**Саратовская государственная академия права**

# Кафедра криминалистики №1

**Учебная дисциплина –** Криминалистика

## Курсовая работа

на тему:

**Тактика и методика расследования преступления в сфере компьютерной информации**

**Выполнил:**

студент гр. 4.4. ЮИПА

***\*\*\*\*\*\*\*\*\*\****

**Проверил:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Саратов 2003 г.**

**СОДЕРЖАНИЕ**

Введение ………………………………………………………………… 3

1. Правовое регулирование отношений в области

компьютерной информации ……………………………………... 5

2. Общая характеристика преступлений в сфере

компьютерной информации ……………………………………... 9

3. Расследование преступления …………………………………….. 14

3.1. Фабула и предварительный план расследования ……………… 14

3.2. План расследования ……………………………………………… 17

3.3. Практические особенности отдельных следственных

действий …………………………………………………………... 18

3.4. Вынесение постановления о назначении необходимых

экспертиз …………………………………………………………. 27

Заключение ………………………………………………………………. 29

Библиография ……………………………………………………………. 31

**ВВЕДЕНИЕ**

В динамичных условиях XX в. общество постоянно сталкивается с проблемами различного характера, порождение которых зачастую вызвано стремлением общества к созданию более совершенных и эффективных моделей своего существования. Сказанное в полной мере относится и к такой специфической сфере, как область применения электронной техники и информационных технологий.

Создание электронно-вычислительной техники последних поколений с практически неограниченными возможностями, их широкое распространение в экономической, социальной и управленческой сферах, появление в быту значительного количества персональных ЭВМ явились не только новым свидетельством технического прогресса, но и с неизбежностью повлекли за собой и негативные последствия, связанные со злоупотреблениями при использовании средств ЭВМ и информационных технологий.

Обвальное появление в России большого числа персональных компьютеров импортного производства и построение на их базе компьютерных сетей, имеющих прямой доступ к глобальным информационным системам, заставляет пристальнее приглядеться к подлинным и мнимым опасностям, которые таит в себе современная информатизация общества, оценить ущерб от взлома широкого класса компьютерных сетей – от локальных до глобальных телекоммуникационных систем.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных (включая и жизнеобеспечивающие) объектов, серьезное нарушение работы ЭВМ и их систем.

Несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям. Опасность компьютерных преступлений многократно возрастает, когда они совершаются в отношении функционирования объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики.

Вышеприведенные факты убедительно свидетельствуют о действительной остроте проблемы с преступлениями в сере компьютерной информации. Преступления данной категории причиняют как серьезный экономический ущерб, так и непосредственную угрозу даже существованию человечества.

Практическим работникам следственных органов довольно сложно расследовать данную категорию дел. Необходимо владеть знаниями компьютерной технологии, а также механизма обработки компьютерных данных.

Цель данной работы – изучение тактики и методики расследования преступлений в сфере компьютерной информации.

Для этого были поставлены следующие задачи:

* изучение основных понятий по данному вопросу, а именно понятие преступления в сфере компьютерной и понятие расследования;
* изучение производства следственных действий по делам рассматриваемой категории, последовательность их проведения;
* выработать план расследования преступлений в сфере компьютерной информации,
* на практическом примере рассмотреть конкретную тактику и методику расследования данного вида преступлений.

**1. Правовое регулирование отношений в**

**области компьютерной информации**

Научно-техническая революция повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов – информационных. Последние отличаются от известных ранее сырьевых, энергетических ресурсов целым рядом особенностей, а именно:

* *они непотребляемы и подвержены не физическому, а моральному износу;*
* *они по своей сущности нематериальны и несводимы к физическому носителю, в котором воплощены;*
* *их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к колоссальной экономии средств;*
* *процесс их создания и использования осуществляется особым способом – с помощью компьютерной техники.*

Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники, средств телекоммуникаций и систем связи.

Появление на рынке в компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини- и большими ЭВМ, дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными.

Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе уголовно-правовые средства защиты.

Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматической обработки информации. Определенным этапом на пути реализации этих пожеланий стало принятие в 1992 г. Закона РФ «О правовой охране программ для электронно-вычислительных машин и баз данных». Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет уголовную ответственность. Однако соответствующих изменений в УК РСФСР так и не было внесено.

В 1994 году был принят Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, в 1995 году – Федеральный закон об информации, информатизации и защите информации. Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления. Определим некоторые основные понятия, используемые в данной работе.

Законодательство России в области «компьютерного права» также включает следующие основные законы: «О средствах массовой информации», « Патентный закон РФ», «О правовой охране топологий интегральных микросхем», «О правовой охране программ для электронных вычислительных машин и баз данных», «О товарных знаках, знаках обслуживания и наименования мест происхождения товаров», «Основы законодательства об Архивном фонде РФ и архивах», «Об авторском праве и смежных правах», «О государственной тайне», «Об обязательном экземпляре документов», «О связи», «Об информации, информатизации и защите информации», «Об участии в международном информационном обмене».

