Министерство общего образования РФ

Курсовая работа по криминалистике

**РАССЛЕДОВАНИЕ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

2002

**Содержание**

Введение 3

1. Проблема информационной безопасности 6

2. Уголовно-правовая и криминалистическая характеристика неправомерного доступа к компьютерной информации 8

3. Особенности первоначального этапа расследования неправомерного доступа к компьютерной информации 13

4. Расследование неправомерного доступа к компьютерной информации на последующем этапе 19

Литература 23

# Введение

В современных условиях научно-технического прогресса четко выделяется тенденция компьютеризации, созда­ния разветвленных систем обработки данных, включающих в себя как мощные вычислительные комплексы, так и персональные компьютеры. Осуществляется ввод коммуникационных локальных, отраслевых, общегосударственных и меж­государственных сетей. Компьютеризация затрагивает практически все стороны общественной жизни от контроля за воздушным и наземным транспортом, до решения проблем национальной безопасности. Внедрение автоматизированных систем обработки информации способствует развитию экономики, приводит к появлению «безбумажных» технологий. Сейчас вряд ли кто может представить деятельность предприятия, организации, учреждения или фирмы, да и деятель­ность отдельных должностных лиц без использования компьютера.

Совершенствование компьютерных технологий привело к появлению новых видов преступлений, в частности, неправомерному доступу к охраняемой законом компьютерной информации. По своему механизму, способам соверше­ния и сокрытия это преступление имеет определенную специфику, характеризу­ется высочайшим уровнем латентности и низким уровнем раскрываемости.

Относительная новизна возникших проблем, стремительное наращива­ние процессов компьютеризации российского общества, рост компьютерной грамотности населения застали врасплох правоохранительные органы, оказав­шиеся неготовыми к адекватному противостоянию и борьбе с этим новым экономико-социально-правовым явлением.

В этих условиях особая роль отводится юридической науке, особенно та­ким ее отраслям, как криминалистика, которая реализует специальные юриди­ческие познания, максимально приближенные к практике борьбы с преступно­стью.

Исследование сферы расследования неправомерного доступа к компью­терной информации является одной из немногих попыток на основе научного прогнозирования, обобщения зарубежною опыта, имеющейся в России следст­венной и судебной практики дать рекомендации но расследованию нового видя преступлений.

Актуальность темы курсовой работы обусловлена по­требностями правоохранительной практики в научно-обоснованных рекоменда­циях расследования неправомерного доступа к охраняемой законом компь­ютерной информации.

Целью работы является изучение отечественного и зарубежного опыта рассматри­ваемой проблематике; разработка краткой уголовно-правовой характеристики неправомерного доступа к компьютерной информации; формирование криминалистической характеристики неправомерного дос­тупа к компьютерной информации (на основе данных о способах совершения, сокрытия, обстановке, орудиях и средствах совершения преступления, следах, механизме противоправного посягательства, а так же личностных свойствах граждан, осуществляющих неправомерный доступ к компьютерной информа­ции.

Предмет и объект исследования. Предметом исследования являются закономерности расследования неправомерного доступа к компьютерной ин­формации: следственные ситуации, складывающиеся при расследовании; после­довательность и тактика проведения процессуальных, организационных и след­ственных действий на первоначальном и последующем этапах расследования.

Объектом исследования является деятельность следователя, лица, произ­водящего дознание при разрешении вопроса о возбуждении уголовного дела, а так же при проведении следственных действий, позволяющих собрать комплекс доказательств, изобличающих преступника.

Методологической и теоретической основой исследования послу­жили положения материалистической диалектики как общенаучного метода по­знания, а так же системно-структурный, сравнительно-правовой, логический, исторический, статистический, контент-анализ, наблюдение, измерение, описа­ние, сравнение и другие методы исследования.

Правовой основой исследования явились законодательство Российской Федерации, указы Президента, нормативные акты Правительства и правоохранительных органов России.

