**ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**Информационные ресурсы и процесс информатизации**

**Государственная политика в сфере формирования информационных ресурсов и информатизации** должна быть направлена на создание условий для эффективного и качественного информационного обеспечения решения стратегических и оперативных задач социального и экономического развития страны, в частности:

• обеспечение условий для развития и защиты всех форм собственности на информационные ресурсы;

• формирование и защита государственных информационных ресурсов;

• создание и развитие федеральных и региональных информационных систем и сетей, обеспечение их совместимости и взаимодействия в едином информационном пространстве;

• создание условий для качественного и эффективного информационного обеспечения граждан, органов государственной власти, организаций и общественных объединений на основе государственных информационных ресурсов;

• обеспечение национальной безопасности в сфере информатизации, а также обеспечение реализации прав граждан, организаций в условиях информатизации;

• содействие формированию рынка информационных ресурсов, услуг, информационных систем, технологий, средств их обеспечения;

• формирование и осуществление единой научно-технической и промышленной политики в сфере информатизации с учетом современного мирового уровня развития информационных технологий;

• поддержка проектов и программ информатизации;

• создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов информатизации;

• развитие законодательства в сфере информационных процессов, информатизации и защиты информации.

**Документирование информации** является обязательным условием включения информации в информационные ресурсы. Документирование осуществляется в порядке, устанавливаемом органами государственной власти, ответственными за организацию делопроизводства, стандартизацию документов и их массивов.

Документ, полученный из информационной системы, приобретает юридическую силу после его подписания должностным лицом в порядке, установленном законом. Юридическая сила документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью.

Юридическая сила электронной цифровой подписи признается при наличии в информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдении установленного режима их использования. Право удостоверять идентичность электронной цифровой подписи осуществляется на основании лицензии.

***Информационные ресурсы*** могут быть государственными и негосударственными и как элемент состава имущества находятся в собственности граждан, органов государственной власти, органов местного самоуправления, организаций и общественных объединений. Отношения по поводу права собственности на информационные ресурсы регулируются соответствующим гражданским законодательством.

*Информационные ресурсы - отдельные Документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);*

*Информационные процессы - процессы сбора, обработки, накопления, хранения, поиска и распространения информации;*

*Информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих**информационные процессы.*

Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы на их средства, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти. Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке органы государственной власти и организации юридическими лицами независимо от их организационно правовой формы и форм собственности, а также гражданами на основании закона, формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию.

**Информационные ресурсы могут быть товаром,** за исключением случаев, предусмотренных соответствующим законодательством. Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услужили при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, ре1улируются договором.

**Государственные информационные ресурсы** формируются гражданами, органами государственной власти, органами местного самоуправления, организациями и общественными объединениям.

Документы, принадлежащие физическим и юридическим лицам, могут быть включены по желанию собственника в состав государственных информационных ресурсов по правилам, установленным для включения документов в соответствующие информационные системы.

Государственные информационные ресурсы - открыты и общедоступны. Исключение составляет документированная информация, отнесенная законом к категории ограниченного доступа.

Документированная информация с ограниченным доступом по условиям ее правового режима подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную.

**Персональные данные** относятся к категории конфиденциальной информации. Не допускаются сбор, хранение, использование и распространение информации о частной жизни, а равно информации, нарушающей личную или семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений физического лица без его согласия, кроме как на основании судебного решения.

Персональные данные не могут быть использованы в целях причинения имущественного и морального вреда гражданам, затруднения реализации их прав и свобод. Ограничение прав граждан на основе использования информации об их социальном происхождении, о расовой, национальной, языковой, религиозной и партийной принадлежности запрещено и карается в соответствии с законодательством.

***Информация*** *- сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;*

***Информатизация*** *- организационный социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов;*

***Информация о гражданах*** *(персональные данные) - сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его**личность.*

Юридические и физические лица, в соответствии со своими полномочиями владеющие информацией о гражданах, получающие и использующие ее, несут ответственность, согласно законодательству, за нарушение режима защиты, обработки и порядка использования этой информации.

При решении правовых вопросов в процессе внедрения современных информационных технологий, нельзя забывать о возможных нарушениях законных прав и интересов граждан в силу недобросовестного поведения пользователей таких систем, скажем, при несанкционированном использовании информации (неправомочным должностным лицом или посторонним) или ее умышленном искажении.

Процесс совершенствования демократии предполагает дальнейшее развитие системы гарантий прав личности от возможных злоупотреблений со стороны должностных лиц. Тем более, что в области охраны информации о личности еще имеется ряд пробелов.

Разумеется, тенденция к расширению числа видов информации о личности, накапливаемых банками данных, носит объективный характер, обусловлена возрастанием роли информации в решении масштабных производственных и социально-культурных задач. Однако представляется очевидным, что собираемые данные должны быть ограничены, во-первых, лишь наиболее необходимыми сведениями, во-вторых, реальной возможностью нанесения вреда законным интересам граждан, о которых информация собирается, должно исключать сбор такой информации.

Появление крупных электронных информационных систем, накапливающих огромные массивы сведений такого рода, позволяет достаточно конкретно создавать образ человека и разрабатывать соответствующую систему контроля за ним. И не только за отдельным человеком, но и за группой людей.

В результате ставится под сомнение общепринятый принцип «презумпции невиновности», так как человек, за которым ведется наблюдение незаконно, без его ведома, попадает в положение подозреваемого или даже обвиняемого.