Значительный пласт компьютерного права составляют указы Президента РФ, которые касаются, прежде всего, вопросов формирования государственной политики в сфере информатизации включая организационные механизмы, создания системы право вой информации и информационно-правового сотрудничества с государствами СНГ, обеспечения информацией органов государственной власти: мер по защите информации в частности, шифрования.[[1]](#footnote-1)

Конституция РФ непосредственно не регулирует отношения в области производства и применения новых информационных технологий, но создает предпосылки для такого регулирования, закрепляя права граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом ч. 4 ст. 29, право граждан на охрану личной тайны ч. 1 ст. 24 и другие обязанности государства, в частности по обеспечению возможности ознакомления гражданина с документами и материалами, непосредственно затрагивающими его права и свободы ч. 2 ст. 24. Соответствующее законодательство формирует механизмы реализации этих норм.

Компьютерная информация – в соответствии со ст. 2 закона *«Об информации, информатизации и защите информации»* под информацией понимаются – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления, но применительно к комментируемым статьям под компьютерной информацией понимаются не сами сведения, а форма их представления в машиночитаемом виде, т.е. совокупность символов зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе). При рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

Под *компьютерными преступлениями* следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть.

**2. Общая характеристика преступлений в**

**сфере компьютерной информации**

В Уголовном кодексе Российской Федерации впервые в нашей стране криминализирован такой вид правонарушений, как компьютерные преступления.

Как видно из предыдущей главы под компьютерными преступлениями понимаются те предусмотренные уголовным законом общественно опасные деяния, в которых машинная информация представляет собой предмет преступного посягательства.

Преступления, имеющие своим предметом только лишь аппаратно-технические средства вычислительных машин (хищение, уничтожение), подпадают под совершенно другой тип уголовных правонарушений, закрепленных в главе 21 «Преступления против собственности». В принципе, можно предположить случаи, когда вредоносное воздействие на ЭВМ осуществляется путем непосредственного влияния на нее информационных команд. Это возможно, если преступнику удастся ввести движущиеся части машины (диски, принтер) в резонансную частоту, увеличить яркость дисплея или его части для прожигания люминофора, зациклить работу компьютера таким образом, чтобы при использовании минимального количества его участков произошел их разогрев и вывод из строя. В этих случаях квалификация содеянного должна проводиться по совокупности статей глав о преступлениях против собственности и компьютерных преступлениях, поскольку в данной ситуации страдают два объекта уголовно-правовой охраны. Равно и при использовании в качестве орудия совершения противоправного деяния не информационной, а одной аппаратно-технической части (нанесение телесных повреждений принтером и т. п.) последнюю можно расценивать наравне с такими предметами, как нож, пистолет, веревка и другие вещи материального мира. В целом же *28-я глава УК РФ «Компьютерные преступления»* имеет своей целью охрану именно информационной безопасности – и только в силу этого защиту и аппаратно технических средств, которые являются материальными носителями информационных ресурсов. Последствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д. Поэтому совершенно оправданно то, что преступления данного вида помещены в раздел *IX «Преступления против общественной безопасности и общественного порядка».*

Таким образом, общим объектом компьютерных преступлений будет выступать совокупность всех общественных отношений, охраняемых уголовным законом; родовым – общественная безопасность и общественный порядок; видовым – совокупность общественных отношений по правомерному и безопасному использованию информации; непосредственный объект трактуется, исходя из названий и диспозиций конкретных статей. Чаще всего непосредственный объект основного состава компьютерного преступления сформулирован альтернативно, в квалифицированных составах количество их, естественно, увеличивается.

Является ли компьютерная информация только лишь предметом преступлений такого вида или же она может выступать и их средством, когда электронно-вычислительная техника используется с целью совершения другого противоправного посягательства на иной объект. Последняя точка зрения высказывалась ранее некоторыми авторами.

Однако принять ее означало бы слишком расширить рамки понятия *«компьютерное преступление»* и затруднить работу, как законодателя, так и правоприменителя.

Разработчики нового УК пошли по первому пути, сформулировав составы главы 28 таким образом, что информация ЭВМ в каждом случае является лишь предметом совершения компьютерного преступления.