# 1. Проблема информационной безопасности

В России по данным ГИЦ МИД РФ в 1998 г. по ст. 272 УК РФ было возбуждено 55 уголовных дел, окончены расследованием 47. Это более чем в 10 раз превы­сило аналогичный показатель 1997 г. За 1999 г. возбуждено 209 уголовных дел. Прогнозирование ситуации показывает, что предстоящий рост неправомерного доступа к компьютерной информации будет объясняться следующими фактора­ми:

1. Ростом количества ЭВМ, используемых в России, и как следствие этого, ростом количества их пользователей, увеличением объемов информации, хранимой в ЭВМ. Этому способствует снижение цен на сами компьютеры и периферийное оборудование (принтеры, сканеры, модемы и др.), а так же то об­стоятельство, что отечественными фирмами налажена самостоятельная сборка компьютеров.

2. Недостаточностью мер по защите ЭВМ и их систем, а так же не все­гда серьезным отношением руководителей к вопросу обеспечения информаци­онной безопасности и защите информации.

3. Недостаточностью защиты программного обеспечения (к примеру, в системе Windows недостаточная защищенность программного обеспечения связана с несовершенным алгоритмом шифрования сохраняемых паролей).

4. Недостаточностью защиты самих технических средств защиты ком­пьютерной техники.

5. Возможностью выхода российских пользователей ЭВМ в мировые информационные сети для обмена информацией, заключения контрактов, проведения платежей и др. Подобный обмен в настоящее время осуществляется абонентами самостоятельно, без контроля со стороны государственных органов, минуя географические и государственные границы.

6. Использованием в преступной деятельности современных техниче­ских средств, в том числе и ЭВМ. Это объясняется следующим: во-первых, ор­ганизованная преступность включена в крупномасштабный бизнес, выходящий за рамки отдельных государств, где без компьютеров невозможно руководить и организовывать сферу незаконной деятельности; во-вторых, из организаций, использующих электронно-вычислительную технику, значительно удобнее «вы­тягивать» деньги с помощью такой же техники, дающей возможность повысить прибыль и сократить риск.

7. Недостаточной защитой средств электронной почты.

8. Небрежностью в работе пользователей ЭВМ.

9. Непродуманной кадровой политикой в вопросах приема на работу и увольнения. Мировой опыт развития компьютерной техники свидетельствует, что специалисты высокой квалификации, неудовлетворенные условиями или оплатой труда, нередко уходят из компаний для того, чтобы начать собствен­ный бизнес. При этом они «прихватывают» с собой различную информацию, являющуюся собственностью владельцев покидаемой фирмы, включая техноло­гию, список потребителей и т.д.

10. Низким уровнем специальной подготовки должностных лиц право­охранительных органов, в том числе и органов внутренних дел, которые долж­ны предупреждать, раскрывать и расследовать неправомерный доступ к компь­ютерной информации.

11. Отсутствием скоординированности в работе государственных и об­щественных структур в сфере обеспечения информационной безопасности.

12. Ограничением на импорт в Россию защищенных от электронного шпионажа компьютеров и сетевого оборудования.

В этих условиях заметно повышается степень риска потери данных, а так­же возможность их копирования, модификации, блокирования. Причем, это не чисто российская, а общемировая тенденция. Представляется, что в скором времени проблема информационной безопасности и защиты данных станет в один ряд с такими глобальными проблемами современности, как межнацио­нальные конфликты, экологический кризис, организованная преступность, от­сталость развивающихся стран и др.

В связи с ростом анализируемых преступлений, возрастает количество тактических и методических ошибок, которые допускаются следователями и со­трудниками органов дознания, что объясняется, в первую очередь, отсутствием научно-обоснованных рекомендаций по расследованию неправомерного доступа к компьютерной информации.