В плане взаимосвязи обеспечения и законности реализации прав и свобод граждан, а также использования возможностей ЭВТ, следует обратить внимание на опыт развитых стран в этой сфере отношений. Так конгрессом США были приняты соответствующие законы, позволяющие гражданам, средствам массово информации и частным организациям знакомиться с информацией федеральных правительственных учреждений.

Право граждан затребовать информацию касается документации федеральных органов исполнительно власти: министерств, административных и военных ведомств, правительственных корпораций и иных учреждений. Под действие этих законов не подпадает документация таких выборных должностей, как президент, вице-президент, сенаторы и члены палаты представителей конгресса.

Кроме того, закон о свободе информации установил ряд ограничений на общие правила, оговорив конкретные категории информации, не выдаваемой гражданам по их запросам. Это:

• засекреченные документы;

• внутриведомственные служебные правила, инструкции, предписания;

• информация, не подлежащая разглашению в соответствии с другими законодательными актами;

• конфиденциальная деловая информация (коммерческая и финансовая информация о предпринимательской деятельности частных лиц и корпораций);

• внутриведомственная служебная корреспонденция;

• информация, затрагивающая частную жизнь человека;

• информация об оперативной и следственной работе правоохранительных органов;

• информация финансовых учреждений.

В тех случаях, когда использование информации может повлечь лишение гражданина прав, льгот или привилегий, гарантируемых федеральными программами социальной помощи, учреждение должно получать информацию по возможности непосредственно от гражданина.

***Документированная информация*** *(документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать;*

***Владелец информационных ресурсов,*** *информационных систем, технологий и средств их обеспечения - субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных Законом;*

***Пользователь (потребитель) информации -*** *субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.*

**Регламентация доступа к информационным ресурсам**

Пользователи - граждане, органы государственной власти, органы местного самоуправления, организации и общественные объединения - обладают равными правами на доступ к государственным информационным ресурсам и не обязаны обосновывать перед владельцем этих ресурсов необходимость получения запрашиваемойими информации. Исключение составляет информация с ограниченным доступом.

Доступ физических и юридических лиц к государственным информационным ресурсам является основой осуществления общественного контроля за деятельностью органов государственной власти, органов местного самоуправления, общественных, политических и иных организаций, а также за состоянием экономики, экологии и других сфер общественной жизни.

Информация, полученная на законных основаниях из государственных информационных ресурсов гражданами и организациями, может быть использована ими для создания производной информации в целях ее коммерческого распространения с обязательной ссылкой на источник информации. Источником прибыли в этом случае является результат труда и вложенных средств при создании производной информации, но не исходная информация.

Порядок накопления и обработки документированной информации с ограниченным доступом, правила ее защиты и порядок доступа к ней определяются органами государственной власти, ответственными за определенные массивы и вид информации, в соответствии с их компетенцией, либо непосредственно ее собственником, в соответствии с законодательством.

Граждане и организации имеют право на доступ к документированной информации о них, на уточнение этой информации в целях обеспечения ее полноты и достоверности, имеют право знать, кто и в каких целях использует или использовал эту информацию. Ограничение доступа граждан и организаций к информации о них допустимо лишь на основаниях, предусмотренных законами.

Владелец информационных ресурсов обязан обеспечить соблюдение режима обработки и правил предоставления информации пользователю, установленных соответствующим законодательством иди собственником этих информационных ресурсов, в соответствии с законодательством. Владелец информационных ресурсов несет юридическую ответственность за нарушение правил работы с информацией в порядке, предусмотренном соответствующим законодательством.

**Информационные системы как объект защиты информации**

Все виды производства информационных систем и сетей, технологий и средств их обеспечения составляют специальную отрасль экономической деятельности, развитие которой определяется государственной научно-технической и промышленной политикой информатизации.

Государственные и негосударственные организации, а также граждане имеют равные права на разработку и производство информационных систем, технологий и средств их обеспечения.

Информационные системы, технологии и средства их обеспечения могут быть объектами собственности физических и юридических лиц, государства. Собственником информационной системы, технологии и средств их обеспечения признается физическое или юридическое лицо, на средства которого эти объекты произведены, приобретены или получены в порядке наследования, дарения или иным законным способом.

Информационные системы, технологии и средства их обеспечения выступают в качестве товара (продукции) при соблюдении исключительных прав их разработчиков. Собственник информационной системы, технологии и средств их обеспечения определяет условия использования этой продукции.

***Средства обеспечения информационных систем*** *и их технологии - программные! технические, лингвистические, правовые, организационные средства (программы для электронных вычислительных машин; средства вычислительной техники и связи; словари, тезаурусы и классификаторы; инструкции и методики; положения, уставы, должностные инструкции; схемы и их описания, другая эксплуатационная и сопроводительная документация), используемые или создаваемые при проектировании информационных систем и обеспечивающие их эксплуатацию;*

***Собственник информационных ресурсов,*** *информационных систем, технологий и средств их обеспечения - субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами;*

Право авторства и право собственности на информационные системы, технологии и средства их обеспечения могут принадлежать разным лицам. Собственник информационной системы, технологии и средств их обеспечения обязан защищать права их автора в соответствии с законодательством

Информационные системы, базы и банки данных, предназначенные для информационного обслуживания граждан и организаций, подлежат сертификации в установленном порядке.

Организации, выполняющие работы в области проектирования, производства средств защиты информации и обработки персональных данных, получают лицензии на этот вид деятельности. Порядок лицензирования определяется соответствующим законодательством.

