ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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

Подобную тенденцию можно проиллюстрировать следующими примерами. Так, в августе 1991 г. было совершено хищение 125,5 тысяч долларов США во Внешэкономбанке СССР, что по курсу Госбанка СССР, действовавшему на день причинения ущерба, составило 4 млн 16 тыс. рублей. В октябре 2003 г. было совершено покушение на хищение денежных средств в крупных размерах из Главного расчетно-кассового центра (РКЦ) Центрального банка России по г. Москве на сумму 68 млрд 309 млн 768 тыс. рублей. В апреле 2008 г. аналогичное преступление было совершено в РКЦ г. Махачкалы на сумму 35 млрд 1 млн 557 тыс. рублей. В 2006 г. была проведена целая серия подобных преступлений: в городах Миасс и Златоуст совершены 2 покушения на хищение, причем в обоих случаях запущенный в ЭВМ вирус (вредоносная программа) стер всю информацию о лицах, направивших запросы на снятие банковских денег; в г. Екатеринбурге двое сотрудников СТЗ-банка путем внесения изменений в компьютерную программу похитили 50 млн рублей и т. д.

Приходится констатировать, что процесс компьютеризации общества привел к возникновению новых видов преступных посягательств, ранее не известных отечественной юридической науке и практике, связанных с использованием средств электронно-вычислительной техники и информационно-обрабатывающих технологий. Данные преступления стали называться компьютерными, исходя из аналогов и терминологии

зарубежной юридической практики. Как свидетельствует статистика, в последнее время количество хищений неуклонно увеличивается, возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от обычных видов преступлений.

Например, из материалов одного уголовного дела известно, что по заказу некоей московской коммерческой структуры лицам, входящим в состав организованной преступной группы, с целью устранения конкурента заказчика удалось осуществить неправомерный доступ к компьютерной информации австрийского банка и таким образом блокировать его работу в течение суток. Криминальная операция была осуществлена с использованием широко распространенных СВТ и средств связи.

Анализируя нынешнее развитие ситуации с точки зрения будущего, специалисты прогнозируют рост организованной преступности, связанной с использованием в корыстных целях электронных средств, одним из которых является персональный компьютер. Предполагается, что в ближайшее время различные учреждения и организации все больше будут полагаться на обработку данных с помощью ЭВМ и новых информационных технологий. По мере развития техники все большее число стран будет подключаться к существующим и вновь образуемым компьютерным информационным сетям, на которых в настоящее время базируется вся мировая экономика, что неизбежно приведет к появлению у преступных групп и сообществ еще большего желания обогатиться. По данным ФБР США, российские специалисты - компьютерщики, входящие в состав отечественных преступных групп и сообществ, осуществляющих свою преступную деятельность на территориях США и западноевропейских стран и обладающих достаточным финансовым и кадровым потенциалом, без особого труда могут «взломать» почти любые коды и получить неправомерный доступ к коммерческим секретам крупнейших многонациональных корпораций. В результате таких действий десятки миллионов долларов в считанные минуты незаконно снимаются со счетов корпораций и переводятся на оффшорные счета, используемые преступниками. Согласно оценкам специалистов, ежемесячно совершается около тысячи подобных « операций », проследить за которыми ни отечественные, ни зарубежные правоохранительные органы пока не могут.

Начиная с 2002 г., отечественным преступным группировкам с помощью СВТ и новейших электронных средств спутниковой связи удалось подключиться к международной подпольной банковской системе для проведения собственных расчетно-кассовых операций в целях финансового обеспечения преступной деятельности.

По данным Следственного комитета МВД России, с начала 2000-ых годов значительную распространенность и повышенную общественную опасность получили различного рода хищения, совершаемые с применением пластиковых карт, являющихся носителями охраняемой законом компьютерной информации. В 2006 г. в целом по Российской Федерации было возбуждено 40 уголовных дел по результатам преступлений данной категории, общий ущерб по которым составил 5 млн долларов США. Так, только по одному из них к уголовной ответственности было привлечено 25 человек, совершивших 300 хищений денежных средств с использованием пластиковых кредитных карточек и поддельных слипов на сумму 600 тыс. долларов. Стоит отметить, что при проведении экспертизы названных платежных документов специалисты были удивлены столь высоким качественным уровнем их подделки.

Расследование подобных преступлений вызывает серьезные затруднения в документировании преступной деятельности, выявлении преступников, требует привлечения специалистов в области вычислительной техники, новейших средств электросвязи и защиты конфиденциальной информации. В настоящее время в Главном управлении по борьбе с экономическими преступлениями МВД России функционирует специализированное подразделение по борьбе с хищениями денежных средств, совершаемых с использованием ЭВМ. Также было создано отдельное управление по борьбе с преступлениями в сфере высоких технологий.

Особенностям расследования преступных посягательств данной категории и посвящается настоящая работа.

1. ПОНЯТИЕ «ИНТЕРНЕТ-ТЕХНОЛОГИИ»

Интернет-технологии – это разного рода технологии и сервисы, которые позволяют осуществлять всю деятельность в компьютерной сети Интернет.

Если выразиться проще, интернет-технологии – это всё, с чем мы работаем в Интернете. В первую очередь – это всевозможные сайты, форумы, блоги. Также к интернет-технологиям относятся программное обеспечение и всевозможные механизмы для работы со «всемирной паутиной».

В основе Интернет-технологий лежат гипертексты (тексты с гиперссылками на другие гипертексты) и сайты, размещаемые в глобальной сети Интернет либо в локальных компьютерных сетях.

Свойствами информационных технологий являются:

- развитие информационных ресурсов общества
- оптимизация информационных процессов
- доведение информации и информационное воздействие между людьми
- ускорение интеллектуального развития общества
- влияние на все сферы деятельности общества

Интернет-технологии представляют собой сложную систему взаимодействия двух составляющих: физической и логической.

Физическая составляющая Интернет - технологий включает:

1) Сеть Интернет
   - Протоколы TCP/IP.
   - Иерархия доменных имен сети Интернет.
   - Опорная сеть Интернета. Маршрутизация.
2) Программное обеспечение в Интернете
   - Сетевые операционные системы.
   - Специальное программное обеспечение для соединения с Интернетом.
   - Прикладные протоколы.
3) Компьютеры (серверы и клиенты) в Интернете
   - Серверы электронной почты

- Веб – серверы.
- FTP-серверы.
- Серверы телеконференций.
- Серверы мгновенных сообщений.

4) Цифровые линии связи
- Выбор провайдера. Подключение к Интернету

5) Доступ в Интернет
- Соединение сетевой карты с локальной сетью
- Кабельные системы Ethernet

6) Удаленный доступ к глобальным сетям
- Доступ «компьютер – сеть»
- Доступ «сеть-сеть»

Логическая составляющая Интернет - технологий включает в себя:

1) Интернет - сервисы
- WWW - Всемирная паутина
- Электронная почта. Системы телеконференций
- Передача данных
- On-line чат
- Передача быстрых сообщений
- Аудио- и видеоконференции.
- Голосовое общение