# 2. Уголовно-правовая и криминалистическая характери­стика неправомерного доступа к компьютерной информации

Способы совершения неправомерного доступа к компьютерной информа­ции можно объединить в три основные группы:

Первая группа - это *способы непосредственного доступа.* При их реали­зации информация уничтожается, блокируется, модифицируется, копируется, а так же может нарушаться работа ЭВМ, системы ЭВМ или их сети путем отдачи соответствующих команд непосредственно с того компьютера, на котором ин­формация находится.

Вторая группа включает *способы опосредованного (удаленного)* доступа к компьютерной информации. К ним можно отнести: подключение к линии связи законного пользователя (например, к телефонной линии) и получение тем са­мым доступа к его системе; проникновение в чужие информационные сети, пу­тем автоматического перебора абонентских номеров с последующим соеди­нением с тем или иным компьютером; проникновение в компьютерную систему с использованием чужих паролей, выдавая при этом себя за законного пользова­теля.

К числу способов опосредованного (удаленного) доступа к компьютерной информации относятся способы непосредственного и электромагнитного пере­хвата. *Непосредственный перехват* осуществляется либо прямо через внешние коммуникационные каналы системы, либо путем непосредственного подключе­ния к линиям периферийных устройств. *Электромагнитный перехват* компьютерный информации осуществляется за счет перехвата излучений центрального процессора, дисплея, коммуникационных каналов, принтера и т.д.

Третью группу составляют *смешанные способы,* которые могут осуществ­ляться как путем непосредственного, так и опосредованного (удаленного) дос­тупа. К числу этих способов относятся: тайное введение в чужую программу таких команд, которые помогают ей осуществить новые, незапланированные функции при одновременном сохранении прежней ее работоспособности; моди­фикация программ путем тайного встраивания в программу набора команд, ко­торые должны сработать при определенных условиях, через какое-либо время; осуществление доступа к базам данных и файлам законного пользователя пу­тем нахождения слабых мест в системах защиты.

Неправомерный доступ к компьютерной информации может быть связан и с насилием над личностью либо угрозой его применения.

Способы сокрытия рассматриваемого преступления в значительной сте­пени детерминированы способами его совершения. При непосредственном дос­тупе к компьютерной информации, сокрытие следов преступления сводится к воссозданию обстановки, предшествующей совершению преступления, т.е. уничтожению оставленных следов (следов пальцев рук, следов обуви, микро­частиц и пр.). При опосредованном (удаленном) доступе сокрытие заключается в самом способе совершения преступления, который затрудняет обнаружение неправомерного доступа. Это достигается применением чужих паролей, иден­тификационных средств доступа и т.д.

Одним из распространенных орудий неправомерного доступа к компью­терной информации является сам компьютер. Необходимо различать орудия непосредственного и опосредованного доступа. К орудиям непосредственного доступа можно отнести, прежде всего, машинные носители информации, а так же все средства преодоления защиты информации.

К орудиям опосредованного (удаленного) доступа относится, прежде все­го, сетевое оборудование (при неправомерном доступе из локальных сетей), а так же средства доступа в удаленные сети (средства телефонной связи, модем).

Другим распространенным средством совершения неправомерного дос­тупа в последнее время стала глобальная мировая телекоммуникационная среда Интернет.

Одним из распространенных орудий неправомерного доступа к компью­терной информации является сам компьютер.

Обстановку совершения неправомерного доступа к компьютерной ин­формации составляют обстоятельства, характеризующие вещественные, техни­ческие, пространственные, временные, социально-психологические особенности события рассматриваемого преступления.