Предназначение вычислительной системы для широкого круга пользователей, создает определенный риск в плане безопасности, поскольку не все клиенты будут выполнять требования по ее обеспечению.

Порядок хранения носителей информации должен быть четко определен в соответствующем правовом акте и предусматривать полную сохранность носителей информации, удобство отыскания необходимых носителей контроль за работой с информацией, ответственность за несанкционированный доступ к носителям информации с целью снятия с них копий, изменения или разрушения и т.д.

Можно скрыто получить доступ к информационным архивам, которые концентрируются в одно месте в больших объемах. Кроме того, появилась возможность дистанционного получения информации через терминалы, расположенные в удалении от мест хранения данных. Поэтому для защиты информации требуются принципиально новые методы и средства, разработанные с учетом ценности информации, условий работы, технических и программных возможностей ЭВМ и других средств сбора, передачи и обработки данных. Особые мероприятия защиты необходимы, когда ресурсы ЭВМ используются несколькими абонентами через терминалы в многопрограммном режиме и в режиме разделения времени.

В этой главе возникает ряд правовых проблем, связанных с массивами информации, сконцентрированных в банках данных, и знаний, представляющих собой общественную и национальную ценность, а их содержание - национальный секрет. Использование такой информации не по назначению наносит значительный ущерб как обществу в целом, так и отдельной личности.

Уместно обратить внимание на правовые аспекты защиты информации, которые могут возникнуть при недостаточно продуманном или злонамеренном использовании электронно-вычислительной техники. К ним относятся:

*1. Правовые вопросы защиты массивов информации от искажений и установления юридической ответственности по обеспечению сохранности информации. 2. Юридические и технические вопросы зашиты хранящейся информации от несанкционированного доступа к ней, исключающие возможность неправомерного использования ее.*

*3. Установление юридически закрепленных норм и методов защиты авторских прав и приоритетов разработчиков программного продукта.*

*4. Разработка мероприятий по приданию юридической силы документам, выдаваемым машинами, и формирование юридических норм, определяющих лиц, ответственных за доброкачественность других документов.*

*5. Правовая защита интересов экспертов, передающих свои знания в фонды банков данных.*

*6. Установление правовых норм и юридической ответственности за использование электронно-вычислительных средств в личных интересах*, противоречащих интересам других личностей и общества и могущих нанести им вред.

Отсутствие надлежащей регистрации и контроля работ, низкая трудовая и производственная дисциплина персонала, доступ посторонних лиц к вычислительным ресурсам создает условия для злоупотреблений и вызывает трудности их обнаружения.

В каждом вычислительном центре принято устанавливать и строго соблюдать регламент доступа в различные служебные помещения для разных категорий сотрудников.

*Степень защиты информации от неправомерного доступа и противозаконных действий зависит от качества разработки организационных мер, направленных на исключение:*

*• доступа к аппаратуре обработки информации;*

*• бесконтрольного выноса персоналом различных носителей информации;*

*• несанкционированного введения данных в память, изменения или стирания хранящейся в ней информации;*

*• незаконного пользования системами обработки информации и полученными данными;*

*• доступа в системы обработки информации посредством самодельных устройств;*

*• неправомочной передачи данных по каналам связи из информационно-вычислительного центра;*

*• бесконтрольный ввод данных в систему;*

*• обработка данных по заказу без соответствующего требования заказчика;*

*• неправомочное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.*

Целью защиты информации является:

• предотвращение утечки, хищения, утраты, искажения, подделки информации;

• предотвращение угроз безопасности личности, общества, государства;

• предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

• предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;

• обеспечение правового режима документированной информации как объекта собственности;

• защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

• сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

• гарантия прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

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

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно-технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти.

Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

*Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований. Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах.*

*Собственник документа, массива документов, информационных систем или уполномоченные им лица в соответствии с законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа**пользователей к информации.*

Владелец документа, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством.

Риск, связанный с использованием не сертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств. Риск, связанный с использованием информации, полученной из не сертифицированной системы, лежит на потребителе информации.

Защита прав субъектов в сфере формирования информационных ресурсов, пользования ими, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба.

Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и на граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров.

Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

**Руководители и другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.**

Однако ряд нормативных положений по защите информации в автоматизированных системах, разработанных ранее, не соответствует современным требованиям и современным информационным технологиям. Работы в этом направлении заметно отстают от потребностей и носят однобокий характер (в основном сведены к защите информации от утечки по техническим каналам перехвата).

Пока еще отсутствует нормативно-правовая и методическая база для построения автоматизированных и вычислительных систем в защищенном исполнении, пригодных для обработки секретной информации в государственных учреждениях и коммерческих структурах.

*При разработке средств защиты возникает ряд проблем правового характера:*

*1. Лицензирование деятельности по разработке программно-аппаратных средств цифровой подписи. Система лицензирования направлена на создание условий, при которых право заниматься защитой информации предоставлено только организациям, имеющим на этот вид деятельности соответствующее разрешение (лицензию).*

*2. Сертификация программно-аппаратных средств с функциями защиты.*

*3. Система сертификации направлена на защиту потребителя от недобросовестного исполнителя. В настоящее время фактически отсутствуют организационно-технические и организационно-методические документы по сертификации средств и комплексов защиты информации, в том числе связанных с криптографическими методами защиты.*

*3. Соответствие разрабатываемых средств защиты концептуальным требованиям к защите, стандартам и другим нормативным документам.*

*4. Отсутствие нормативно-правового обеспечения для решения спорных ситуаций с использованием цифровой подписи в арбитражном суде.*

Круг нормативных и концептуальных документов в области защиты информации крайне ограничен, а имеющиеся документы не в полной мере отвечают современным требованиям. Нормативно-правовые документы, содержащие термины и определения, концепцию применения и алгоритмы выработки и проверки цифровой подписи отсутствуют.