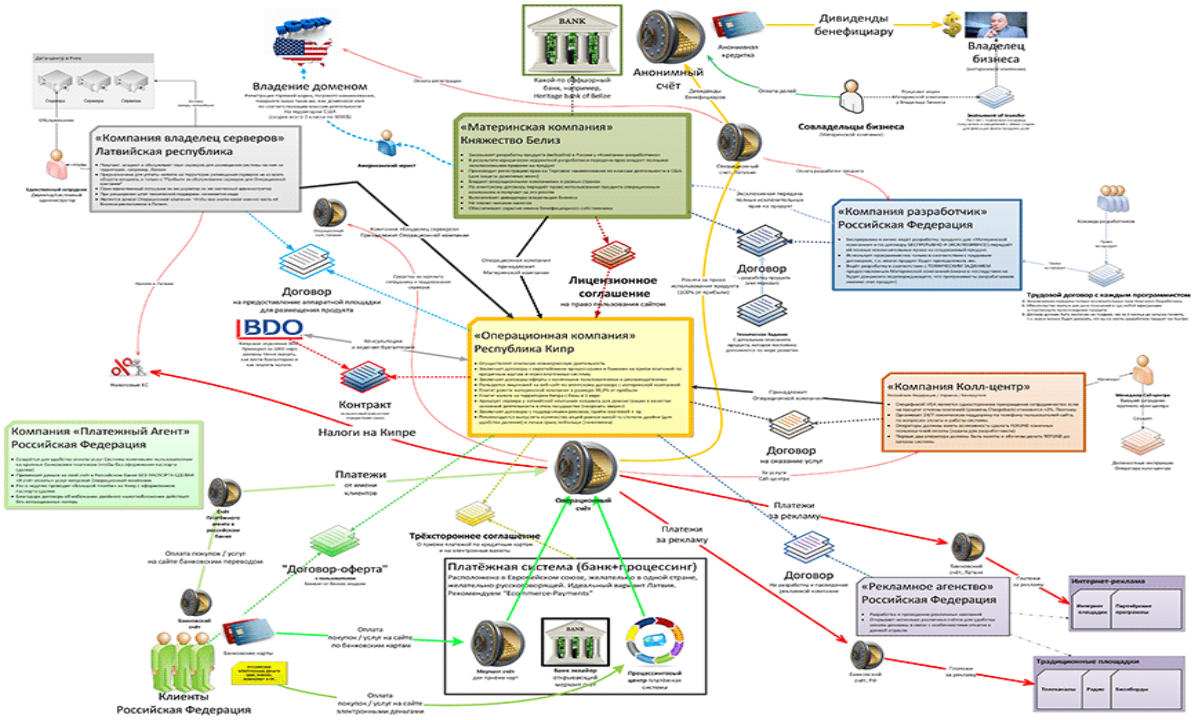
2) Работа в Интернете
- Браузеры
- Поисковые системы. Навигация в Интернете
- Просмотр страниц в браузере

3) Информационные ресурсы в Интернете
- Веб -страницы, интернет-магазины, интернет-порталы. Веб – пространство
- URL и протоколы передачи данных, адресация
- Создание Веб-сайтов. Языки Веб-программирования
- Записи в Интернете. Представительство

Этот список может быть не полным, так как с каждым днем интернет-технологии развиваются всё быстрее и быстрее и возникают новые виды как технических, так и логических составляющих.

Пример оффшорной схемы интернет бизнеса

Модель полностью легальна, налоговые потери ~1%, бенефициарный собственник не определяем.



Таким образом, интернет-технологии неоспоримо производят огромное влияние как на жизнь, так и на развитие человека во всех сферах его существования, поэтому они и дальше будут развиваться.

Базовые определения

Сервер - компьютер (сетевой узел), обеспечивающий пользователям сети доступ к файлам, устройствам печати, коммуникационным и другим службам. Обычно сервер более мощный по основным техническим параметрам, чем однопользовательские рабочие станции. Многие серверы подключаются к источникам бесперебойного питания и обладают повышенной отказоустойчивостью.

Программа-сервер - специальная программа обслуживания доступа к серверу.

Программа-клиент - программа, которая может устанавливать связь с сервером определенного типа, для того чтобы получить определенную информацию, хранящуюся на сервере.

В основу взаимодействия компонентов информационных сервисов Сети в большинстве случаев положена модель "клиент-сервер". Как правило, в качестве клиента выступает программа, которая установлена на компьютере пользователя, а в качестве сервера - программа, установленная у провайдера.

Провайдер - организация или частное лицо, которое ведет (поддерживает) информационные ресурсы.

Протокол - набор правил, которых придерживаются компании, чтобы обеспечить совместимость аппаратного и программного обеспечения.

Интернет работает под совокупностью протоколов разных уровней, которую называют (семейством протоколов или стеком) TCP/IP (Transmission Control Protocol/Internet Protocol). В стеке TCP/IP накоплено большое количество протоколов и сервисов прикладного уровня.

(Замечание: одним термином может обозначаться и протокол, и информационный ресурс, и программа). Так, например:

FTP (File Transfer Protocol):

протокол, используемый для получения доступа к сети, просмотра списка файлов и каталогов, а также для передачи файлов;

система файловых архивов - огромное хранилище всевозможной информации (тексты, программы, фильмы, фотографии, аудиозаписи и пр.), накопленной за последние 10-15 лет в Сети;

интерфейс пользователя при обмене файлами по одноименному протоколу (Интерфейс – программное или аппаратное обеспечение, предназначенное для связи одного компьютера с другим; способ взаимодействия пользователя с программой).

HTTP (Hypertext Transfer Protocol) – протокол передачи гипертекста, доступа к удаленным гипертекстовым базам данных во всемирной паутине WWW.

POP, SMTP – протоколы передачи электронной почты, входящей и исходящей.

NNTP – передача новостей и телеконференций.

Краткая характеристика основных Интернет-ресурсов:

FTP – см. выше

Usenet – система телеконференций Интернета. Система построена по принципу электронных досок объявлений, когда любой пользователь мо-

жет поместить свою информацию в одну из групп новостей Usenet и эта информация станет доступной другим пользователям, которые на данную группу новостей подписаны.

WAIS – это распределенная информационно-поисковая система Интернета. Широко применяется как поисковая машина в других информационных серверах Интернета, например WWW и Gopher.

LISTSERV – строго говоря, не сервис Интернета, а система почтовых списков сети BIT-NET (сеть образовательных учреждений). Однако это очень популярный ресурс в глобальных компьютерных сетях. LISTSERV специально ориентирован на применение в качестве транспорта электронной почты. Доступ к нему в интерактивном режиме затруднен. В мире насчитываются многие сотни списков LISTSERV, которые организованы по группам интересов.

WHOIS – служба содержит информацию о пользователях сети, их электронные и обычные адреса, идентификаторы и реальные имена.

Hytelnet – обширная база данных, одна из самых старых информационных технологий Интернет. Содержит список адресов локальных баз данных большого количества библиотек как европейских, так и американских университетов, правительственных учреждений и международных организаций.

IRC (Internet Relay Chat) – средство для переговоров в реальном масштабе времени, которое дает возможность разговаривать с людьми в режиме прямого диалога.

World Wide Web (WWW) – распределенная гипертекстовая информационная система. Она представляет удобный доступ к большинству информационных архивов Сети. Особенностью системы является механизм гипертекстовых ссылок, который позволяет просматривать материалы в порядке выбора этих ссылок пользователем. Выбор интересующего материала может быть осуществлен простым нажатием кнопки «мыши» на нужном слове. В WWW существует большое количество различного рода каталогов, которые позволяют ориентироваться в сети, кроме этого пользователи могут выполнять даже удаленные программы или смотреть фильмы по сети. Такой сервис не обеспечивается другими информационными системами Интернета.

(Гипертекст – система связанных слов и фраз, позволяющая осуществлять навигацию между страницами. Гипермедиа – среда, основанная на внутренних взаимосвязях. Развив концепцию гипертекста включением в нее фотографий, видео, звука, получим то, что известно как гипермедиа).

Как же осуществляется поиск необходимого информационного ресурса?

В Интернете каждой машине приписан определенный адрес, по которому к ней и осуществляется доступ. Существует одновременно как числовая адресация (так называемый IP-адрес, состоящий из набора четырех чисел, разделенных точками, например 144.206.160.32), так и более удобная для восприятия человеком система осмысленных доменных имен. В Интернете принята система адресов, которая базируется на доменном адресе машины.

URL-адрес (Uniform Resourse Protocol) - унифицированная форма записи адресов документов в Интернет.

Например: http://www.tstu.ru/rus/index.htm#ref1

Правила записи в этой форме таковы, что позволяют однозначно определить местонахождение документа в Сети. Адрес URL может состоять из четырех полей:

1) имени протокола (http://, ftp://,...)