Однако при использовании машинной информации в качестве средства совершения другого преступления отношения по ее охране страдают неизбежно, т. е. она сама становится предметом общественно опасного деяния. Невозможно противоправно воспользоваться информацией, хранящейся в ЭВМ, не нарушив при этом ее защиты, т.е. не совершив одного из действий, перечисленных в *ст. 20 Федерального закона «Об информации, информатизации и защите информации»:* утечки, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования и других форм незаконного вмешательства в информационные ресурсы и системы. Даже если не пострадают сведения конкретной ЭВМ, правомерно употребляемые ее законным пользователем, практически неизбежно подвергнутся ущербу те, с которыми она связана сетью. Таким образом, даже при совершении такого классического преступления, как электронное хищение денег, ответственность за это должна наступать по правилам идеальной совокупности преступлений.

Почти все составы главы 28 относятся к преступлениям небольшой и средней тяжести, и только один – к тяжким преступлениям. Характеризуя объективную сторону рассматриваемых составов, заметим, в первую очередь, что даже большинство из них конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно-опасного деяния, но и наступление общественно-опасных последствий, а также установление причинной связи между этими двумя признаками.

Однако нельзя не признать, что уничтожение, блокирование, модификация и копирование информации не исключают совершения самостоятельных действий. В учебной литературе[[2]](#footnote-2) указывается, что правильнее было бы рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ сопряжен с уничтожением, блокированием и т.д. (т.е. такому доступу следовало бы придать значение не только причины, но и необходимого условия).

В силу *ч. 2 ст. 9 УК РФ* временем совершения каждого из этих преступлений будет признаваться время окончания именно деяния независимо от времени наступления последствий. Сами же общественно опасные деяния чаще всего выступают здесь в форме действий и лишь иногда – как бездействие. В одном случае такой признак объективной стороны состава преступления, как способ его совершения, сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных он, а также время, место, обстановка, орудия, средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств.

Из всех признаков субъективной стороны значение будет иметь только один – вина. При этом, исходя из *ч. 2 ст. 24 УК*, для всех преступлений данного вида необходимо наличие вины в форме умысла, и лишь два квалифицированных состава предусматривают две ее формы: умысел по отношению к деянию и неосторожность в отношении наступивших общественно-опасных последствий. Факультативные признаки субъективной стороны так же, как и в вопросе о стороне объективной, не будут иметь значения для квалификации преступления. Так, мотивами совершения таких деяний чаще всего бывают корысть либо хулиганские побуждения, но могут быть и соображения интереса, чувство мести; не исключено совершение их, с целью скрыть другое преступление и т.д. Естественно, что особую трудность вызовет проблема отграничения неосторожного и невиновного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в сетях и системах ЭВМ.

Субъект нескольких составов является специальным. В остальных случаях им может стать, в принципе, любой человек, особенно если учесть всевозрастающую компьютерную грамотность населения. Ответственность за преступления против компьютерной безопасности наступает *с 16 лет (ст. 20 УК).*

Диспозиции статей 28-й главы описательные, зачастую – бланкетные или отсылочные. Для их применения необходимо обратиться к *ст. 35 УК,* к нормативно-правовому акту об охране компьютерной информации, правилам эксплуатации ЭВМ и т. п. Санкции – альтернативные, за исключением двух квалифицированных составов, где они – в силу тяжести последствий преступления – *«урезаны»* до относительно-определенных.

Первоначально в проекте УК РФ глава о компьютерных преступлениях содержала 5 статей. Однако в дальнейшем в силу замечаний, высказанных как теоретиками уголовного права, так и практиками компьютерного дела, первые три статьи были объединены, и в настоящее время глава предстает в следующем составе:

* ст. 272. Неправомерный доступ к компьютерной информации;
* ст. 273. Создание, использование и распространение вредоносных программ для ЭВМ;
* ст. 274. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

**3. Расследование преступления**

**3.1. Фабула и предварительный план расследования**

**Фабула**

10 ноября 2002 г. членами организованной преступной группы был осуществлен несанкционированный доступ к средствам компьютерной техники коммерческого банка «Альянс». И в течение суток банк не смог нормально осуществлять все операции по платежам. Только прямой ущерб составил около 60 тысяч рублей.

В результате осмотра места преступления и осмотра компьютерной сети банка было обнаружено следующее. В программном обеспечении компьютерной сети банка выявлен «вирус». В 10.30 часов из-за «вируса» главный сервер отключил всю компьютерную сеть и заблокировал ее.

В ходе расследования были задержаны гр-не Т. и П. И у них были изъяты мощные компьютеры и программной обеспечение с компьютерными «вирусами».

**Предварительный план расследования преступления.**

«УТВЕРЖДАЮ»

Прокурор г. Саратова советник

юстиции Демидов Н.М. \_\_\_\_\_\_\_\_\_

10 ноября 2002 года

**ПЛАН**

**расследования по уголовному делу №11764,**

**возбужденному по факту несанкционированного доступа к средствам компьютерной техники коммерческого банка «Альянс»**

В целях раскрытия преступления, совершенного в отношении коммерческого банка «Альянс», установления лица (лиц), его совершивших, и проверки следственно-оперативным путем вероятных версий совершения преступления необходимо следующее:

**1) Вопросы и обстоятельства, общие для всех версий:**

1. Назначить по делу судебно-бухгалтерскую экспертизу для определения, имеются ли нарушения требований положений о документообороте и установления лиц, ответственных за эти преступления.