**Преступление в компьютерной сфере**

Развитие вычислительной техники и ее широкое применение государственными органами и частными учреждениями привели к возникновению и распространению так называемых компьютерных преступлений. Такое положение вызывает беспокойство и в тех организациях, где применяется компьютерная техника, и в органах поддержания правопорядка, и среди широких слоев населения, пользующихся новыми видами информационного обслуживания.

*Термин* ***«компьютерная преступность»*** *впервые был использован еще в начале 70-х годов. Однако до настоящего времени продолжается дискуссия о том, какие противозаконные действия подразумеваются под ним. Было предложено ряд уголовно-правовых определений компьютерной преступности. Часто оно трактуется как преступление, прямо или косвенно связанное с ЭВМ, включающее в себя целую серию незаконных актов, совершаемых либо с помощью системы электронной обработки данных, либо против нее. Другие под компьютерной преступностью подразумевают любое деяние, влекущее незаконное вмешательство в имущественные права, возникающее в связи с использованием ЭВМ. Третьи вкладывают в это определение все преднамеренные и противозаконные действия, которые приводят к нанесению ущерба имуществу, совершение которых стало возможным, прежде всего, благодаря электронной обработке информации.*

Выделяют следующие формы проявления компьютерной преступности: манипуляции с ЭВМ, хищение машинного времени, экономический шпионаж, саботаж, компьютерное вымогательство, деятельность «хакеров».

Под **компьютерными манипуляциями** подразумевается неправомочное изменение содержимого носителя информации и программ, а также недопустимое вмешательство в процесс обработки данных. Основные сферы компьютерных манипуляций таковы: совершение покупок и кредитование (манипуляции с расчетами и платежами, доставка товаров по ложному адресу); сбыт товара и счета дебиторов (уничтожение счетов или условий, оговоренных в счетах, махинации с активами); расчеты заработной платы (изменение отдельных статей начисления платежей, внесение в платежную ведомость фиктивных лиц). Для компьютерных манипуляций характерны некоторые особенности, обусловленные спецификой самого объекта преступных действий. Например, используется возможность отладки программ, составленных с преступными целями; многократная реализация однажды найденной возможности для незаконных действий.

Вследствие простоты передачи программного обеспечения в сетях и машинах возникает опасность заражения их компьютерным «вирусом», т.е. опасность появления программ, способных присоединяться к другим программам машины и нарушать ее работу.

Противозаконные манипуляции с системным программным обеспечением доступны только узкому кругу специалистов-программистов. Значительно меньший объем специальных знаний необходим для осуществления манипуляций с входными и выходными данными. Такие неправомочные действия могут совершать даже лица, не имеющие непосредственного отношения к информационной технике.

Наряду с непосредственным незаконным использованием информационных систем к категории преступлений относятся также действия, связанные с несанкционированным доступом к сети передачи информации и проведение идентификационных процедур.

**Незаконное получение информации** может осуществляться и путем регистрации электромагнитного излучения различных устройств, используемых в процессе ее обработки.

*Распространенным способом совершения компьютерных преступлений анализируемой категории является незаконный доступ в информационные системы. Для его осуществления преступник должен располагать следующими исходными данными: телефонным номером подключения к системе, процедурой заявки, ключевым словом, номером счета. Номер телефонного подключения к информационной системе чаще всего имеется в телефонной книге для внутреннего пользования организации. Данный номер может быть передан преступнику сотрудниками этой организации или идентифицирован правонарушителем с помощью программы поиска. Остальная исходная информация также* может быть передана преступнику сотрудниками учреждения, имеющими к ней доступ.

**Компьютерный шпионаж** преследует, как правило, экономические цели. Преступления этой категории чаще всего совершаются для получения следующей информации: программ обработки данных, результатов научных исследований, конструкторской документации и калькуляции, сведений о стратегии сбыта продукции и списков клиентов конкурирующих фирм, административных данных, сведений о планах и о технологии производства.

Наиболее распространенная в настоящее время форма компьютерных преступлений - деятельность **хакеров**, владельцев персональных компьютеров, незаконно проникающих в информационные сети. Хакеры - это квалифицированные и изобретательные программисты, занимающиеся разными видами компьютерных махинаций, начиная с нарушений запретов на доступ к компьютерам в совокупности с их несанкционированным использованием, вплоть до хищения секретных сведений.

Компьютерные преступления отличаются от обычных особенными пространственно-временными характеристиками. Так, подобные деяния совершаются в течение нескольких секунд, а пространственные ограничения оказываются полностью устраненными. Лица, совершающие компьютерные преступления, также имеют свои особенности: они, как правило, молоды, имеют высшее образование, знакомы с методами раскрытия кодов и внедрения в компьютерные системы.