2) имени компьютера (www.tstu.ru)

3) пути поиска документов на этом компьютере (/rus/index.htm)

4) ссылки на определенное место внутри документа (#ref1)

Существуют специальные программы-клиенты для просмотра содержимого Web-страниц – браузеры

На сегодняшний день наиболее популярные:

Internet Explorer

Netscape Navigator

Opera

Поисковая машина – специальный Web-узел, предназначенный для поиска информации в Интернет.

http://www.aport.ru

http://www.rambler.ru

http://www.yandex.ru

Электронная почта (e-mail) является чрезвычайно важным информационным ресурсом Интернет. Помимо того, что она представляет собой самое массовое средство электронных коммуникаций, через нее можно принять или послать сообщения еще в два десятка международных компьютерных сетей, часть из которых не имеют on-line сервиса (т.е. прямого подключения к Интернету).

Электронная почта во многом похожа на обычную почтовую службу. Корреспонденция подготавливается пользователем на своем рабочем месте либо программой подготовки почты, либо обычным текстовым редактором. Затем пользователь должен вызвать программу отправки почты, которая посылает сообщение на почтовый сервер отправителя. Тот в свою очередь посылает его на почтовый сервер адресата, где специальная программа занимается сортировкой почты и рассылкой ее по ящикам конечных пользователей. Почтовые серверы постоянно подключены к Сети, тогда как компьютеры участников переписки могут устанавливать соединение с ними по мере необходимости.

Основой любой почтовой службы является система адресов. Адрес e-mail состоит из двух частей: идентификатора пользователя, который записывается перед знаком «@» (коммерческое эй) и доменного адреса машины, который записывается после этого знака. Например, адрес электронной почты (e-mail): ipk@ipk.tambov.su.

Телеконференции – это электронная связь между двумя или более людьми на расстоянии. Можно выделить три основных типа:

1. Аудиотелеконференции по существу являются телефонными конференциями, поскольку участники связываются посредством телефонной техники с использованием наушников и микрофонов. Целесообразны при небольшом количестве участников (до 10-12 человек).

Пример – селекторные совещания.

2. Видеоконференция соединяет аудио- и видеосредства для обеспечения интерактивной голосовой коммуникации и обмена телевизионными изображениями. На экран дисплея может быть выведен любой материал, отснятый с помощью видеокамеры. Преимущество видеотелеконференции заключается в возможности передачи движущегося изображения. В учебном процессе используется для проведения лекций, консультаций в интерактивном режиме.

3. Компьютерные конференции позволяют нескольким участникам общаться друг с другом через компьютерные терминалы, однако не в режиме реального времени. Они подобны электронной почте, поскольку поступающие сообщения хранятся в компьютере и пользователь может прочитывать их и отвечать на них позже. Компьютерные конференции используются в преподавании учебных курсов, консультировании слушателей, курсантов в информационном обмене.

Базы и банки данных.

Под автоматизированным банком данных понимается организационно-техническая система, представляющая собой совокупность баз данных пользователей, технических и программных средств формирования и ведения этих баз и коллектива специалистов, обеспечивающих функционирование системы.

Основные функции банка данных:

адекватное информационное отображение предметной области;

обеспечение хранения, обновления и выдачи необходимых данных пользователям.

Составными частями любого банка данных являются база данных, система управления базой данных (СУБД), администратор базы данных, прикладное программное обеспечение.

База данных – совокупность хранимых в памяти ЭВМ и специальным образом организованных взаимосвязанных данных, отображающих состояние предметной области.

2. КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-ТЕХНОЛОГИЙ. ОБСТОЯТЕЛЬСТВА, ПОДЛЕЖАЩИЕ УСТАНОВЛЕНИЮ

Криминалистическая характеристика хищений, совершенных с использованием интернет-технологий, отличается от уже известных преступных посягательств определенной спецификой. Основные структурные элементы преступлений данного вида обладают существенным своеобразием. В первую очередь выделяют следующие криминалистически значимые сведения:

- о личности правонарушителя;
- о мотивах и целях его преступного поведения;
- о типичных способах подготовки, совершения и сокрытия преступления;
- о времени, месте и обстановке посягательств.

Обстановка совершения хищений, совершенных с использованием интернет-технологий включает в себя материальные, производственные и социально-психологические факторы среды, в которой происходит преступное деяние. Она способна влиять на формирование всех остальных элементов криминалистической характеристики преступления рассматриваемой категории, определять особенности поведения преступника и потерпевшей стороны.

Наиболее важными компонентами обстановки подготовки, исполнения и сокрытия преступления в данном случае являются специфические условия деятельности потерпевших сторон (физических и юридических лиц) и среди них следующие объективные:

- вид деятельности или род занятия (сфера деятельности - хозяйственная, коммерческая, управленческая, производственная, информационная, посредническая, финансовая, топливно-энергетическая, транспортная, услуг и т.д.);
- форма собственности предприятия или физического лица, правовой режим отдельных видов имущества, в т.ч. информации и информационных ресурсов;
- назначение и структура организации производственного процесса, характер потребляемых ресурсов и выпускаемой продукции (в т. ч. и интеллектуальной);
- система учета и отчетности;

- кадровое и материально-техническое обеспечение;

- вид используемых СВТ, связи и телекоммуникаций, их тактико-технические данные и конструктивное несовершенство;

- погодные условия;

- наличие необходимых помещений и оборудования;

- порядок отпуска и реализации продукции, ценностей;

- наличие и техническое состояние средств учета, защиты информации, охраны и т. д.

К субъективным условиям относятся такие факторы социально-психологического и организационно-управленческого характера, как:

- отступление от технологических режимов обработки информации, правил производства, проведения пусконаладочных, ремонтных, регламентных (техническое обслуживание) работ, эксплуатации СВТ, а также учета, хранения, распределения и расходования ценностей;

- несовершенство этих правил;

- отсутствие или несовершенство средств защиты информации;

- нарушение правил работы с охраняемой законом компьютерной информацией;

- необоснованность использования СВТ в конкретных технологических процессах и операциях;

- неудовлетворительная организация производственных процессов, наличие одновременно ручных и автоматизированных этапов обработки документов;

-психологически неправильные межличностные взаимоотношения руководителей с подчиненными и другими работниками и т. д.

Субъективные факторы могут существенно влиять на обстановку совершения хищений и определенным образом формировать ее. Существенным компонентом криминалистической характеристики преступлений, связанных с использованием СВТ, являются сведения об особенностях личности правонарушителя.

На жаргонном языке компьютерных правонарушителей называют:

• «хакерами» (от английского слова «hacker») – пользователь ЭВМ, системы ЭВМ или их сети, занимающийся поиском способов получения несанкционированного доступа к средствам электронно - вычислительной техники и охраняемой законом компьютерной информации;

• «крэкерами» (от английского слова «cracker») – пользователь ЭВМ, системы ЭВМ или их сети, занимающийся «взломом» (модификацией, блокированием, уничтожением) программно-аппаратных средств защиты компьютерной информации, охраняемых законом;

• «фрэкерами» (от английского слова «phreacker») – субъект, специализирующийся на совершении преступлений в области электросвязи с использованием конфиденциальной компьютерной информации.

Данные лица обычно обладают достаточно высокими специальными познаниями и практическими навыками в области новых компьютерных технологий. Как правило, это увлеченные компьютерной техникой школьники, студенты и молодые специалисты, совершенствующиеся в этом виде деятельности.

По последним данным, хакеры в России объединены в региональные группы, издают свои электронные средства массовой информации (газеты, журналы, электронные доски со срочными объявлениями), проводят электронные конференции, имеют свой жаргонный словарь, который постоянно пополняется и распространяется с помощью компьютерных бюллетеней. В таких «литературных» источниках имеются все необходимые сведения для повышения мастерства начинающего правонарушителя - методики и конкретные способы совершения и сокрытия хищений, от самых простых и до очень изощренных и сложных. Российские хакеры тесно контактируют с зарубежными, обмениваются с ними опытом по глобальным телекоммуникационным каналам электросвязи.

Возраст преступников колеблется от 15 до 45 лет. Например, по данным некоторых исследователей, на момент совершения преступления возраст 33% преступников не превышал 20 лет, 13% - старше 40 лет и 54% - 20-40 лет.

Стоит подчеркнуть, что 87% преступников - это служащие предприятий, учреждений и организаций, в которых было совершено преступление.

