоне радиочастот работает данное устройство и какова его мощность в антенне? Укажите дальность радиосвязи и другие тактико-технические характеристики приема/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 ПК 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.

Эксперт - лицо, обладающее специальными знаниями и назначенное в порядке, установленном настоящим Кодексом, для производства судебной экспертизы и дачи заключения.

Вызов эксперта, назначение и производство судебной экспертизы осуществляются в порядке, установленном УПК РФ.

Эксперт вправе:

- знакомиться с материалами уголовного дела, относящимися к предмету судебной экспертизы;
- ходатайствовать о предоставлении ему дополнительных материалов, необходимых для дачи заключения, либо привлечении к производству судебной экспертизы других экспертов;
- участвовать с разрешения дознавателя, следователя и суда в процессуальных действиях и задавать вопросы, относящиеся к предмету судебной экспертизы;
- давать заключение в пределах своей компетенции, в том числе по вопросам, хотя и не поставленным в постановлении о назначении судебной экспертизы, но имеющим отношение к предмету экспертного исследования;
- приносить жалобы на действия (бездействие) и решения дознавателя, следователя, прокурора и суда, ограничивающие его права;
- отказаться от дачи заключения по вопросам, выходящим за пределы специальных знаний, а также в случаях, если представленные ему материалы недостаточны для дачи заключения. Отказ от дачи заключения должен быть заявлен экспертом в письменном виде с изложением мотивов отказа.

Эксперт не вправе:

- без ведома следователя и суда вести переговоры с участниками уголовного судопроизводства по вопросам, связанным с производством судебной экспертизы;

- самостоятельно собирать материалы для экспертного исследования;
- проводить без разрешения дознавателя, следователя, суда исследования, могущие повлечь полное или частичное уничтожение объектов либо изменение их внешнего вида или основных свойств;
- давать заведомо ложное заключение;
- разглашать данные предварительного расследования, ставшие известными ему в связи с участием в уголовном деле в качестве эксперта, если он был об этом заранее предупрежден в порядке, установленном статьей 161 настоящего Кодекса;
- уклоняться от явки по вызовам дознавателя, следователя или в суд.

За дачу заведомо ложного заключения, а также разглашение данных предварительного расследования эксперт несет ответственность в соответствии УК РФ.

Судебная экспертиза производится государственными судебными экспертами и иными экспертами из числа лиц, обладающих специальными знаниями.

Эксперт вправе указать в своем экспертном заключении выявленные при производстве экспертизы факты или обстоятельства имеющие значения для уголовного дела, но по которым перед экспертом не были поставлены вопросы.

Если при производстве судебной экспертизы эксперт установит обстоятельства, которые имеют значение для уголовного дела, но по поводу которых ему не были поставлены вопросы, то он вправе указать на них в своем заключении.

Материалы, иллюстрирующие заключение эксперта (фотографии, схемы, графики и т.п.), выносятся в приложение к заключению эксперта и являются его составной частью.

При производстве компьютерных экспертиз и исследований основным является обеспечение неизменности информации на исследуемых носителях

информации. Для этого применяют аппаратные или программные средства блокирования записи.

При производстве судебной компьютерной экспертизы решают следующие задачи:

1. Поиск информации.

2. Определение обстоятельств установки и использования программных продуктов и оборудования.

К задачам поиска информации относят:

- поиск текстовой информации по ключевым словоформам;
- поиск графической информации по заданным критериям;
- поиск текстовой и графической информации по соответствию предоставленным образцам;
- поиск информации о сетевых подключениях (выход в сеть «internet»);
- поиск программных продуктов и др.

Для решения задачи поиска компьютерной информации вопросы, выносимые на компьютерную экспертизу, могут быть сформулированы следующим образом:

- имеется ли на представленных, на исследование машинных носителях (дать перечень) информация, содержащая следующие ключевые слова: (дать перечень ключевых слов)?
- имеется ли на предоставленных, на исследование машинных носителях (дать перечень) информация о (изложить о чем)?

Перед началом поиска информации необходимо выполнить восстановление удаленной информации, при этом восстановление информации следует выполнять с использованием различных специализированных программных продуктов.

Поиск текстовой информации проводится по ключевым словам (приводятся в вопросах постановления о назначении экспертизы). Для поиска

текстовой информации используются стандартные средства поиска «Windows», программы «Архивариус 3000», «AVSearch» и встроенные средства поиска файловых менеджеров.