Особенностью данного преступления является то, что на него практиче­ски не оказывают влияние природно-климатические факторы. Дополнитель­ными факторами, характеризующими обстановку совершения неправомерного доступа к компьютерной информации могут являться наличие и состояние средств защиты компьютерной техники (организационных, технических, про­граммных), сложившаяся на объекте дисциплина, требовательность со стороны руководителей по соблюдению норм и правил информационной безопасности и эксплуатации ЭВМ. Для обстановки, в которой возможно совершение рассмат­риваемого преступления, наиболее свойственно следующее: невысокий технико-организационный уровень хозяйственной деятельности и контроль за информа­ционной безопасностью, неналаженная система защиты информации, атмосфера безразличия к случаям нарушения требований информационной безопасности. Так же особенностью неправомерного доступа к компьютерной информации является то, что место непосредственного совершения противоправного деяния - (место, где выполнялись действия объективной стороны состава преступления) и место наступления вредных последствий (место, где наступил результат про­тивоправного деяния) могут не совпадать.

Следы неправомерного доступа к компьютерной информации подразде­ляются на два вида: традиционные следы, рассматриваемые трассологией, и не­традиционные - информационные следы.

К первому тину относятся материальные следы. Ими могут быть рукописные записи, распечатки и т.п., свидетельствующие о приготовлении и совершении преступления. Материальные следы могут остаться и на самой вычислительной технике (следы пальцев рук, микрочастицы на клавиату­ре, дисководах, принтере и т.д.), а так же на магнитных носителях и CD-ROM дисках.

Информационные следы образуются в результате воздействия (уничто­жения, модификации, копирования, блокирования) на компьютерную информа­цию путем доступа к ней и представляют собой любые изменения компьютер­ной информации, связанные с событием преступления. Прежде всего, они оста­ются на магнитных носителях информации и отражают изменения в хранящейся в них информации (по сравнению с исходным состоянием). Речь идет о следах модификации информации (баз данных, программ, текстовых файлов), находя­щейся на жестких дисках ЭВМ, дискетах, магнитных лентах, лазерных и магнито-оптических дисках. Кроме того, магнитные носители могут нести следы уничтожения или модификации информации (удаление из каталогов имен фай­лов, стирание или добавление отдельных записей, физическое разрушение или размагничивание носителей). Информационными следами являются так же ре­зультаты работы антивирусных и тестовых программ. Данные следы могут быть выявлены при изучении компьютерного оборудования, рабочих записей про­граммистов, протоколов работы антивирусных программ, а так же программ­ного обеспечения. Для выявления подобных следов необходимо участие спе­циалистов в сфере программного обеспечения и вычислительной техники.

# 3. Особенности первоначального этапа расследования не­правомерного доступа к компьютерной информации

Наиболее распростра­ненными поводами к возбуждению уголовного дела по ст. 272 УК РФ являются: сообщения должностных лиц организаций или их объединений (около 40 %); заявления граждан (около 35 %); непосредственное обнаружение органом доз­нания, следователем или прокурором сведений, указывающих на признаки преступления (около 20 %); сообщения в средствах массовой информации и иные поводы (около 5 %).

В зависимости от источника и содержания сведений о неправомерном дос­тупе к компьютерной информации, могут складываться различные проверочные ситуации:

1. Неправомерный доступ обнаружен при реализации компьютерной ин­формации незаконным пользователем (например, при распространении сведе­ний, носящих конфиденциальный характер).

2. Факт неправомерного доступа к компьютерной информации обнаружен законным пользователем, но лицо, совершившее это, не установлено.

3. Неправомерный доступ обнаружен законным пользователем с фикса­цией на своей ЭВМ данных о лице, осуществляющем «перекачку» информации через сеть.

4. Неправомерный доступ обнаружен оператором, программистом или иным лицом в результате того, что преступник застигнут на месте преступле­ния.

5. Имел место неправомерный доступ к компьютерной информации (имеются иные сведения об этом), однако лицо, его совершившее, не установлено.

Для установления основания для возбуждения уголовного дела и разре­шения приведенных проверочных ситуаций необходимо осуществление прове­рочных действий в соответствии со ст. 109 УПК РСФСР: получение объясне­ний, производство осмотра места происшествия, истребование необходимых ма­териалов, осуществление оперативно-розыскных мероприятий.