Характерные мотивы и цели хищений, совершенных с использованием интернет-технологий, следующие:

- незаконное получение денег, ценных бумаг, кредита, материальных ценностей, товаров, услуг, привилегий, льгот, квот, недвижимости, топливно-сырьевых и энергетических ресурсов, стратегического сырья;

- уклонение от уплаты налогов, платежей, сборов и т. п.;

- легализация (отмывание) преступных доходов;

- подделка или изготовление поддельных документов, штампов, печатей, бланков, денежных билетов в корыстных целях;

- получение конфиденциальнойльной информации в корыстных или политических целях;

- месть на почве личных неприязненных отношений с администрацией или сослуживцами по работе;

- дезорганизация валютной системы страны в корыстных или политических целях;

- дестабилизация обстановки в стране, территориально-административном образовании, населенном пункте (в политических целях);

- дезорганизация работы учреждения, предприятия или системы с целью вымогательства, устранения конкурента или в политических целях;

- стремление скрыть другое преступление;

- хулиганские побуждения и озорство;

- исследовательские цели;

- демонстрация личных интеллектуальных способностей или превосходства.

Время совершения преступлений рассматриваемой категории лишь в относительно редких случаях устанавливается с точностью до дня и очень редко - до часов и минут. Такая точность обычно требуется при выявлении отдельных эпизодов преступной деятельности. Как правило, время совершения данных преступных деяний исчисляют различными по продолжительности периодами, связанными с деятельностью определенных лиц или организаций. При этом согласно ч. 2 ст. 9 УК РФ временем совершения каждого преступления признается время окончания общественно опасного деяния независимо от момента наступления последствий.

Местом совершения хищений, совершенных с использованием интернет-технологий, являются как конкретные точки и участки территории, так и те учреждения, организации, предприятия и системы, в которых используется то или иное средство электронно-вычислительной техники в каком-либо технологическом процессе. Следовательно, по делам данной категории мест совершения преступных посягательств может быть несколько, в том числе значительно удаленных друг от друга и расположенных как в разных странах, так и на различных континентах. Последнее возможно по причине практически неограниченного радиуса

действия и мобильности электронных средств связи и телекоммуникаций, неотъемлемой частью которых являются СВТ.

Ярким примером этому может служить одно из уголовных дел, расследование которого осуществлялось отечественными правоохранительными органами в тесном контакте с правоохранительными органами США. Уголовное дело было возбуждено в отношении 13 граждан Российской Федерации и Нидерландов, которые вступили в сговор с целью похищения денежных средств в крупных размерах, принадлежащих «City Bank of America», расположенному в Нью-Йорке. Образовав устойчивую преступную группу, они в период с конца июня по сентябрь 2011 года, используя электронную компьютерную систему телекоммуникационной связи ИНТЕРНЕТ и преодолев семь рубежей многоконтурной защиты от несанкционированного доступа, с помощью персонального компьютера из офиса АО «Сатурн», находящегося в городе Санкт-Петербурге, вводили в систему управления наличными фондами указанного банка ложные сведения. В результате этих действий преступники осуществили около 40 переводов денежных средств на общую сумму 10 млн 700 тыс. 952 доллара США со счетов клиентов названного банка, находящихся в 9 странах мира, на счета лиц, входящих в состав преступной группы и проживавших в 7-ми других странах - США, Финляндии, Израиле, Швейцарии, Германии, России и Нидерландах.

Важнейшим и определяющим элементом криминалистической характеристики любого, в том числе и компьютерного преступления, является совокупность данных, характеризующих способ его совершения.

Все способы подготовки, совершения и сокрытия хищений, совершенных с использованием интернет-технологий, имеют свои индивидуальные, присущие только им признаки, по которым их можно распознать и классифицировать в отдельные общие группы. При этом в качестве основного классифицирующего признака выступает метод, с помощью которого преступником осуществляется целенаправленное воздействие на средства вычислительной техники и компьютерную информацию. Выделяют следующие общие группы:

Изъятие СВТ;

Перехват информации;

Несанкционированный доступ к СВТ и компьютерной информации;

Манипуляция данными и управляющими командами;

Комплексные методы.

К первой группе относятся традиционные способы совершения преступлений, в которых действия преступника направлены на изъятие чужого имущества. Под чужим имуществом в данном случае понимается любое СВТ. С уголовно-правовой точки зрения подобные преступные деяния будут квалифицироваться по совокупности соответствующими статьями УК Российской Федерации. Например, как свидетельствуют материалы одного из уголовных дел, в г. Волжском Волгоградской области преступники, перепилив с помощью ножовки по металлу прутья оконных металлических решеток, проникли в 3.00 час. в необорудованный охранной сигнализацией операционный зал Сбербанка, откуда похитили два системных блока персональных компьютеров стандартной конфигурации, содержащих в своей постоянной памяти сведения на всех вкладчиков - физических и юридических лиц, кредиторов - с полными установочными данными. Такой способ совершения компьютерного преступления достаточно прост и традиционен и относится к рассматриваемой группе, как и те, которые связаны с противоправным изъятием различных физических носителей ценной информации - дискет, оптических и магнитооптических компакт-дисков,

пластиковых карт, интегральных микросхем и т. п.

Ко второй группе способов совершения хищений относятся те, которые основаны на получении преступником компьютерной информации посредством использования методов аудиовизуального и электромагнитного перехвата, широко практикуемые в оперативно-розыскной деятельности. К ним, в частности, относятся:

1. Пассивный (бесконтактный) перехват, осуществляемый путем дистанционного перехвата электромагнитных излучений, испускаемых при работе СВТ:

- перехват оптических сигналов (изображений) в видимом, инфракрасном (ИК) и ультрафиолетовом (УФ) диапазонах волн (осуществляется преступником с помощью оптических, оптикоэлектронных, телевизионных, тепловизионных, лазерных, фото- и других визуальных средств съема информации);

- перехват акустических сигналов, распространяющихся в воздушной, водной и твердой средах (осуществляется с использованием акустических, гидроакустических, виброакустических, лазерных и сейсмических средств;

- перехват электромагнитных сигналов, распространяющихся по техническим каналам основных и вспомогательных средств и систем в виде паразитных информативных физических полей: побочных электромагнитных излучений и наводок (ПЭМИН), паразитных модуляций ВЧ сигналов, паразитных информативных токов и напряжений, образуемых за счет эффекта электроакустического преобразования сигналов в сетях электросвязи, электрификации, электрочасофикации, охранно-пожарной сигнализации, в сетях СВТ, в блоках СВТ и т.п.

2. Активный (контактный) перехват, осуществляемый путем непосредственного подключения к СВТ или системе передачи данных с помощью различных штатных оперативно-технических и специально изготовленных, разработанных, приспособленных и запрограммированных средств негласного получения информации, иногда с использованием скрытых (замаскированных, зашифрованных) каналов. В данном случае преступник может целенаправленно воздействовать на СВТ в целом, на его составляющие, на систему санкционирования доступа, на каналы передачи данных и на саму компьютерную информацию.

К третьей группе относятся способы совершения компьютерного преступления, направленные на получение преступником несанкционированного доступа к СВТ, например, с использованием метода легендирования («электрик», «сантехник», «мастер по ремонту телефонов», «сотрудник рекламного агентства», «сотрудник сервисной обслуживающей организации» и т.п.), а также путем несанкционированного подключения к системе передачи компьютерной информации с целью перехвата управления вызовом абонента сети «на себя» и т. п.

Четвертая группа - это действия преступника, связанные с использованием методов манипуляции входными-выходными данными и управляющими командами средств вычислительной техники. Они используются часто и достаточно хорошо известны сотрудникам подразделений по борьбе с экономическими преступлениями, например, осуществление подмены входных и выходных данных бухгалтерского

учета в процессе автоматизированной обработки документов или внесение умышленного изменения в существующую программу, заведомо приводящего к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. В качестве наглядных примеров можно привести такие способы, как «троянский конь», «троянская матрешка», «салями», «воздушный змей», «временная» или «логическая бомба», «люк», «компьютерный вирус» и т. п.

К пятой группе относятся комплексные способы совершения компьютерного преступления, основанные на применении преступником двух и более способов различных групп, причем один из них всегда используется как основной, а другие выполняют вспомогательные функции, например, сокрытие следов преступления.