Поиск графической информации проводится путем просмотра графических файлов. Важно заметить, что изображения так же могут содержаться, например, в файлах созданных приложениями Office, однако данные файлы графическими являться не будут. С помощью программ поиска текстовой информации, возможно, искать графические файлы, например содержащие информацию EXIF. При этом возможно установить графические файлы, созданные с помощью определённых моделей цифровых фотоаппаратов или камер мобильных телефонов.

Для поиска графической информации с помощью «Архивариус 3000» возможно вводить в поисковый запрос сведения EXIF цифровой фототехники, например модель или серийный номер цифровой фотокамеры.

Так же возможен поиск по расширению файлов. Найденные файлы копируются на стендовый носитель, для дальнейшего исследования (просмотра).

Определение обстоятельств установки и использования программных продуктов и оборудования проводится следующим образом:

- исследуется установленное программное обеспечение на контрафактность;
- проверяются параметры и регистрационные данные программного обеспечения;
- поиск следов использования программного обеспечения и оборудования.

В среде «Windows» большинство основных данных об установленном программном обеспечении и оборудование хранится в реестре.

Рассмотрим, для примера, исследование параметров программного продукта «1С» версии 7.

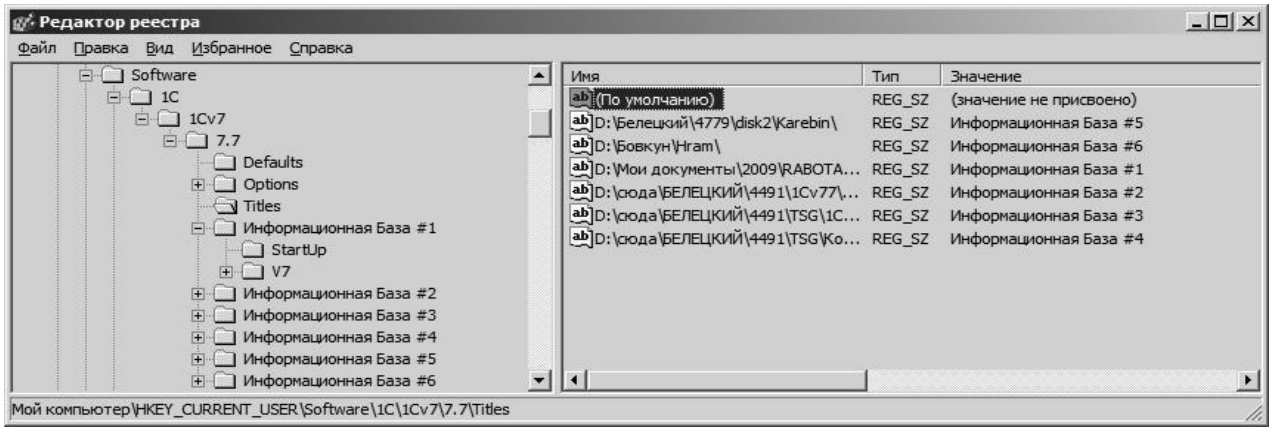


Рис.2 Снимок экрана ветви реестра

Сведения о подключении баз экономических программных продуктов «1С» и проведенных с ними действиях содержатся в файле «NTUSER.DAT» из директории «:\Documents and Settings\ (пользователь)», где (пользователь)» - имя пользователя. Данный файл содержит информацию из ветви реестра «HKEY_CURRENT_USER» OS MS Windows, содержащей настройки, соответствующие текущему активному пользователю, выполнившему вход в систему (строка «Software\1C\1Cv7\7.7\Titles» ветви реестра [HKEY_CURRENT_USER]) (Рис.1).

Также ряд данных хранится в ключах реестра в файлах: system, default, SAM, SECURITY, software из директории WINDOWS\system32\config\.

Для определения проведённых действий операционной системой семейства «Windows» производится просмотр журнала событий операционной системы содержащихся в файлах «SysEvent.Evt» и «AppEvent.Evt», расположенных в директории «:\WINDOWS\system32\config\» для Windows XP и в файлах «Application.Evtx» и «System.Evtx», расположенных в директории %SystemRoot%\System32\Winevt\Logs\ для Windows 7.

Просмотром данных журналов возможно определить:

- временные рамки работы операционной системы;

- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы «Windows»;

- временные рамки подключения - отключения сетевых ресурсов (сетевого адаптера) запуск которых отображается в журнале событий операционной системы «Windows», и ряд других параметров.