*Как свидетельствует практика, один из важнейших способов повышения эффективности борьбы с компьютерной преступностью - создание надлежащей правовой основы для преследования в уголовном порядке лиц, виновных в преступлениях такого рода. В настоящее время развитие правовой основы для борьбы с преступлениями, объектом которых является «интеллектуальный» элемент ЭВМ, идет в следующих направлениях:*

*1. Создание уголовно-правовых норм, предусматривающих раздельную защиту программного обеспечения ЭВМ и баз данных, а также «осязаемых» элементов электронно-вычислительных систем;*

*2. Использование существующего законодательства.*

Несмотря на то, что существующие уголовные законы достаточно гибки для квалификации нарушений этого типа, однако социальные и технические изменения создают все новые и новые проблемы, часть которых оказывается вне рамок любой из нынешних правовых систем. Потому и «подготовка нормативно-правовых актов о компьютерной безопасности исключительно сложна, поскольку связана с технологией, опережающей нормотворческий процесс».

Развитие законодательства не всегда успевает за развитием техники и преступным использованием ее последних достижений. Так, в существующем законодательстве отсутствуют правовые нормы относительно преступлений, совершаемых с помощью ЭВМ. Это порождает проблему: каким образом обвинять преступников посредством обычных норм права.

В компьютерных преступлениях ЭВМ может быть как объектом, так и субъектом преступления. В тех случаях, когда ЭВМ - объект преступления, т.е. ей наносится материальный ущерб путем физического повреждения, не возникает проблем с применением существующего законодательства. Но те случаи, когда ЭВМ используется для совершения актов обмана, укрывательства или присвоения с целью получения денег, услуг, собственности или деловых преимуществ, представляют собой новые правовые ситуации.

Существует ряд характерных черт преступлений, связанных с использованием ЭВМ, которые усложняют расследование и предъявление обвинения по ним. Помимо юридических трудностей возникают и другие проблемы, с которыми может столкнуться следствие. Среди них:

• сложность обнаружения преступлений, связанных с использованием ЭВМ;

• большая дальность действия современных средств связи делает возможным внесение незаконных изменений в программу ЭВМ с помощью дистанционных терминалов либо закодированных телефонных сигналов практически из любого района;

• затруднения в понимании порядка работы ЭВМ в технологически сложных случаях;

• информация преступного характера, заложенная в память ЭВМ и служащая доказательством для обвинения, может быть ликвидирована почти мгновенно;

• обычные методы финансовой ревизии в случае этих преступлений не применимы, т.к. для передачи информации используются электронные импульсы, а не финансовые документы.

В 1988 г. только в Европе было совершено четыре неудачных попытки нелегального перевода денег с банковских счетов (потери в каждом из этих случаев могли превысить сумму в 50 млн. дол.). Характерно, что все эти попытки оказались неудачными только благодаря «чрезмерной жадности» преступников. В Чикаго, например, 7 преступников решили похитить 70 млн. дол. и были задержаны в тот момент, когда имели на своем счету более 49 млн. дол.

Кроме того, отмечается, что только 3 из 20 обнаруженных случаев регистрируются в полицейской статистике, и только 1 из 33 зарегистрированных случаев заканчивается вынесением обвинения. В целом наказание следует только в одном из 22 тыс. компьютерных преступлений.

*Согласно анализу более чем 3 тыс. досье таких преступлений, накопленных в международном институте SRI interational известным экспертом в данной области Доном Паркером (организатором international information integnity institut), компьютеры, данные и программы могут быть: а)объектом нападения; б)объектом совершения преступления; в) средством подготовки преступлений; г) средством запугивания или обмана. С учетом темпов компьютеризации общества, а также масштабов и возможностей компьютерных злоупотреблений можно полагать, что к 2000 г. практически все преступления в деловой сфере будут совершаться при помощи компьютеров, а ущерб от компьютерной преступности будет расти экспоненциально, возможно, при некоторой стабилизации числа таких преступлений. При этом некоторые западные аналитики утверждают, что обнаруживается* только 1 из 100 компьютерных преступлений.

**Средняя стоимость потерь одного компьютерного преступления оценивается в 450 тыс. дол.** и значительно превышает средний ущерб от ограблений банков и других видов преступлений (по даннымФБР, среди стоимость потерь от ограбления банков в США составляет 3,2 тыс. дол. и от мошенничества - 23 тыс. дол Темпы роста потерь от компьютерных злоупотреблений существенно зависят от видов преступлений и мо1 достигать 430 тыс. дол. в год (как это наблюдалось в США в 1982 г., когда объем потерь от злоупотреблений) банковскими кредитными карточками в течение 12 месяцев увеличился с 5,5 до 29 млн. дол.).

Большинство пострадавших обращаются в правоохранительные органы, если их потери превышают 15-150 тыс. да и при этом только в 60-65 случаях обвиняемые подпадают под действие существующего в США законодательства

*Основным действующим лицом при совершении компьютерных преступлений в сфере бизнеса становятся высокообразованные «белые воротнички» из числа сотрудников пострадавших организаций. По данным MIS Traiding institut (США), на их долю приходится 63% всех случаев рассматриваемых преступлений и злоупотреблений. Более чем 36% нарушивших закон сотрудников относится к категории не руководящего персонала, не связанного непосредственно с обслуживанием и эксплуатацией компьютеров, 29%-профессиональные программисты, 25% - прочие сотрудники вычислительных центров обслуживающий персонал, операторы ЭВМ и пр., 7% - руководители соответствующих компьютерных центров.*

Существенно меняются и мотивы преступлений. На первый план выдвигаются проблемы личного план (работа, борьба за сохранение положения и выживание фирмы, месть, стремление к превосходству, ревность здоровье, физическая или нравственная зависимость, увлечения, финансовый или семейный кризис, стремление к самоутверждению и т.д.). Эту тенденцию отражает и официальная статистика, согласно которой около 40% компьютерных преступлений совершается для решения финансовых проблем, 20% мотивируется «интеллектуальным вызовом» обществу, 17% - стремлением решить личные проблемы производственного характера, 8% - проблемы корпорации или организации, 4% - стремлением к общественному признанию, 3% -ущемлением прав и т.д.