Обобщение практики расследования хищений позволяет выделить следующие основные обстоятельства, подлежащие обязательному установлению и доказыванию по делам рассматриваемой категории:

1. Наличие преступления (либо это правонарушение иного рода); непосредственная причина (причины) нарушения безопасности компьютерной информации и орудий ее обработки; не является ли происшедшее следствием непреодолимых факторов.

2. Объект преступного посягательства (данное обстоятельство имеет решающее значение для применения следователем той или иной методики расследования конкретного преступления или их совокупности).

3. Предмет преступного посягательства.

4. Способ совершения преступления.

5. Наименование и назначение объекта, где совершено преступление.

6. Конкретное место совершения преступления в данном предприятии, учреждении, организации, на участке местности; наличие иных мест совершения преступления (было ли преступление совершено дистанционно, вне помещения - по каналам электросвязи и локальной вычислительной сети).

7. Режим работы объекта.

8. Средства вычислительной техники и компьютерной информации, с помощью которых совершено преступление (тип, вид, модификация, функциональное назначение, техническое состояние и другие

характеристики). Конкретный терминал или участок сети (абонентский номер, код, шифр, рабочая частота).

9. Режим работы СВТ.

10. Возможность утечки конфиденциальной информации.

11. Период (дата, время) совершения преступления.

12. Размер материального ущерба, из чего он складывается.

13. Служебные действия и операции технологического процесса, с которыми связано преступление; перечень должностных лиц или работников, несущих ответственность и имеющих непосредственное отношение к данным действиям (операциям) в силу технологии производства или командно-административного управления.

14. Мотив совершения преступления (корысть, месть, хулиганские побуждения, демонстрация личных интеллектуальных способностей, с целью сокрытия другого преступления и др.); цели, преследуемые и достигнутые преступником; наличие у преступника в момент совершения преступления состоянии внезапно возникшего сильного душевного волнения, аффекта, либо психического заболевания (информационного невроза или компьютерной фобии).

15. Субъект преступления, его характеристика. Если преступление совершено группой лиц, анализ ее состава и роли каждого соучастника.

16. Наличие причинной связи деяний с наступившими последствиями. Необходимо проверить и доказать, что именно деяния данного лица и обязательно те, которые ему инкриминируются, являются причиной наступивших последствий, например, наличие минимально необходимых специальных познаний у преступника.

17. Причины и условия, способствовавшие подготовке, совершению и сокрытию преступления; факторы, усугубившие их проявление (нарушения нормативных актов, положений, инструкций, правил, организации работы другими лицами, кем именно и по каким причинам; не подлежат ли они привлечению к уголовной ответственности за допущенные нарушения, способствовавшие совершению расследуемого преступления, например, по ст. 274 УК РФ).

3. ТИПИЧНЫЕ СЛЕДСТВЕННЫЕ СИТУАЦИИ И ДЕЙСТВИЯ СЛЕДОВАТЕЛЯ НА ПЕРВОНАЧАЛЬНОМ ЭТАПЕ РАССЛЕДОВАНИЯ ХИЩЕНИЙ С ПОМОЩЬЮ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

Раскрывать преступления, совершаемые с использованием средств электронно-вычислительной техники, сложно, т. к. нередко преступники прибегают к различным уловкам, маскируют свои преступные деяния многочисленными объективными и субъективными причинами, которые действительно могут иметь место. К ним, как правило, относятся следующие:

1. Естественные:

- стихийные бедствия, природные явления (пожары, землетрясения, наводнения, ураганы, смерчи, тайфуны, циклоны и т.п.);

- самопроизвольное разрушение элементов, составляющих СВТ.

2. Обусловленные неумышленной деятельностью человека вследствие непреодолимых факторов:

- ошибки при создании (изготовлении) СВТ (недочеты проектирования, в т. ч. системы защиты, кодирования информации, в изготовлении элементов СВТ);

- ошибки в процессе работы (эксплуатации) СВТ (неадекватность концепции обеспечения безопасности СВТ; недочеты управления системой защиты, ошибки персонала, сбои и отказы оборудования и программного обеспечения, ошибки при производстве пусконаладочных и ремонтных работ).

Эти ошибки часто используются преступниками в личных корыстных целях для прикрытия преступных деяний, поэтому в процессе расследования разграничить административные правонарушения и преступления бывает нелегко.

Поводами и основаниями для возбуждения уголовных дел о преступлениях в сфере компьютерной информации чаще всего служат:

- заявления граждан (конкретных потерпевших);

- сообщения с предприятий, учреждений, от организаций и должностных лиц (базирующиеся, как правило, на материалах контрольно-ревизионных проверок и сообщениях служб безопасности);

- сведения, полученные в результате проведения оперативно-розыскных мероприятий;

- статьи, заметки и письма, опубликованные в средствах массовой информации;

- непосредственное обнаружение следователем, прокурором или судом признаков преступления.

Обычно возбуждению уголовного дела предшествует предварительная проверка материалов, поступивших в правоохранительные органы. В связи с этим, следователь может заблаговременно ознакомиться с собранными по делу материалами, совместно с оперативными сотрудниками выбрать в тактическом отношении наиболее оптимальный момент для возбуждения дела, а также определить характер и последовательность первоначальных следственных действий, организационных и иных мероприятий. Как показывает практика, успех расследования преступления, связанного с использованием СВТ, обеспечивают быстрота и решительность действий следователя в самые первые часы производства по делу, организованное взаимодействие с оперативными подразделениями, а также наличие специалиста в области СВТ.

Например, в отдельных случаях оперативные работники должны выяснить (проверить) некоторые конкретные вопросы и материалы, произвести задержание преступника, выполнить другие мероприятия оперативного характера. Промедление при этом недопустимо, т. к. может привести к утечке информации, утрате материальных следов, уничтожению документов и идентификационных признаков предметов, которые в дальнейшем могут использоваться в качестве вещественных доказательств.

В ходе предварительной проверки материалов при решении вопроса о возбуждении уголовного дела следователь должен прежде всего получить четкое и полное представление о характере деятельности и структуре объекта, где, возможно, было совершено преступление, изучить конкретные условия его деятельности, существующий там порядок учета и отчетности, систему товаро- и документооборота, коммуникативные и иные тактико - технические характеристики используемой компьютерной техники, организацию охраны информации. Необходимо также хорошо

знать служебные обязанности лиц, имеющих прямые или косвенные отношения к ценностям, которые стали предметом правонарушения.

Для того чтобы детально разобраться в особенностях деятельности потерпевшей стороны (физического или юридического лица), следователю необходимо ознакомиться с соответствующей справочной литературой, изучить ведомственные нормативные акты. Исключительно важное значение при расследовании хищений имеют консультации со специалистами, в качестве которых могут выступать любые лица, обладающие необходимыми знаниями и опытом. Как правило, ими могут быть квалифицированные работники различных организаций, осуществляющих свою деятельность в области компьютерных и телекоммуникационных технологий, но большее предпочтение следует отдавать сотрудникам Государственной технической комиссии при Президенте Российской Федерации, действующей на основании Указа Президента Российской Федерации № 9 от 5.01.92 г. «О создании Государственной технической комиссии при Президенте Российской Федерации»; Федерального агентства правительственной связи и информации (ФАПСИ).1

Тактика и последовательность проведения первоначальных следственных действий, оперативно-розыскных и организационных мероприятий зависят от сложившейся следственной ситуации. По делам рассматриваемой категории можно выделить следующие исходные следственные ситуации:

I. Информация о причинах возникновения общественно опасных деяний, способе их совершения и личности правонарушителя отсутствует.

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

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

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

1. Допрос заявителя или лиц, на которых указано в исходной информации как на возможных свидетелей.

---

[1] Закон Российской Федерации «О федеральных органах правительственной связи и информации» // Ведомости Верховного Совета РФ. 1993. № 12.

2. Решение вопроса о возможности задержания преступника с поличным и о необходимых в связи с этим мероприятиях.

3. Вызов необходимых специалистов для участия в осмотре места происшествия.

4. Осмотр места происшествия.