Исполнители: следователь Срок: 5 декабря 2002 года.

2. Назначить по делу программно-техническую судебную экспертизу для определения места, с которого был произведен несанкционированный доступ в систему, и ряда других технических деталей преступления.

Исполнители: следователь Срок: 5 декабря 2002 года.

3. В случае установления личности подозреваемого назначить по делу дополнительную дактилоскопическую экспертизу по изъятым на месте происшествия отпечаткам пальцев рук.

Исполнители: следователь Срок: в ходе расследования

**Версия 1. Несанкционированный доступ совершен с целью хулиганства.**

1. Провести осмотр и фиксацию состояния ЭВМ, сетей ЭВМ и машинных носителей, допросы лиц, обеспечивающих работу информационной системы банка.

Исполнители: следователь Срок: до 15 ноября 2002 года.

**Версия 2. Несанкционированный доступ произведен из корыстных побуждений (с целью хищения денежных средств или получения информации) бывшим работником банка.**

1. Оперативным путем установить и проверить на причастность к совершению преступления лиц, ранее работающих в банке.

Исполнители: следователь Срок: до 20 ноября 2002 года.

**Версия 3. Несанкционированный доступ произведен из корыстных побуждений (с целью хищения денежных средств или получения информации) «по найму» сотрудником банка.**

1. Оперативным путем установить и проверить на причастность к совершению преступления лиц, работающих в банке.

2. Следственно-оперативным путем установить лиц, из числа сотрудников банка, у которых могут иметься соответствующие компьютерные знания и аппаратура. Провести обыски по месту их жительства.

Исполнители: следователь Срок: до 20 ноября 2002 года.

Следователь прокуратуры

Волжского района г. Саратова

юрист 2 класса Иванов И.П.

**3.2. План расследования**

«УТВЕРЖДАЮ»

Прокурор г. Саратова советник

юстиции Демидов Н.М. \_\_\_\_\_\_\_\_\_

10 ноября 2002 года

**ПЛАН**

**расследования по уголовному делу №11764,**

**возбужденному по факту несанкционированного доступа к средствам**

**компьютерной техники коммерческого банка «Альянс»**

В целях раскрытия преступления, совершенного в отношении коммерческого банка «Альянс», установления лица (лиц), его совершивших, с учетом данных полученных на первоначальном этапе расследования, следует выдвинуть следующую версию:

Несанкционированный доступ произведен из корыстных побуждений (с целью хищения денежных средств или получения информации) бывшим работником банка Т и его подельником П.

Для проверки следственно-оперативным путем данной версии совершения преступления необходимо:

1. Получить образцы отпечатков пальцев рук подозреваемых гр. Т., П.

Исполнители: следователь Срок: 30 ноября 2002 года.

2. Назначить по делу дополнительную дактилоскопическую экспертизу по изъятым на месте происшествия отпечаткам пальцев рук и проверить их на принадлежность гр. Т., П.

Исполнители: следователь Срок: 30 ноября 2002 года.

3. Следственно-оперативным путем (путем проведения опроса и допросов работников банка и сослуживцев) установить, имелось ли соответствующая аппаратура у гр. Т. Провести обыски по месту жительства Т., П. и принять меры по обнаружению и изъятию аппаратуры.

Исполнители: следователь Срок: 30 ноября 2002 года.

4. Предъявить гр. П. на опознание сослуживцам Т.

5. В случае дачи подозреваемыми признательных показаний провести с их участием проверку показаний на месте совершения преступлений.

Исполнители: следователь Срок: в ходе расследования.

Следователь прокуратуры

Волжского района г. Саратова

юрист 2 класса Иванов И.П.

**3.3. Практические особенности отдельных следственных**

**действий**

При расследовании компьютерных преступлений можно выделить три типичные следственные ситуации:

1. Собственник информационной системы собственными силами выявил нарушение целостности / конфиденциальности информации в системе, обнаружил виновное лицо и заявил об этом в правоохранительные органы.

2. Собственник информационной системы собственными силами выявил нарушение целостности / конфиденциальности информации в системе, не смог обнаружить виновное лицо и заявил об этом в правоохранительные органы.

3. Данные о нарушении целостности/конфиденциальности информации в информационной системе и виновном лице стали общеизвестными или непосредственно обнаружены органом дознания (например, в ходе проведения оперативно-розыскных мероприятий по другому делу).