Для уточнения оснований к возбуждению уго­ловного дела по ст. 272 УК РФ необходимо получить объяснения у инженеров-программистов, занимавшихся разработкой программного обеспечения и его сопровождением (отладкой и обслуживанием), операторов, специалистов по техническому обеспечению, занимающихся эксплуатацией и ремонтом средств компьютерной техники, системных программистов, инженеров по средствам связи и телекоммуникационному оборудованию, специалистов по обеспечению безопасности компьютерных систем и др.

При подготовке к проведению осмотра места происшествия необходимо пригласить соответствующих специалистов и понятых из числа лиц, владеющих компьютерной техникой, подготовить соответствующую компьютерную техни­ку, проинструктировать членов следственной группы и провести консультации со специалистами. По прибытии на место происшествия необходимо:

1. зафик­сировать обстановку, сложившуюся на момент осмотра места происшествия;
2. исключить возможность посторонним лицам (да и участникам следственно-оперативной группы) соприкасаться с оборудованием;
3. определить, соедине­ны ли находящиеся в помещении компьютеры в локальную вычислительную сеть;
4. установить, имеются ли соединения компьютера с оборудованием или вычислительной техникой вне осматриваемого помещения;
5. пояснить, под­ключен ли компьютер к телефонной или телетайпной линиям;
6. определить, запущены ли программы на ЭВМ и какие именно.

При изъятии компьютерной информации необходимо руководствоваться следующими рекомендациями:

1. в случае невозможности изъятия средства компьютерной техники, после его осмотре необходимо блокировать соответствующее помещение, отключать источ­ники энергопитания аппаратуры;
2. при изъятии, магнитного носителя информа­ции нужно их перемещать и хранить только в специальных опломбированных и экранированных контейнерах или в стандартных футлярах заводского изготов­ления, исключающих разрушающее воздействие различных электромагнитных и магнитных полей, направленных излучении;
3. при необходимости изъятия информации из оперативной памяти компьютера, ее копируют на физический носитель с использованием стандартных программных средств; 4) изъятие средств компьютерной техники производится только в выключенном состоянии.

При решении вопроса о возбуждении уголовного дела целесообразно ис­требовать:

* + журнал учета сбоев в работе компьютерной сети, выхода отдельных компьютеров или технических устройств из строя; журнал учета рабочего вре­мени;
  + документы о проведенных в течение дня операциях; физические (матери­альные) носители информации; программное обеспечение ЭВМ (при невозмож­ности изъять физические носители);
  + файл администратора сети, в котором фик­сируется вся работа сети (моменты включения и выключения, результаты тес­тирования, протоколы сбойных ситуаций);
  + системный блок и выносные нако­пители информации; информация (в виде файлов) о попытках незаконного ис­пользования компьютера, несанкционированного подключения к сети;
  + акты по результатам антивирусных проверок контрольные суммы файлов, которые хранятся в соответствующих программах; список лиц, которые имеют право доступа к той или иной компьютерной информации и список паролей, под кото­рыми они идентифицированы в компьютере;
  + технические средства распознания пользователей (магнитные карты, ключи блокировки и пр.) с целью предотвра­тить доступ пользователей к компьютерам в период проведения проверки; и др.

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

* + 1. Установлен неправомерный доступ к компьютерной информации, есть следы, есть подозреваемый, который дает правдивые показания.
    2. Установлен неправомерный доступ к компьютерной информации, имеются следы, прямо указывающие на конкретного подозреваемого, но он от­рицает свою причастность к совершению преступления.
    3. Установлен неправомерный доступ к компьютерной информации, из­вестны лица, несущие по своему служебному положению за это ответствен­ность, но характер их личной вины, а так же обстоятельства доступа не уста­новлены.
    4. Установлен факт неправомерного доступа к компьютерной информа­ции, совершить который и воспользоваться его результатами могли только лица из определенного круга (по своему положению, профессиональным навыкам и знаниям) либо известны лица (фирмы, организации), заинтересованные в полу­чении данной информации.