Возникновение компьютерной преступности и масштабы ущерба вызвали необходимость разработки законодательных норм, устанавливающих ответственность за подобные действия. Все изложенное в полной мер относится и к Российской Федерации, где взрыв компьютерной преступности сдерживается только слабым развитием информатизации. Однако там, где вычислительная техника используется широко, информационные преступления уже наблюдаются. В качестве примера можно привести случай во Внешэкономбанке РФ где из-под учета ЭВМ было выведено около 1 млн. дол., а 125 тыс. дол. - похищено.

Вместе с тем, отсутствие надежных защищенных автоматизированных систем межбанковских расчете позволяет совершать массовые хищения денежных средств («дело о 30 миллиардах»).

Массовый характер приобрело распространение компьютерных вирусов. Внедрение программы-вируса в технологическую АСУ Игналинской АЭС привело к аварийной остановке реактора, что само по себе - серьезное нарушение ядерной безопасности.

На первый взгляд кажется, что компьютерные преступления могут быть расследованы в соответствии с традиционным законодательством, относящимся к краже, растрате, нанесению вреда собственности и т.д. Однако несоответствие традиционного уголовного законодательства в применении к этой новой форме преступления становится очевидным, как только мы попытаемся установить наличие всех элементов состава традиционного преступления, совершенных с помощью ЭВМ. Например, если злоумышленник вошел в помещение, где расположена ЭВМ, незаконно или с преступной целью, тогда закон может быть применен традиционно. Если преступник вошел в помещение, где находится ЭВМ, для того, чтобы причинить вред материальной части машины, украсть программу, то одно лишь вторжение с незаконным намерением будет достаточным для предъявления обвинения по делу. Однако, если лицо пытается получить доступ к данным, внесенным в память ЭВМ для того, чтобы похитить ценную информацию, хранящуюся в ЭВМ, предъявление обвинения, в соответствии с традиционным законом, вряд ли будет возможным. Доступ может быть получен через дистанционный терминал, установленный на дому у преступника или посредством секретного телефонного кода. Такие нетрадиционные формы «вторжения» не предусмотрены законом. Также не всегда возможно доказать, как того требует закон, что имело место какое-либо изъятие собственности. Например, компьютерная программа может быть «считана» с отдаленного компьютерного терминала. Такое изъятие не затрагивает элементов материальной реализации ЭВМ и может даже не затронуть программное обеспечение, т.к. закодированная информация может быть только списана (т.е. скопирована) где-либо еще, по-прежнему оставаясь в ЭВМ. Требования обычного права к такому составу преступления, как хищение, а именно, чтобы обязательно имело место «изъятие», - неадекватно по отношению к современным методам копирования и хищения информации, которые не изменяют оригинала и не изымают его физически из владения.

**До тех пор, пока не будет принят закон о защите информации и компьютерных преступлениях, эффективно бороться с правонарушениями в этой области будет невозможно.**

Принятие специального законодательства в отношении преступных действий, связанных с компьютеризацией, даст ряд положительных результатов.

*Во-первых, правоохранительные органы получат единообразное средство уголовного преследования лиц, использующих вычислительную технику в преступных целях.*

*Во-вторых, наличие законодательства, направленного на пресечение компьютерных преступлений, будет способствовать ограничению распространения этого вида преступления.*

*В-третьих, в будущем облегчит работу юридическим фирмам, которые хотели бы взять на себя охрану прав клиентов-владельцев ЭВМ.*

В-четвертых, принятие закона приведет к тому, что данные о компьютерных преступлениях будут концентрироваться в одном каком-то органе, что позволит не только иметь подробную статистику, но и создаст базу для научного анализа компьютерных преступлений.

В пользу законодательства, направленного на борьбу с компьютерными преступлениями говорит и тот факт, что государство опирается на вычислительную технику, а выведение ее из строя грозит серьезными последствиями во многих областях деятельности: экономической, финансовой, военной и многих других.

**Особенностью западного компьютерного права** является то, что, как правило, оно формируется по прецеденту и представляет собой в основном законодательные акты прямого действия, принимаемые на государственном (Великобритания, Франция, Германия) или федеративном и региональном уровнях (США).

*Ответственность за правонарушения при работе с информацией, компьютерами и компьютерной информацией устанавливается*

***В США:***

*Законом о безопасности компьютерных систем 1987 г.;*

*Актом о злоупотреблениях с использованием ЭВМ 1986 г.;*

*Законопроектом об искоренении компьютерного вируса 1988 г.;*

*Законом о свободе информации;*

***Законом о*** *соблюдении* ***тайн 1974 г.;***

*Законом о финансовых тайнах;*

*Законом о справедливых кредитах;*

*Законом о защите вычислительных средств небольших фирм и образовании 1984 г.*

***В Канаде:***

*Законом о компьютерных и информационных преступлениях («Билль» С-18) 1985 г.* ***Во Франции:***

*Законом об информатике, картотеках и свободах 1978 г.* ***В Великобритании:***

***Законом о*** *защите информации* ***1984 г.***

***В ФРГ:***

*Законом о дальнейшем развитии электронной обработки и о защите данных 1990 г.;*

*Законом о хозяйственной преступности 1986 г.;*

*Германским Уголовным кодексом 1986 г.;*

*Германским Гражданским кодексом;*

*Законом об авторском праве;*

*Федеральным законом о защите данных 1978 г.*

Федеральный закон ФРГ об охране данных обязывает учреждения и организации принимать необходимые технические и организационные меры по обеспечению сохранности указанных в законе данных. Действие закона не распространяется на широко известные или передаваемые устно сведения о том или ином лице, а также данные, хранящиеся в специальных актах и делах, доступ к которым строго ограничен.