5. Проведение оперативно-розыскных мероприятий в целях установления причин совершения преступления, выявления лиц, виновных в его совершении, обнаружения следов и других вещественных доказательств.

6. Выемка и последующий осмотр средств электронно-вычислительной техники, предметов, материалов и документов (в т. ч. находящихся в электронной форме на машинных носителях информации), характеризующих производственную операцию, в ходе которой, по имеющимся данным, совершены преступные действия.

7. Допросы свидетелей (очевидцев).

8. Допросы подозреваемых (свидетелей), ответственных за данный участок работы, конкретную производственную операцию и защиту конфиденциальной информации.

9. Обыски на рабочих местах и по месту проживания подозреваемых.

10. Назначение программно-технической, радиотехнической, технической, бухгалтерской и иных экспертиз.

Дальнейшие действия планируются с учетом дополнительной информации.

Для третьей следственной ситуации может быть предложена следующая программа расследования и действий следователя на первоначальном этапе:

1. Изучение поступивших материалов с позиций их полноты, соблюдения норм уголовно-процессуального законодательства и порядка передачи в органы следствия. При необходимости принятие мер к получению недостающей информации.

2. Возбуждение уголовного дела.

3. Вызов необходимых специалистов для участия в осмотре места происшествия.

4. Осмотр места происшествия.

5. Личные обыски задержанных, их рабочих мест и места проживания.

6. Допрос подозреваемых.

7. Выемка и осмотр вещественных и письменных доказательств.

8. Изъятие и осмотр подлинных документов, удостоверяющих личность задержанных, а также документов, характеризующих те производственные операции, в процессе которых допущены нарушения и преступные действия (в т. ч. и тех документов, которые находятся в электронной форме на машинных носителях информации).

9. Допрос лиц, названных в документах, переданных в следственные органы, как допустивших нарушения, ответственных за работу (денежные средства, материальные ценности, услуги и т. п.) по фактам установленных нарушений.

10. Истребование, а при необходимости производство выемки нормативных актов и документов, характеризующих порядок и организацию работы в данном подразделении (в т. ч. с конфиденциальной информацией, бланками строгой отчетности, использование СВТ и т. п.).

11. Допрос свидетелей, причастных к соответствующим производственным операциям или подозреваемых в связях с лицами, совершившими преступные действия.

12. Анализ полученной информации и решение вопроса о необходимости назначения экспертиз, проведения ревизии или проверки, в т. ч. повторной (по каким позициям, за какой период и с участием каких специалистов).

При выполнении вышеуказанных программ следует учитывать особенности методики расследования конкретного вида преступления, о совершении которого выдвинуты версии.

4. ОСОБЕННОСТИ ТАКТИКИ ПРОИЗВОДСТВА СЛЕДСТВЕННЫХ ДЕЙСТВИЙ И ОРГАНИЗАЦИОННЫХ МЕРОПРИЯТИЙ

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

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

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

4.1. Осмотр места происшествия

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

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

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

- специалист по СВТ;

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

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

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

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

- участковый инспектор, обслуживающий данную территорию;

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

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

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

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

2. Определить последовательность действия лиц при осмотре места происшествия;

3. Пригласить соответствующих квалифицированных специалистов;

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

5. Провести подбор и инструктаж понятых, в качестве которых целесообразнее привлекать лиц, обладающих минимально необходимыми знаниями в области СВТ и компьютерных технологий, разъяснить их права и обязанности.

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

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

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

- территория места происшествия;

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

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

Следователю необходимо знать, что к изменению или уничтожению информации (следов) может привести не только работа за пультом управления СВТ (клавиатурой), но и включение-выключение СВТ или разрыв соединения между ними. Поэтому если на момент производства следственного действия какие-либо СВТ и иные электротехнические приборы и оборудование были включены или выключены, то они должны оставаться в таком состоянии до момента окончания осмотра их специалистом.

2. Опросить потерпевшего, материально ответственное лицо и очевидцев (операторов СВТ) об изменениях, внесенных в обстановку, о категории обрабатываемой информации (общедоступная или конфиденциальная), а также о действиях потерпевшего до прибытия СОГ. Вопросы необходимо конкретизировать по мере детального осмотра места происшествия, поиска следов и других вещественных доказательств.

В протоколе осмотра следует отразить следующие фактические данные:

- наименование и назначение объекта, где совершено преступление;

- территориальное расположение объекта осмотра (на улице, в помещении, в банке, в магазине, на автостоянке, бензоколонке, станции метро, в ресторане, гостинице, помещении кассы, на складе, вокзале, контрольно-пропускном пункте и т. д.) и его ориентация относительно сторон света;

- ближайшее окружение объекта и подступы к нему - здания, технические сооружения, площади, зоны, участки (производственные, административные, жилые) и расстояние до них; наличие дорог, подъездных путей (в т. ч. и водного транспорта), парковок и автостоянок;

наличие линий и пунктов (колодцев, концентраторов, коробов, потерн и т. д.) инженерно-технических коммуникаций (электросвязи, электропередачи, тепло- , водо- и газоснабжения, вентиляции и т. д.);

- технические и конструктивные особенности местности, связанные с установкой и эксплуатацией СВТ (этажность, материал стен и других строительных конструкций, форма строения, наличие дверей, окон, ограждений, фальшполов и подвесных потолков, наличие и фактическое состояние устройств электропитания и др.);

- наличие, внешнее состояние и расположение охраны объекта, специальных защитных и сигнальных устройств от несанкционированного съема и утечки информации - постов охраны, охранно-пожарной сигнализации, контрольно-пропускных пунктов доступа лиц на данную территорию (неавтоматический, полуавтоматический или автоматический), освещения, металлических решеток, штор, жалюзи, рольставен, замков и запорных механизмов, экранов, заземлений, специальных стекол и пленок, генераторов шума, фильтров и т. д.;

- расположение СВТ относительно вентиляционных и иных отверстий в строительных конструкциях, дверных и оконных проемов, технических средств видеонаблюдения, а также других рабочих мест (если таковых несколько в одном помещении);

- расположение в одном помещении вместе с СВТ других электрических устройств и приборов - телефонных и иных аппаратов электросвязи, систем электрочасофикации, оргтехники (ксероксов, аудио-, видеомагнитофонов, автоответчиков, электрических пишущих машинок и т. п.), приборов электроосвещения (настольных, напольных, настенных, потолочных, подвесных и т. д.), абонентских громкоговорителей, телевизоров и мониторов, радиоприемников и магнитол, электроплиток, печей, чайников, кондиционеров и т. д.;

- наличие в одном помещении со СВТ линий, пунктов, разъемов промежуточных и оконечных устройств систем инженерно-технических коммуникаций (электросвязи, электропередачи, антенн-проводов, тепло- , водо- и газоснабжения);

- наличие или отсутствие технических средств сопряжения СВТ с каналами электросвязи и между собой (на это могут указывать кабели и

провода, которыми СВТ соединены между собой, а также с аппаратами или линией электросвязи);

- наличие или отсутствие соединений СВТ с оборудованием или вычислительной техникой, находящейся вне территории (помещения) осмотра; на это могут указывать кабели и провода, идущие от осматриваемого СВТ за границу места осмотра (в другие помещения или здания) либо к аппаратам внутренней связи (в этом случае граница осмотра места происшествия значительно расширяется);

- наличие на объекте, путях подхода и отхода следов преступления и преступника, специфическими среди которых являются: следы орудий взлома, повреждения, уничтожения и/или модификации охранных и сигнальных устройств; показания регистрирующей (электронный журнал) или специальной мониторинговой (тестовой) аппаратуры; следы пальцев рук на СВТ, охранных и сигнальных устройствах, на их клавиатуре, соединительных и электропитающих проводах и разъемах, на розетках и штепсельных вилках, тумблерах, кнопках и рубильниках, включающих СВТ и электрооборудование; остатки соединительных проводов и изоляционных материалов, капли припоя, канифоли или флюса; следы проплавления, прокола, надреза изоляции проводов СВТ, наличие участков механического сдавливания и приклеивания сторонних предметов;

- наличие или отсутствие учетно-справочной документации к СВТ - технического паспорта и подобного ему документа; журнала оператора или протокола автоматической фиксации расчетно-кассовых и иных операций; журнала учета машинных носителей информации (МНИ), машинных документов, заказов (заданий или запросов); журнала (карточки) учета выдачи МНИ и машинных документов; журнала (карточки) учета массивов (участков, зон), программ, записанных на МНИ; журнала учета уничтожения брака бумажных МНИ и машинных документов; актов на стирание конфиденциальной информации, уничтожение машинных носителей с конфиденциальной информацией, конфиденциальных машинных документов.