Последняя из приведенных следственных ситуаций, является наиболее сложной, так как отсутствуют сведения о виновном лице, следы преступления, не известен способ совершения и другие данные.

Для разрешения следственных ситуаций, складывающихся на первона­чальном этапе расследования, производятся следующие следственные действия: допрос свидетелей, обыск помещений, допрос подозреваемого, проверки по оперативно-справочным, розыскным и криминалистическим учетам.

Рассмотрим специфические особенности тактики проведения первоначальных следственных действий при расследовании непра­вомерного доступа к компьютерной информации. Учитывая особенности такти­ки, отмечается, что при его подготовке необходимо:

* выяснить, какая вычисли­тельная техника имеется в обыскиваемом помещении и ее количество;
* устано­вить, используется ли в комплекте с вычислительной техникой устройства автономного или бесперебойного питания;
* пригласить специалиста по компью­терным системам; подготовить соответствующую компьютерную технику;
* изучить личность владельца компьютера, его профессиональные навыки по владению компьютерной техникой;
* определить меры, обеспечивающие конфи­денциальность обыска;
* спрогнозировать характер возможно находящейся в компьютере информации; ее роль в быстром и результативном обыске, опре­делить, какую компьютерную информацию необходимо изучить на месте, а ка­кую изъять для дальнейшего исследования.

По прибытии к месту проведения обыска необходимо быстро и неожиданно войти в обыскиваемое помещение, после чего необходимо организовать охрану компьютеров. На обзорной ста­дии обыска необходимо:

* определить, соединены ли находящиеся в помещении компьютеры в локальную вычислительную сеть;
* установить, имеются ли соеди­нения компьютера с оборудованием или вычислительной техникой вне обыскиваемого помещения;
* выяснить, подключен ли компьютер к телефонной или телетайпной линиям;
* определить, запущены ли программы на ЭВМ и какие именно;
* установить, не содержится ли на компьютере информация, которая может способствовать более плодотворному поиску.

На детальной ста­дии обыска нужно четко организовать поисковые мероприятия, направленные на поиск тайников, в которых могут находиться обычные документы и пред­меты. Таким тайником может служить и сам компьютер. На заключительной стадии рассматриваемого следственного действия составляется протокол и описи к нему, вычерчиваются планы и схемы обыскиваемых помещений, про­водятся дополнительные фотосъемка и видеозапись.

# 4. Расследование неправомерного доступа к компью­терной информации на последующем этапе

На последующем этапе расследования неправомерного доступа к компью­терной информации, началом которого является привлечение лица в качестве обвиняемого, в зависимости от того, насколько обвиняемый признает свою ви­ну, могут складываться следующие следственные ситуации:

* 1. Обвиняемый признает свою вину и дает развернутые правдивые по­казания.
  2. Обвиняемый частично признает свою вину, но отрицает свое уча­стие в основных эпизодах преступной деятельности.
  3. Обвиняемые признают свою вину, но не установлены все эпизоды преступной деятельности.
  4. Обвиняемые (при совершении преступления группой лиц по пред­варительному сговору или организованной группой) отрицают свою причаст­ность к преступлению, дают противоречивые показания.
  5. Обвиняемый признает свою вину, но не называет соучастников пре­ступления.

Выдвигая и проверяя следственные версии, следователь проводит ком­плекс последующих следственных действий, в число которых входит: допрос обвиняемого (обвиняемых), очные ставки, назначение экспертиз, предъявление для опознания, следственный эксперимент, проверка и уточнение показаний на месте и др.