Для определения сведений об операционной системе следует использовать данные из реестра.

Дата инсталляции InstallDate (дата инсталляции дата установки операционной системы хранится в шестнадцатеричном и десятичном виде).

Идентификационные номера продукта и пути установки

Если система находится в активном состоянии, включена, то используют данные, полученные с помощью команды: «systeminfo».

Информация о подключенных внешних устройствах хранится в реестре операционных систем, журналах событий и в файле «setupapi.log», расположенном в директории «Windows» для Windows XP и в файле «setupapi.dev.log», расположенном в директории \Windows\inf\ для Windows 7». В данных ветвях содержится информация о типе и виде подключенных устройств, а так же их серийный номер и уникальный номер (Globally Unique Identifier - GUID), который идентифицирует устройство для системы.

Ниже на рисунке 3 приведены данные из реестра о подключении внешних устройств:

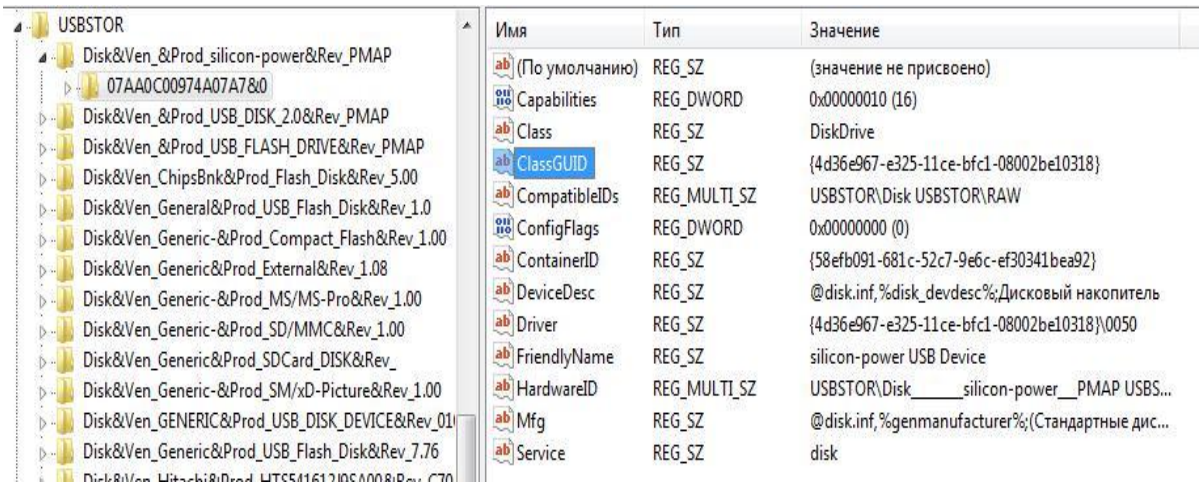


Рис. 3. Реестр о подключении внешних устройств

Используя данные из файла: «setupapi.log» для Windows XP и данные из файла «setupapi.dev.log» для Windows 7, по серийному номеру устройства можно определить дату и время его подключения. Для чего необходимо:

- открыть файл для просмотра;
- определить с помощью поиска строку, содержащую серийный номер устройства или GUID;
- выше в скобках будет указана дата и время подключения.

Важно отметить, что данная информация изменяется через определенное время и не может мгновенно отразить данные о подключении устройств.

Данные о подключенных устройствах отражаются в журнале событий, в частности в меню «приложение» и «система».

Для меню «Система» Windows 7 коды событий, где можно посмотреть информацию о подключённых внешних устройствах: «20001», «10000», «20003». Данные коды событий можно задать в «фильтре» программы просмотра журналов.