4.2. Осмотр средства вычислительной техники

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

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

2. Выяснения обстановки происшествия для восстановления механизма совершения преступления;

3. Установления технического состояния СВТ.

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

- по обслуживанию и ремонту СВТ (для осмотра аппаратной части СВТ и соединительной арматуры; для ЭВМ - инженер-системотехник);

- в области сетевых технологий (для осмотра СВТ, используемых в системах дистанционной передачи данных - компьютерных сетях, периферийного оборудования удаленного доступа, удаленных терминалов);

- по средствам связи и телекоммуникациям (для осмотра оборудования электросвязи, используемого для передачи компьютерных данных и команд, а также СВТ, являющихся средствами связи);

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

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

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

Отметим, что во избежание уничтожения (повреждения) СВТ и следов преступления при работе специалиста - криминалиста по осмотру СВТ недопустимо использование магнитосодержащих материалов, инструментов, приборов и оборудования, направленных источников электромагнитного излучения (магнитного порошка, магнитной кисточки, электромагнита, металлодетектора, мощных ламп освещения, мощных УФ и ИК излучателей и т. д.), а также кислотно-щелочных материалов и нагревательных приборов. При осмотре места происшествия и при производстве других следственных действий вышеуказанными материалами и оборудованием можно пользоваться с особой осторожностью на расстоянии более 1 метра от СВТ и их соединительных проводов.

В протоколе осмотра СВТ фиксируются следующие данные:

- тип, марка, конфигурация, цвет и заводской номер (или инвентарный, учетный номер) изделия;

- тип (назначение), цвет и индивидуальные признаки соединительных и электропитающих проводов;

- состояние СВТ на момент проведения осмотра (выключено или включено);

- техническое состояние - внешний вид, целостность корпуса, комплектность СВТ - наличие и работоспособность необходимых блоков, узлов, деталей и правильность их соединения между собой, наличие расходных материалов, тип используемого машинного носителя информации и т. д. (проверку проводит соответствующий специалист);

- тип источника электропитания, его тактико-технические характеристики и техническое состояние (рабочее напряжение, частота тока, рабочая нагрузка, наличие предохранителя, стабилизатора, сетевого фильтра, количество подключенных к нему электроприборов, число разъемов - розеток и т. д.);

- наличие заземления («зануления») СВТ и его техническое состояние;

- наличие и техническая возможность подключения к СВТ периферийного оборудования и/или самого СВТ к такому оборудованию

либо к каналу электросвязи (определяется специалистом по наличию у СВТ соответствующих портов и разъемов);

- повреждения, не предусмотренные 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 машинном носителе информации 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 основные действия, производимые специалистом при осмотре СВТ (порядок нажатия на клавиши и запорные механизмы, корректного приостановления работы и закрытия исполняемой операции или программы, выключения СВТ, отключения от источника электропитания, рассоединения или соединения СВТ и ее составляющих, отсоединения

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

4.3. Осмотр машинного носителя информации (МНИ)

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

Осмотр МНИ производится с участием специалиста и начинается с определения типа, вида, назначения, технических параметров и ознакомления с его содержанием.

К машинным носителям информации относятся:

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

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

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

- пластиковые карты (карточки);

- интегральные микросхемы (ИМС) в виде оперативной памяти (ОЗУ) и/или постоянного запоминающего устройства (ПЗУ), в т. ч. находящиеся в различных СВТ (персональных компьютерах, пейджерах, сотовых и иных аппаратах электросвязи, электронных записных книжках, электронных переносных справочниках и переводчиках, контрольно-кассовых аппаратах, банкоматах, контрольно-пропускных устройствах, смарт-картах и т. д.).

В протоколе осмотра должны быть зафиксированы следующие фактические данные:

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

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

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

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

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

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

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

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

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

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

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

12. Ссылка на то, что используемые в процессе осмотра СВТ перед началом следственного действия были тестированы специалистом на предмет отсутствия в них вредоносных программных и аппаратных средств.

Примечания:

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.

4.4. Осмотр машинного документа

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

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

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

Документы, используемые в документообороте юридических лиц (учреждений, организаций, предприятий и т. д.), могут создаваться как для внешнего, так и внутреннего пользования. Однако в соответствии с требованиями ГОСТ 6.38-72 «Система организационно - распорядительной документации. Основные положения» рассматриваемые документы должны всегда иметь следующие реквизиты: наименование юридического лица, выдавшего (или создавшего) документ; номер документа и дата его составления; заголовок; адресат; содержание; подпись и печать на документах, требующих особого удостоверения их подлинности (или код лица, утвердившего документ).

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

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

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

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

В протоколе осмотра документа должны быть отражены следующие данные:

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

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

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

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

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

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

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

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

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

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

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

12. Какими реквизитами заверен (ЭЦП; кодом (позывным) лица, ответственного за правильность изготовления, копирования или передачу документа по телекоммуникационным каналам; собственноручной подписью уполномоченного лица; печатью; индивидуальным кодом абонента сети дистанционной передачи данных - «электронной почты»; специальным позывным кодом аппаратуры связи).

13. Индивидуальные признаки документа (название файла - программы); структура расположения символов; машинный формат текста (формат MS DOS, WORD for WINDOWS и т. д.); наличие маркеров страниц, выделений текста; тип и цвет печати (матричный, струйный, электрографический, смешанный) указать конкретно для каждого элемента; наличие защитных знаков и т. д.).

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

Примечания:

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.

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.

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.

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

4.5. 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:

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

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

- определено и корректно приостановлено выполнение вычислительной операции;

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

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

- выключено электропитание СВТ и всех его периферийных устройств;

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

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

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

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

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

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

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

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

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

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

носителей информации, то всегда составляется опись вложения с указанием индивидуальных признаков каждого носителя.

5. Недопустимо приклеивать что-либо непосредственно к МНИ и документам, пропускать через них бечеву, пробивать стиплером, делать пометки или маркировки, накалывать твердым предметом знаки, использовать пластилиновые или сургучовые печати и т. д.

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

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

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

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

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

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

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

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

- В протоколе следственного действия должны обязательно фиксироваться конкретные признаки изымаемых СВТ (марка, быстродействие, марка процессора, объем памяти и т. д.).2

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 предме-

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

тов, на которых имеются повреждения и следы, и с обязательным использованием фото- и/или видеосъемки. Важно сфотографировать или произвести видеозапись не только места происшествия, отдельных объектов, СВТ и их соединений, но и все действия специалистов, участвующих в осмотре.

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

4.6. 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 - комби-

нированные) и расположение пунктов обесточивания помещения и аппаратуры, подлежащих обыску;

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

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

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

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

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

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

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

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

- при оказании сопротивления со стороны лиц, находящихся на объекте обыска, - обыскиваемого, его родственников, охранников (сторожей), сотрудников организации и т. п. - принять срочные меры по нейтрализации противодействия и скорейшему проникновению в обыскиваемое помещение;

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

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

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

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

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

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

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

На обзорной стадии обыска необходимо:

1. Определить и отключить специальные средства защиты информации и СВТ от несанкционированного доступа, особенно те, которые автоматически уничтожают информацию и МНИ при нарушении процедуры доступа к СВТ и машинной информации, порядка их использования

и/или установленных правил работы с ними; принять меры к установлению пароля, ключа санкционированного доступа и шифрования-дешифрования информации.