При наличии заподозренного виновного лица первоначальная задача следствия заключается в сборе с помощью собственника информационной системы и процессуальной фиксации доказательств:

а) нарушения целостности/конфиденциальности информации в системе;

б) размера ущерба, причиненного нарушением целостности/конфиденциальности информации;

в) причинной связи между действиями, образующими способ нарушения, и наступившими последствиями путем детализации способа нарушения целостности/конфиденциальности информации в системе и характера совершенных виновным действий;

г) отношения виновного лица к совершенным действиям и наступившим последствиям.

Т.к. подозреваемые задержаны сразу же после совершения преступления, для данной ситуации характерны следующие первоначальные следственные действия:

а) личный обыск задержанных;

б) допрос задержанных;

в) обыск по месту жительства задержанных.

Осмотр и обыск (выемка) по делам данной категории являются важнейшими инструментами установления обстоятельств расследуемого события.

Известно, что главными процессуальными способами изъятия вещественных доказательств являются осмотр, обыск и выемка.

Следует напомнить, что осмотр – это непосредственное обнаружение, восприятие и исследование следователем материальных объектов, имеющих отношение к исследуемому событию. Обыск – следственное действие, в процессе которого производится поиск и принудительное изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства. Выемка – следственное действие, в процессе которого производится изъятие объектов, имеющих значение для правильного решения задач уголовного судопроизводства, в тех случаях, когда их местонахождение точно известно следователю и изъятие прямо или косвенно не нарушает прав личности.

Носители информации, имеющей отношение к расследуемому событию, могут быть с соблюдением установленного УПК РФ порядка изъяты и приобщены к уголовному делу в качестве вещественного доказательства.

Для участия в обыске и выемке целесообразно приглашать специалиста в области компьютерной техники.

При осмотрах, обысках, выемках, сопряженных с изъятием ЭВМ, машинных носителей и информации возникает ряд общих проблем, связанных со спецификой изымаемых технических средств.

Так, необходимо предвидеть меры безопасности, предпринимаемые преступниками с целью уничтожения вещественных доказательств.

Например, они могут использовать специальное оборудование, в критических случаях создающее сильное магнитное поле, стирающее магнитные записи. Известна легенда о хакере, который создал в дверном проеме магнитное поле такой силы, что оно уничтожало магнитные носители информации при выносе их из его комнаты.

Преступник имеет возможность включить в состав программного обеспечения своей машины программу, которая заставит компьютер периодически требовать пароль, и, если несколько секунд правильный пароль не введен, данные в компьютере автоматически уничтожаются.

Желательно иметь с собой и использовать при обыске и осмотре устройство для определения и измерения магнитных полей.

Вещественные доказательства в виде ЭВМ, машинных носителей требуют особой аккуратности при транспортировке и хранении. Им противопоказаны резкие броски, удары, повышенные температуры, влажность. Все эти внешние факторы могут повлечь потерю данных, информации и свойств аппаратуры.

Не следует забывать при осмотрах и обысках о возможностях сбора традиционных доказательств (скрытых отпечатков пальцев на клавиатуре, выключателях и др., шифрованных рукописных записей и пр.).

Осмотру подлежат все устройства конкретной ЭВМ.

Фактически оптимальный вариант изъятия ЭВМ и машинных носителей информации – это фиксация их и их конфигурации на месте обнаружения и упаковка таким образом, чтобы аппаратуру можно было бы успешно, правильно и точно так же, как на месте обнаружения, соединить в лабораторных условиях или в месте производства следствия с участием специалистов.

Указанные следственные действия могут производиться с целями:

а) осмотра и изъятия ЭВМ и ее устройств;

б) поиска и изъятия информации и следов воздействия на нее в ЭВМ и ее устройствах;

в) поиска и изъятия информации и следов воздействия на нее вне ЭВМ.

По прибытии на место осмотра или обыска следует принять меры к обеспечению сохранности информации на находящихся здесь компьютерах и магнитных носителях. Для этого необходимо:

1) не разрешать кому бы то ни было из лиц, работающих на объекте обыска, прикасаться к работающим компьютерам, магнитным носителям, включать и выключать компьютеры;

2) самому не производить никаких манипуляций с компьютерной техникой, если результат этих манипуляций заранее не известен;

3) при наличии в помещении, где находятся СКТ и магнитные носители информации, взрывчатых, легковоспламеняющихся, токсичных и едких веществ или материалов как можно скорее удалить эти вещества в другое помещение.

**Особенности производства осмотров и обысков**

Если компьютер работает, ситуация для следователя, производящего следственное действие без помощи специалиста, существенно осложняется, однако и в этом случае не следует отказываться от оперативного изъятия необходимых данных.