На рисунке 4 приведено изображение окна программы с выборкой фильтра «10000»:

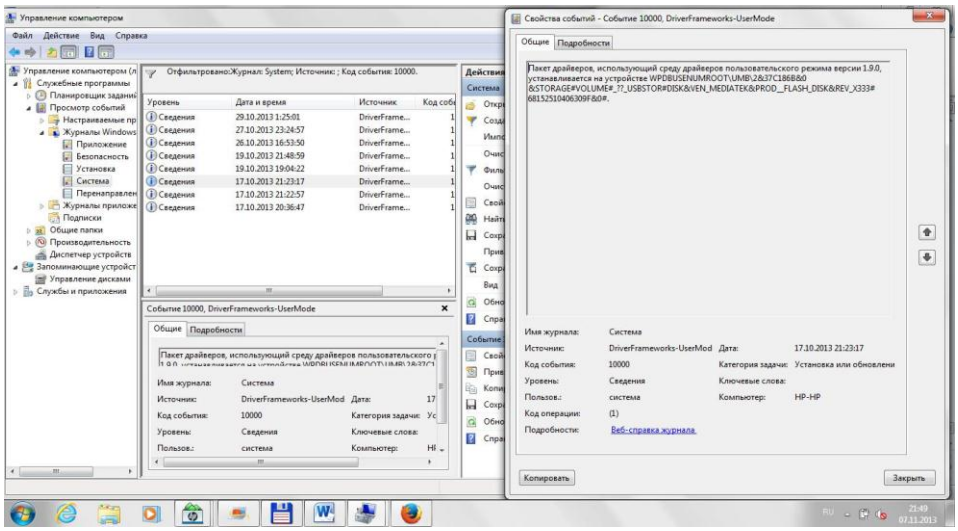


Рис. 4 Окно программы выборки

Для просмотра файлов журналов событий можно использовать штатные средства операционной системы, в меню «действия» программного обеспечения «управление компьютером» открыв исследуемый файл. Или воспользоваться специализированным программным обеспечением, например «Event Log Explorer».

Для определения проведенных действий операционной системой семейства «Windows» производится просмотр журналов событий операционной системы.

В «WindowsXP» данные файлы по умолчанию расположены в директории «%SYSTEMROOT%\system32\config\ и имеют расширение «.Evt»

Для Windows 7 данные файлы по умолчанию расположены в директории «%SYSTEMROOT%\System32\Winevt\Logs\» и имеют расширение «.Evtx».

Просмотром данного журнала возможно определить:

- временные рамки работы операционной системы;
- временные рамки запуска ряда программных продуктов, запуск которых отображается в журнале событий операционной системы «Windows»;
- временные рамки подключения - отключения сетевых ресурсов (сетевого адаптера), запуск которых отображается в журнале событий операционной системы «Windows», и ряд других параметров.

К программным продуктам, которые оставляют различные следы при работе в операционных системах относятся:

- Браузеры (Internet Explorer, Opera, Mozila Firefox, Google Chrome идр.);
- Программы для переписки (ICQ, QIP, Skype и д.р.);
- Программы – почты (Outlook Express, The Bat);
- Другие программы – игры, торенты и т.д.

При работе в браузерах следы остаются в файлах cookies, cache

браузера и реестре.

Cookies («куки») – это текстовые файлы содержащие информацию о работе браузера, в том числе данные о посещении ресурсов и «кэши» паролей обращения к сетевым ресурсам.

Требования к вопросам, выносимым на судебную компьютерную экспертизу

Общие требования:

1. При постановке вопроса необходимо использовать устоявшийся понятийный аппарат, исключающий жаргонные и полупрофессиональные термины («винчестер», «логи», «взлом» и т.п.). В случае отсутствия терминов, определенных законодательными или нормативными актами, необходимо использовать те термины, которые употребляют разработчики технических средств, программных продуктов в документации, описаниях, справках и т.п.

2. Вопрос должен быть четким и однозначным.

3. Формулировка вопроса не должна касаться этапов исследования информации (описание характеристик носителей информации и особенностей размещения информации на них, восстановление и исследование информации среди удаленных файлов являются обязательным этапом исследования информации).

4. Вопросы не должны носить справочный характер.

5. Вопросы не должны носить правовой характер и выходить за пределы компетенции эксперта.

6. Вопросы должны соответствовать существующей методической и технической базе.

Частные требования:

1. Вопросы должны быть направлены на установление конкретных обстоятельств расследуемого события.

2. Вопросы должны быть поставлены так, чтобы при решении конкретных задач расследования затраты (финансовые, технические, временные и пр.) на проведение исследований были минимальными.

3. Вопросы должны соответствовать уровню подготовки и инструментальному оснащению экспертов того экспертного учреждения, которому назначается экспертиза.

4. Вопросы должны соответствовать представляемым на исследование вещественным доказательствам.

При постанове вопросов о работоспособности программного обеспечения можно сослаться на ГОСТ 28195-89 (Оценка качества программных средств. Общие положения).