На последующем этапе расследования неправомерного доступа к компьютерной информации назначаются и проводятся различные экспертизы, в том числе традиционные кримина­листические, экспертизы веществ и материалов, экономические, инженерно-технические и другие экспертизы. Представляется, что можно выделить сле­дующие виды компьютерно-технических экспертиз, необходимость назначения которых возникает при расследовании неправомерного доступа к компьютерной информации:

1. техническая экспертиза компьютеров и периферийных устройств. Она назначается и проводится в целях изучения технических особенно­стей компьютера, его периферийных устройств, технических параметров ком­пьютерных сетей, а также причин возникновения сбоев в работе компьютерного оборудования;
2. техническая экспертиза оборудования защиты компьютерной информации. Проводится в целях изучения технических устройств защиты ин­формации, используемых на данном предприятии, организации, учреждении или фирме;
3. экспертиза машинных данных и программного обеспечения ЭВМ. Осуществляется в целях изучения информации, хранящейся в компьютере и на магнитных носителях, в том числе изучение программных методов защиты компьютерной информации;
4. экспертиза программного обеспечения и данных, используемых в компьютерной сети. Проводится в целях изучения информации, которая обрабатывается с помощью компьютерных сетей, эксплуатируемых на данном предприятия, организации, учреждении, фирме или компании.

Предъявление для опознания компьютерной информации, обладающей рядом идентификационных признаков, таких, как ее содержание, вид, атрибуты, носители, имена и размер файлов, даты и время их создания, шрифт, кегль (вы­сота букв), интерлиньяж (расстояние между строк), величину абзацных отступов) особый стиль выделения заголовков, размер полей, особенности нумерации страниц; назначение, выполняемые функции, интерфейс, графическое и музы­кальное оформление и т.д. принципиально возможно, но имеет определенные тактические особенности.

В практике при расследовании анализируемого преступления проводятся следующие эксперименты:

* по проверке возможности проникновения в помеще­ние (через двери, окно, с отключением и без отключения сигнализации);
* по про­верке возможности подключения компьютерной техники и совершения непо­средственного доступа к компьютерной информации;
* по проверке возможности проникновения в закрытые зоны (путем подбора паролей, идентификационных кодов и установлению периода времени на данный подбор);
* по проверке воз­можности подключения к компьютерной сети; по проверке возможности элек­тромагнитного перехвата;
* по установлению периода времени, необходимого на подключение к компьютерной сети; по установлению периода времени, необходимого на отключение технических средств защиты информации;
* по установ­лению промежутка времени, необходимого для модификации, копирования компьютерной информации;
* по проверке возможности совершения определен­ных операций с компьютерной информацией в одиночку;
* по проверке возмож­ности совершения определенных операций с помощью конкретной компьютер­ной техники за определенный промежуток времени и др.

Так же как иные след­ственные действия, производство следственного эксперимента при расследова­нии неправомерного доступа к компьютерной информации обладает рядом спе­цифических особенностей.

# Литература

1. Бахин В.П. Следственная тактика: проблемы изучения и совершенствования. — К., 1991.
2. Белкин Р.С. Курс криминалистики. 3 т. — М., “Юрист”, 1997.
3. Гаврилин Ю.В. Особенности криминалистической характеристики неправомерного дос­тупа к компьютерной информации // Известия Тульского государственного уни­верситета. — Тула, 1999.
4. Криминалистика: Учебник / Под ред. В.А. Образцова. — М., “Юрист”, 1997.
5. Криминалистика: Учебник. / Под. ред. В.Ю. Шепитько. Х., Одиссей, 2001.
6. Расследование неправомерного доступа к компьютерной информации. Научно-практическое пособие. Под ред. Н.Г. Шурухнова. — М., 1999.
7. Реховский А.Ф. Теоретические учения о криминалистических версиях. — Владивосток, 1996.
8. Салтевский М.В. Криминалистика: Учебно-практическое пособие. Харьков, 1997.
9. Современное состояние законодательства в сфере компьютерной ин­формации // Материалы «Круглого стола» 23-24 сентября 1998 г. — Москва—Тула, 1999.