В данной ситуации:

а) определить, какая программа выполняется. Для этого необходимо изучить изображение на экране дисплея и по возможности детально описать его.

После остановки программы и выхода в операционную систему иногда при нажатии функциональной клавиши «F3» можно восстановить наименование вызывавшейся последний раз программы.

Можно осуществить фотографирование или видеозапись изображения;

б) остановить исполнение программы. Остановка осуществляется одновременным нажатием клавиш Ctrl-C, либо Ctrl-Break;

в) зафиксировать (отразить в протоколе) результаты своих действий и реакции компьютера на них;

г) определить наличие у компьютера внешних устройств – накопителей информации на жестких магнитных дисках и виртуального диска;

д) определить наличие у компьютера внешних устройств удаленного доступа к системе и определить их состояние (отразить в протоколе), после чего разъединить сетевые кабели так, чтобы никто не мог изменить или стереть информацию в ходе обыска (например, отключить телефонный шнур из модема);

е) скопировать программы и файлы данных. Копирование осуществляется стандартными средствами ЭВМ или командой DOS COPY;

ж) выключить подачу энергии в компьютер и далее действовать по схеме «компьютер не работает».

Если компьютер не работает, следует:

а) точно отразить в протоколе и на прилагаемой к нему схеме местонахождение ПК и его периферийных устройств;

б) точно описать порядок соединения между собой этих устройств с указанием особенностей (цвет, количество соединительных разъемов, их спецификация) соединительных проводов и кабелей; перед разъединением полезно осуществить видеозапись или фотографирование мест соединения;

в) с соблюдением всех мер предосторожности разъединить устройства компьютера, предварительно обесточив его;

г) упаковать раздельно носители на дискетах и магнитных лентах и поместить их в оболочки, не несущие заряда статического электричества;

д) упаковать каждое устройство и соединительные кабели, провода;

е) защитить дисководы гибких дисков согласно рекомендации изготовителя (вставить новую дискету или часть картона в щель дисковода);

ж) особой осторожности требует транспортировка винчестера.

**Поиск и изъятие информации и следов воздействия на нее в ЭВМ**

**и ее устройствах**

В компьютере информация может находиться непосредственно в оперативном запоминающем устройстве (ОЗУ) при выполнении программы, в ОЗУ периферийных устройств и на внешних запоминающих устройствах (ВЗУ).

Наиболее эффективным и простым способом фиксации данных из ОЗУ является распечатка на бумагу информации, появляющейся на дисплее.

Если компьютер не работает, информация может находиться в ВЗУ и других компьютерах информационной системы или в «почтовых ящиках» электронной почты или сети ЭВМ.

Необходимо произвести детальный осмотр файлов и структур их расположения; лучше это осуществить с участием специалиста в лабораторных условиях или на рабочем месте следователя.

Следует обращать внимание на поиск так называемых «скрытых» файлов и архивов, где может храниться важная информация.

Периферийные устройства ввода-вывода могут также некоторое время сохранять фрагменты программного обеспечения и информации, однако для вывода этой информации необходимы глубокие специальные познания.

Осмотр компьютеров и изъятие информации производится в присутствии понятых, которые расписываются на распечатках информации, изготовленных в ходе осмотра.

В ходе осмотров по делам данной категории могут быть обнаружены и изъяты следующие виды важных документов, которые могут стать вещественными доказательствами по делу:

а) документы, носящие следы совершенного преступления, – телефонные счета, пароли и коды доступа, дневники связи и пр.;

б) документы со следами действия аппаратуры. Всегда следует искать в устройствах вывода (например, в принтерах) бумажные носители информации, которые могли остаться внутри их в результате сбоя в работе устройства;

в) документы, описывающие аппаратуру и программное обеспечение;

г) документы, устанавливающие правила работы с ЭВМ, нормативные акты, регламентирующие правила работы с данной ЭВМ, системой, сетью, доказывающие, что преступник их знал и умышленно нарушал;

д) личные документы подозреваемого или обвиняемого.

Комплекс неотложных следственных действий обязательных для первоначального этапа расследования также включает:

1. Проведение обыска в служебном помещении, на рабочем месте подозреваемого с целью обнаружения и изъятия физических носителей машинной информации и других документов, имеющих или возможно имеющих отношение к несанкционированному отношению программного обеспечения или носящих иные следы подготовки к хищению денежных средств.

2. Исследование:

* журналов сбойных ситуаций, рабочего времени ЭВМ, по передачи смен операторами;
* средств защиты и контроля банковских компьютерных систем, регистрирующих пользователей, моменты включения (активации) системы либо подключение к ним абонентов с определенным индексом или без такового;
* протоколов вечернего решения, представляющих собой копию действий операторов, отображенную на бумажном носителе в ходе вечерней обработки информации, которая проводится по истечении каждого операционного дня;
* контрольных чисел файлов;
* всего программного обеспечения ЭВМ;
* «прошитых» микросхем постоянно запоминающих устройств, микропроцессоров и их схемного исследования.