Не подлежат охране данные, собираемые и обрабатываемые в целях их последующей публикации, показа или огласки средствами кино, радио и прессы. Порядок обращения с информацией в данной области регламентируется специальными законами.

В соответствии с законом об охране данных, объектом охраны являются содержащиеся в картотеках и памяти ЭВМ сведения, затрагивающие личные интересы граждан, и, будучи введенными в ЭВМ, легко могут быть доступны третьим лицам.

Национальный совет Австрии принял закон о неразглашении персональных данных. В нем указывается, что каждый гражданин имеет право требовать сохранения в тайне касающихся его личности данных. Если эти данные обрабатываются с помощью автоматизированных средств, он имеет право на исправление неточностей и на изъятие данных, собранных и обработанных недоступными методами. Разглашение тайны относительно хранящихся персональных данных и неправомочное вмешательство в их обработку может повлечь за собой наказание с лишением свободы сроком до одного года.

*При всем различии национальных законодательств в них имеется ряд общих моментов.*

*1. Практически* ***во всех*** *странах законодательно установлена ответственность за нарушение порядка обработки и использования персональных данных.*

*2. Информационные (компьютерные) преступления расцениваются как представляющие особую опасность для граждан, государства и общества в целом; характеризуются значительно более жесткими мерами наказания, чем аналогичные преступления, совершенные без использования компьютерной техники.*

*3. Квалифицируются как преступления также действия, создающие только предпосылки к нанесению ущерба, например попытка проникновения в систему, внедрение* программы-вируса и т.д.

**Российское законодательство по защите информационных технологий** предусматривает ответственность за совершение преступлений и правонарушений при работе с информацией, выраженной документально (бланк и пр.). Достаточно детально разработан вопрос установления ответственности за разглашение сведений, составляющих государственную и военную тайну.

*Существующее законодательство позволяет классифицировать и установить ответственность за различные формы преступлений и правонарушений, связанных с информацией, представленной в виде сведений или документов. К ним относятся:*

*• особо опасные государственные преступления (измена Родине, шпионаж, диверсия, разглашение государственной тайны, утрата документов, содержащих государственную или служебную тайну);*

*• корыстные преступления (хищение, грабеж, разбой, присвоение, подлог, подделка);*

*• преступления, совершенные по неосторожности или халатности (уничтожение, повреждение, утеря);*

*• хозяйственные преступления (выпуск недоброкачественной продукции).*

Всего в УК РФ в настоящее время содержится 22 нормы, предусматривающие ответственность за перечисленные преступления. Рядом статей АК РФ также устанавливается административная ответственность за правонарушения, не представляющие собой большой общественной опасности.

Очевидно, что правоохранительное законодательство в области информационной безопасности должно максимально базироваться на существующих нормах уголовного и административного права. Однако в законодательстве до настоящего времени не нашли отражения две обширные темы, непосредственно связанные с обработкой информации и обеспечением прав личности.

Во-первых, **не установлена ответственность за нарушение прав личности путем незаконного сбора персональных данных, их обработки, разглашения и отказа источнику в доступе к ним.**

Во-вторых, **отсутствуют разделы, устанавливающие ответственность субъектов отношений, возникающих на основе использования новых информационных технологий.**

В то же время обработка информации с использованием новых информационных технологий имеет ряд существенных особенностей. К ним относятся:

• существование информации и программ в виде нематериальной «электронной копии»;

• возможность неограниченного, скрытого и бесследного доступа посторонних лиц к «электронной копии» информации и программ с целью их хищения (копирования), модификации или уничтожения;

• возможность введения в ЭВМ не оговоренных технологией программных средств, в том числе и вирусного характера, что само по себе представляет серьезную угрозу.

*Как утверждают специалисты, для решения задачи установления ответственности за злоупотребления с использованием компьютерной техники целесообразно:*

*1. Распространить на информацию и программы для ЭВМ, представленные в форме «Электронной копии», свойства объекта имущественного права, т.е. признать их объектом права собственности и товарным продуктом.*

*2. Установить правовой режим информации, предусматривающий ее обязательное документирование (как механизм признания информации объектом права собственности).*

*3. Признать противоправными умышленные деяния, подпадающие под категории «нарушение норм защиты», «хищение» (копирование),»несанкционированный доступ» и «разработка», а также - распространение компьютерных вирусов» вне зависимости от последствий, к которым они привели.*

*4. Установить ответственность администрации за непринятие мер безопасности, приведшее к совершению компьютерных преступлений.*

Ан*ализ субъектов информационных отношений показывает, что среди них выделяются следующие категории лиц:*

*• владельцы информационных систем;*

*• персонал информационных систем;*

*• собственники информации;*

*• источники информации;*

*• пользователи;*

*• посторонние лица.*

*В среде традиционной обработки информации все указанные категории можно разделить на две группы: лица, которым разрешен доступ к информации, и лица, которым такой доступ не разрешен. Правонарушения и преступления могут быть совершены:*