Под «работоспособностью программного средства» понимается «способность программы функционировать в заданных режимах и объемах обрабатываемой информации в соответствии с программными документами при отсутствии технических средств».

В соответствии, с которым для решения данного вопроса необходим весь комплект документации по рассматриваемому программному обеспечению. При этом продукт должен содержать все задекларированные разработчиком возможности, которые известны только разработчику.

Последовательность действий эксперта

Действия эксперта должны проводиться в следующем порядке:

1. Осмотреть и описать упаковку объектов, представленных на экспертизу. Опционально – сфотографировать упаковку.
2. Извлечь объекты из упаковки, сфотографировать (с линейкой) и описать.
3. При описании системного блока привести:

- габаритные размеры (ширина х, высота х, глубина в мм);
- цвет корпуса;

- расположение и описание устройств, кнопок, индикаторов, разъемов, наклеек на передней панели (лицевой стороне) системного блока;

- описание разъемов, наклеек и т.п. на задней панели (тыльной стороне) системного блока;

- описание боковых панелей системного блока (при наличии на них кнопок, разъемов и т.п.);

- описание индивидуализирующих особенностей (надписей, наклеек, повреждений и т.п.);

- описание основных компонентов системного блока (маркировочных обозначений на системной плате, платах расширения и пр.);

- сфотографировать системный блок со снятой боковой крышкой.

4. Извлечь из системного блока машинные носители и описать их. При описании указать:

- размерные характеристики (форм-фактор);

- основные маркировочные обозначения на НЖМД (марка, модель, емкость, серийный номер).

5. Просмотреть настройки даты и времени на системной плате с помощью базовой системы ввода-вывода (BIOS) и сопоставить их с текущими с указанием установленного и текущего часовых поясов.

При ответах на поставленные вопросы необходимо:

- выявить программное обеспечение, работа которого требует регистрации в операционной системе;

- выявить программное обеспечение, работа которого не требует установки в операционной системе;

- выявить удаленное программное обеспечение либо сведения, оставшиеся в операционной системе от ранее установленного и впоследствии удаленного программного обеспечения;

- описать и просмотреть наличие и содержимое возможных мест расположения следовой информации на машинных носителях.

При необходимости сопоставить найденную информацию между собой на предмет ее непротиворечивости и последовательности по времени.

6. Формулирование выводов эксперта.

По результатам проведенного исследования формулируется вывод о наличии или отсутствии искомой информации на машинных носителях.

Примеры вопросов выносимых на судебную компьютерную экспертизу

По дискам с программами:

1. Какие программные продукты, правообладателем которых, указаны (например: корпорация «Microsoft», компания «Autodesk» и ЗАО «1С») содержатся на представленных оптических дисках?

2. Возможно, ли использовать данные программные продукты без их активации (регистрации), если нет, то имеются ли, на представленных, на исследование, оптических носителях программы, коды или иная информация, служащая для активации (регистрации) указанных программных продуктов?

По установленному ПО:

1. Какие программные продукты, правообладателем которых указана корпорация «Microsoft», компания «Autodesk» и ЗАО «1С», установлены на носители информации предоставленного системного блока?

2. Имеются следы использования данных программных продуктов?

По установщикам:

1. Какие программные продукты, правообладателем которых указана корпорация «Microsoft», компания «Autodesk» и ЗАО «1С», установлены на носители информации предоставленного системного блока?

2. Какие установочные версии программных продуктов, аналогичные версиям, установленным на носители информации предоставленного системного блока, программных продуктов, правообладателем которых указана корпорация «Microsoft» компания «Autodesk» и ЗАО «1С», имеются

на предоставленных носителях информации (оптических дисках, флэш-накопителе и …)?

3. Могли ли быть установлены вышеуказанные программные продукты на носители информации предоставленного системного блока с предоставленных носителей информации (оптических дисков, флэш-накопителя)?

По поиску информации:

- Имеются ли на предоставленном носителе информации файлы, одновременно содержащие тексты (указать какие)?

По результатам исследования согласно ст. 204 УПК РФ составляется заключение эксперта[18].

Выводы должны соответствовать поставленным вопросам.

Количество выводов должно соответствовать количеству вопросов.

[18] "Уголовно-процессуальный кодекс Российской Федерации" от 18.12.2001 N 174-ФЗ (ред. от 06.07.2016) (с изм. и доп., вступ. в силу с 01.09.2016).