3. Истребование и анализ технических указаний по обработке ежедневной бухгалтерской информации с перечнем выходящих форм.

4. Допрос лиц из числа инженеров-программистов, занимавшихся разработкой программного обеспечения и его сопровождением, специалистов отвечающих за защиту информации и специалистов электронщиков, занимающихся эксплуатацией и ремонтов вычислительной техники.

5. Назначение комплексной судебно-бухгалтерской и программно-технической экспертизы с привлечением специалистов правоохранительных органов, специалистов в области средств компьютерной техники, по ведению банковского учета с использованием средств компьютерной техники, документообороту, организации бухучета и отчетности, специалистов по обеспечению безопасности информации в компьютерных системах.

В ходе судебно-бухгалтерской экспертизы должно быть установлено, имеются ли нарушения требований положений о документообороте при отображении первичных документов в регистрах бухгалтерского учета и отчетности зафиксированных на машинном носителе, установлены их причины (с целью совершения преступления, злоупотребления или ошибки), ответственных лиц за эти нарушения.

Результаты программно-технической экспертизы должны быть оформлены как заключение экспертов для того, чтобы они могли играть роль доказательств в процессе суда. В настоящее время с помощью таких экспертиз могут решаться следующие задачи:

1. Воспроизведение и распечатка всей или части информации, содержащейся на физических носителях. В том числе находящихся в нетекстовой форме.

2. Восстановление информации, ранее содержавшейся на физических носителях и в последствии стертой или измененной по различным причинам.

3. Установление времени ввода, изменение, уничтожение либо копирование той или иной информации.

4. Расшифровка закодированной информации, подбор паролей и раскрытие систем защиты.

5. Установление авторства, места, средства, подготовки и способа изготовления документов (файлов, программ).

6. Выяснения возможных каналов утечки информации из компьютерной сети и помещений.

7. Выяснение технического состояния, исправности программно-аппаратных комплексов БИВС, возможности их адаптации под конкретного пользователя.

8. Установления уровня профессиональной подготовки отдельных лиц, проходящих по делу в области программирования и в качестве пользователя.

**3.4. Вынесение постановления о назначении необходимых**

**экспертиз**

Постановление

о назначении программно-технической судебной экспертизы

г. Саратов 12 ноября 2002 г.

Следователь прокуратуры Волжского района г. Саратова юрист 2 класса Иванов И.П., рассмотрев материалы уголовного дела № 11764,

**Установил:**

10 ноября 2002 г. членами организованной преступной группы был осуществлен несанкционированный доступ к средствам компьютерной техники коммерческого банка «Альянс». В течение суток банк не смог нормально осуществлять все операции по платежам. Прямой ущерб составил около 60 тысяч рублей.

В результате осмотра места преступления и осмотра компьютерной сети банка было обнаружено следующее. В программном обеспечении компьютерной сети банка выявлен «вирус». В 10.30 часов из-за «вируса» главный сервер отключил всю компьютерную сеть и заблокировал ее.

В ходе расследования были задержаны гр-не Т. и П. И у них были изъяты мощные компьютеры и программной обеспечение с компьютерными «вирусами».

На основании изложенного и руководствуясь ст.195 (196) и 199 УПК РФ,

**Постановил:**

1. Назначить программно-техническую судебную экспертизу, производство которой поручить эксперту ЭКО г. Саратова.
2. Поставить перед экспертом вопросы:

1. Какова конфигурация и состав компьютерных средств и можно ли с помощью этих средств осуществить действия, инкриминируемые обвиняемым?

2. Какие информационные ресурсы находятся в данной ЭВМ?

3. Не являются ли обнаруженные файлы копиями информации, находившейся на конкретной ЭВМ?

4. Не являются ли представленные файлы с программами, зараженными вирусом, и если да, то каким именно?

5. Не являются ли представленные тексты на бумажном носителе записями исходного кода программы, и каково назначение этой программы?

6. Подвергалась ли данная компьютерная информация уничтожению, копированию, модификации?

7. Какие правила эксплуатации ЭВМ существуют в данной информационной системе, и были ли нарушены эти правила?

8. Находится ли нарушение правил эксплуатации в причинной связи с уничтожением, копированием, модификацией?

1. Предоставить в распоряжение эксперта материалы:

– копию настоящего постановления;

– материалы настоящего уголовного дела;

– возможность экспертного осмотра места происшествия и ЭВМ.

4. Поручить разъяснить эксперту права и обязанности, предусмотренные ст. 57 УПК РФ, и предупредить его об уголовной ответственности по ст. 307 УК РФ за дачу заведомо ложного заключения.