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

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

Следователь должен знать, что при наличии соединения СВТ с другим оборудованием и электронно-вычислительной техникой, находящимися вне периметра обыскиваемой зоны (в другом помещении, здании, населенном пункте и т. д.), существует реальная возможность непосредственного доступа к машинной информации и совершения любых действий с ней и СВТ (стирание, уничтожение, модификация, копирование, блокирование, нарушение работы). Для предотвращения этого необходимо, в зависимости от ситуации и рекомендаций специалиста, временно или на длительный срок, частично или полностью отключить СВТ или локальную вычислительную сеть целиком от технических устройств, находящихся за периметром обыскиваемой зоны. Отключение может

быть произведено как на программном, так и аппаратном уровне. Если СВТ работает в режиме «электронной почты», то предпочтительнее оставить его до конца обыска в работающем состоянии в режиме «приема почты», исключив возможность какой-либо обработки и передачи информации. Эту работу может сделать только квалифицированный специалист. Все выполняемые им действия должны быть зафиксированы с помощью видеозаписи и отражены в протоколе обыска.

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

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

4. При обследовании персонального компьютера необходимо:

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

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

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

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

Следователю стоит придерживаться следующих рекомендаций:

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

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

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

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

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

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

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

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

4.7. Назначение экспертиз

Глава 27 УПК РФ определяет использование необходимых специальных познаний в науке, технике, искусстве или ремесле при производстве дознания, предварительного следствия и при судебном разбирательстве.

По делам рассматриваемой категории в процессе расследования существует постоянная необходимость использования 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 компьютерно - технических.

В настоящее время с их помощью можно решать следующие задачи:

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

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

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

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

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

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

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

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

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

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

- выяснять причины и условия, способствующие совершению правонарушения, связанному с использованием СВТ.[3]

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

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

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

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

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

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

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

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

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

21. Какой материальный ущерб причинен потерпевшему?

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

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

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

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

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

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

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

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

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

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

- обстоятельства уголовного дела;
- сведения о лицах, причастных к совершению преступления;
- документы, сведения о которых могут содержаться на машинных носителях, представляемых на исследование;
- сведения, которые могут быть использованы в качестве «ключевых» слов при восстановлении и/или поиске экспертом информации (например, названия фирм, учреждений и организаций, фамилии клиентов, предполагаемые номера счетов и т. д.).

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

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

Нередко в процессе расследования компьютерного преступления возникает необходимость в установлении этапов обработки бухгалтерских данных с использованием СВТ, на которых вносились те или иные изменения, а также признаков интеллектуального подлога в первичных и сводных бухгалтерских документах, составленных на ЭВМ; в определении фактов уменьшения облагаемой налогом прибыли, выявлении счетных работников, причастных к совершению компьютерного преступления, путем исследования носителей оперативной информации, а также лиц, вводивших соответствующие данные в ЭВМ, и т. д. Для этих целей необходимо использовать возможности судебно - бухгалтерской экспертизы, позволяющей при проведении исследований установить, насколько соблюдены те или иные требования положений о документах и документообороте в бухгалтерском учете при оформлении различных хозяйствен-

ных и иных операций первичными документами и отображении их в регистрах бухгалтерского учета и отчетности, в том числе выраженных в форме, зафиксированной на машинном носителе и машинограмме, созданных средствами компьютерной техники.

В случаях выявления нарушения этих нормативных документов эксперт-бухгалтер может установить их причины (не сделаны ли они с целью совершения преступления - злоупотребления, сокрытия недостачи материальных ценностей, уменьшения их размера и т. д.) и сделать вывод о том, насколько эти нарушения положений повлияли на состояние бухгалтерского учета и выполнение функций лицами, ответственными за это в управлении хозяйственной или иной деятельностью. При этом возможно установление лиц, ответственных за созданные или допущенные нарушения правил составления первичных документов и учетных регистров.4

Наиболее оптимальным вариантом в некоторых случаях является назначение комплексной компьютерно-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, в частности, технико - криминалистические экспертизы документов, созданных с использованием СВТ и новых репрографических технологий, и т. д.

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

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

---

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

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

3. В работе какого канала электросвязи используется данное устройство?

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

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

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

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

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

ЛИТЕРАТУРА

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

Белуха Н.Т. Судебно-бухгалтерская экспертиза/ Н.Т. Белуха. - М.: Дело, 2013. - 270 с.

Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / В.Б. Вехов; под ред. акад. Б.П. Смагоринского. – М.: Право и закон. 2013. 182 с.

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

Комиссаров А.Ю. Идентификация пользователя ЭВМ и автора программного продукта: методические рекомендации/ А.Ю. Комиссаров, А.В. Подлесный. – М.: ЭКЦ МВД России, 1996. - 40 с.

Лучин И.Н. Методические рекомендации по изъятию компьютерной информации при проведении обыска/ И.Н. Лучин, Н.Г. Шуруханов // Информационный бюллетень СК МВД России. - 2012. - № 4(89). - С. 22-28.

Ляпунов Ю. Ответственность за компьютерные преступления/ Ю. Ляпунов, В.Максимов // Законность. - 2013. - № 1. - С. 8-14.

Петрунев В.П. Процессуальные вопросы по оформлению машинных документов и использованию информации по уголовному делу, хранящейся в памяти ПЭВМ/ В.П. Петрунев, И.А. Котов // Применение ЭВМ в деятельности следователя. - М.: НИИ МВД России, 2012. - С. 27-36.

Россинская Е.Р. Судебная экспертиза в уголовном, гражданском, арбитражном процессе/ Е.Р. Россинская. – М.: Право и закон, 2013. - 224 с.

СЛОВАРЬ
специальных терминов

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

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

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

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

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

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

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

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

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

Гибкий магнитный диск (ГМД, или флоппи-диск) - сменный магнитный диск на гибком физическом носителе, используемый в персональной ЭВМ в качестве внешней памяти прямого доступа. Вы-

пускаются диски диаметром 200 мм (8 дюймов), 133 мм (5,25 дюйма) и 90 мм (3,5 дюйма).

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

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

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

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

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

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

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

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

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

Каталог (директорий) - справочник файлов и библиотек программ со ссылками на их расположение. Используется операционной системой для определения местоположения файла (библиотеки программ). Система

каталогов может включать главный (корневой) каталог и подкаталоги (поддиректории).

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

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

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

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

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

Криптография - метод шифрования и дешифрования данных.

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

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

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

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

Монитор - видеоконтрольное устройство.

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

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

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

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

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

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

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

Персональная ЭВМ (персональный компьютер) - универсальная микрокомпьютерная система, предназначенная для использования в автономном режиме, системе ЭВМ или их сети для решения задач

различной профессиональной ориентации, например, используемая в качестве рабочего места специалиста.

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

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

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

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

Программный модуль - единица программного обеспечения.

Пластиковая карта (карточка) - машинный носитель информации в форме прямоугольной пластины, выполненной из поливинилхлорида (ПВХ), полихлорвинила (ПХВ) либо из композиционного материала, одним из компонентов которого являются данные пластики. Пластиковая карта, как правило, имеет следующие линейные размеры - 85×54×0,76 мм.

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

Порт - многоразрядный вход или выход в техническом устройстве; точка взаимодействия двух технических устройств (например, ЭВМ с

принтером или ЭВМ с адаптером канала связи - модемом); конец логического канала.

Принтер - алфавитно-цифровое печатающее устройство.

Протокол - 1. Результат регистрации в хронологическом порядке информации о ходе вычислительного процесса.-

Протокол -2. В вычислительных сетях - совокупность семантических и синтаксических правил, определяющих работу функциональных устройств в процессе связи.

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

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

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

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

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

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

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

Спецификация - формализованное описание свойств, характеристик и функций объекта.

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

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

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

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

Телекоммуникация - дистанционная связь; дистанционная передача данных.

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

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

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

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

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

Файл - поименованная область во внешней памяти ЭВМ.

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

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

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

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

УЧЕБНОЕ ИЗДАНИЕ

РАССЛЕДОВАНИЕ ХИЩЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНТЕРНЕТ-ТЕХНОЛОГИЙ

Учебно-практическое пособие

Составитель И.Е. Мазуров

Под общей редакцией С.Я.Казанцева

Корректор О.Н. Хрусталева

Подписано в печать 28.09.2015
Формат 60х90 1/16 Усл. печ. л. 4,5 Тираж 30

Типография КЮИ МВД России
420108, г. Казань, ул. Магистральная, 35