Следователь Иванов И.П.

Права и обязанности, предусмотренные ст. 57 УПК РФ, мне разъяснены 12 ноября 2002 г. Одновременно я предупрежден об уголовной ответственности по ст. 307 УК РФ за дачу заведомо ложного заключения.

Эксперт \_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ЗАКЛЮЧЕНИЕ**

В ходе изучения действующего уголовного законодательства в области регулирования компьютерного права и специфики расследования преступлений в сфере компьютерной информации были сделаны определенные обобщения:

Преступления в области компьютерной информации являются частью информационных преступлений: объединенных единым инструментом обработки информации – компьютером. Практически все преступления относятся к преступлениям средней тяжести. Исключением является лишь преступления, квалифицируемые ч. 2 ст. 273, относящиеся к тяжким преступлениям. Для всех преступлений данного вида необходимо наличие вины в форме умысла. Субъектом преступления может стать любой человек старше 16 лет, особенно если учесть всевозрастающую компьютерную грамотность населения.

Известные на сегодня способы совершения компьютерных преступлений отличаются значительным и постоянно расширяющимся разнообразием. Совершают преступления данной категории чаще всего люди со специальной подготовкой в области автоматизированной обработки информации, причем более половины из их числа в составе преступных групп. Основная опасность исходит от внутренних пользователей – ими совершается более 90 преступлений.

Типичными следственными действиями, применяющимися при расследовании преступлений в сфере компьютерной информации, являются следственный осмотр, допрос свидетеля, потерпевшего, обвиняемого, подозреваемого, производство судебных информационно-технических экспертиз, обыск и выемка, а также следственный эксперимент.

При расследовании преступлений в сфере компьютерной информации следственные задачи решаются в следующей последовательности:

* Установление факта совершения преступления: времени его совершения: способа и других обстоятельств, знание которых необходимо для успешного проведения расследования;
* установление лица или лиц, совершившего преступное деяние: виновности и мотивов преступления;
* установление вредных последствий преступления и выявление обстоятельств, способствовавших преступлению.

При производстве следственных осмотра объектов преступления в целях обнаружения следов преступления, выяснения обстановки происшествия и иных значимых для дела обстоятельств целесообразно привлекать к ним технических специалистов с достаточно высокой степенью компетенции. Соответствующие специалисты призываются также для участия при производстве обыска последующего осмотра изъятого и следственного эксперимента.

Вышеуказанные участники следственных действий должны оказать помощь следователю при установлении факта совершения преступления, времени его совершения, способа совершения и обстоятельств, способствовавших преступлению. Весьма важным является значение проведения судебных информационно-технических экспертиз.

В соответствии с источниками рекомендуется предусмотреть в форме плана расследования следующие данные:

* наименование дела;
* дату его возбуждения;
* срок окончания расследования;
* графы: доверсионные вопросы нуждающиеся в выяснении еще до выдвижения какой-либо версии, версии, подлежащие выяснению вопросы, необходимые мероприятия применительно к каждой версии и каждому выясняемому вопросу, срок выполнения каждого мероприятия, исполнитель каждого мероприятия, отметка о выполнении мероприятия.

**БИБЛИОГРАФИЯ**

1. Божкова Н.Р. и др. Следственная (криминалистическая) тактика. – Саратов, 1996.
2. Быстряков Е.Н., Иванов А.Н., Климов В.Л. Расследование компьютерных преступлений. – Саратов, 2000.
3. Волчинская Е.К. Есть ли в России компьютерное право? /Российская юстиция. – 1997. – 6.
4. Гульбин Ю. Преступления в сфере компьютерной информации.// Российская юстиция № 10, 1997.
5. Криминалистика / Под. ред. Белкина Р.С. – М., 1999.
6. Криминалистика: Учебник. / Отв.ред. Н.П. Яблоков. – М.: Юристъ, 1999.
7. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления. //Законность №1. – 1997.
8. Рачук Т. Компьютерные преступления – новое в уголовном законодательстве России. // Материалы Национальной службы новостей, 1997.
9. Россинская Е.Р. Судебная экспертиза в уголовном, гражданском, арбитражном процессе. – М., 1996.
10. Уголовное право. Особенная часть. Учебник. Под ред. И.Я. Козаченко, – М.: ИНФРА-М-НОРМА, 1997.
11. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. №174-ФЗ

1. Волчинская Е.К. Есть ли в России компьютерное право? /Российская юстиция. – 1997. – 6. – С. 9-19. [↑](#footnote-ref-1)
2. Уголовное право. Особенная часть. Учебник. Под ред. И.Я. Козаченко, – М.: ИНФРА-М-НОРМА, 1997. [↑](#footnote-ref-2)