*• по неосторожности (по некомпетентности);*

*• по халатности;*

*• умышленно.*

*При классификации правонарушений и преступлений следует руководствоваться также: их высокой общественной опасностью, что требует классифицировать даже те действия, которые не нанесли ущерба, но создали предпосылки для его нанесения нарушение технологии обработки, нарушение норм защищенности, непринятие должных мер по организации защиты); степенью ущерба. При этом* ***ущерб******от совершенного преступления*** *может выражаться в форме:*

*• упущенной выгоды;*

*• прямых финансовых потерь;*

*• морального ущерба.*

*Иногда задача оценки информации в стоимостном выражении крайне проблематична и часто напрямую не может быть решена, например при возникновении угроз информационным системам, обрабатывающим секретную информацию. В этом случае ответственность устанавливается по аналогии с действующими нормами уголовного права.*

*Анализ показывает, что в целом* ***можно выделить следующие критерии состава злоупотреблений в сфере обработки информации****:*

*1. Нарушение правил регистрации информационных систем и перечней обрабатываемой информации.*

*2. Нарушение правил сбора информации, а именно: получение информации без разрешения и сбор ее сверх разрешенного перечня.*

*3. Хранение персональной информации сверх установленного срока.*

*4. Ненадлежащее хранение информации.*

*5. Передача третьим лицам сведений, составляющих коммерческую тайну, или персональных сведений-*

*6. Несвоевременное информирование населения о событиях, явлениях и фактах, могущих причинить вред их здоровью или нанести материальный ущерб.*

*7. Превышение пределов компетенции учетной деятельности, допущение неполных учетных записей ифальсификации данных.*

*8. Предоставление заинтересованным лицам заведомо неточной информации.*

*9. Нарушение установленного порядка обеспечения безопасности информации.*

*10. Нарушение правил и технологии безопасной обработки информации.*

*11. Нарушение норм защищенности информации, установленных Законом.*

*12. Нарушение правил доступа к информации или к техническим средствам.*

*13. Нарушение механизма защиты информации и проникновение в систему.*

*14. Обход средств защиты и проникновение в систему.*

*15. Хищение информации с использованием:*

*а) технических средств,*

*б) доступа к носителям данных.*

*16. Несанкционированное уничтожение данных в информационных системах.*

*17. Несанкционированная модификация данных в информационных системах.*

*18. Искажение (модификация) программного обеспечения.*

*19. Перехват электромагнитных, акустических или оптических излучений.*

*20. Перехват информации, передаваемой по пиниям связи путем подключения к ним дистанционного (бесконтактного) съема или любыми другими известными способами.*

*21. Изготовление и распространение заведомо непригодного ПО.*

*22. Распространение компьютерных вирусов.*

*23. Разглашение парольно-ключевой информации.*

*24. Несанкционированное ознакомление (попытка) с защищаемыми данными.*

*25. Несанкционированное копирование (хищение).*

*26. Внесение в программную среду не оговоренных изменений, в том числе и вирусного характера.*

*Анализ уголовных дел и иной доступной информации показал, что механизм совершения преступления в целом состоит в следующем:*

*• преступники имели отношение к разработке программного обеспечения и эксплуатации компьютерной техники;*

*• использовали указанные возможности для несанкционированного дописывания в массивы «операционного дня» необходимой им информации;*

*• несанкционированный доступ осуществлялся в течение короткого времени (до 1 минуты) под видом законного пользователя с неизвестного терминала, имеющего телекоммуникационную связь с единой сетью ЭВМ;*

*• для дальнейших операций была заранее разработана и внедрена специальная программа, которая в пользу каких-либо лиц (юридических или физических, реальных и вымышленных) открыла технологические счета, имеющие первоначально нулевой остаток, в РКЦ были дополнительно внедрены для дальнейшей обработки и рассылки по нужным адресам бумажные носители - фальшивые платежные поручения с поддельными печатями РКЦ, якобы прошедшие там обработку;*

*• для усложнения бухгалтерского контроля под предлогом произошедшего, якобы, сбоя программы не выдавались необходимые документы: контрольные и оборотные ведомости по балансовым счетам, а также ведомость остатков в разрезе кодов валют за день перерасчета (как это реально случилось с одним крупным российским банком);*

*• получение со счетов наличными осуществлялось в заранее разработанном порядке и без следов.*

*Возможность осуществления преступных деяний в областях автоматизации производства и бухгалтерского учета заключалась прежде всего в слабой готовности противостоять мошенничеству, неумении осуществить систему разделения доступа,* обновления паролей, ключевых слов и т.д.

Наиболее опасными субъектами компьютерных мошенничеств являются так называемые **хакеры, крекеры** и представители групп, занимающихся промышленным шпионажем. В этой связи, как рекомендуют специалисты по безопасности, особое внимание следует обращать на вновь принимаемых сотрудников-специалистов в области компьютерной техники, программирования и защиты компьютерной информации.

Известны случаи, когда отдельные хакеры в целях личного обогащения пытались устроиться на работу в информационные службы крупных коммерческих структур. Но наибольшую опасность могут представлять такие специалисты в сговоре с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами; в этих случаях причиняемый ущерб и тяжесть последствий значительно увеличиваются.

Стали использовать компьютеры в преступных целях и сами руководители коммерческих и банковских структур для нанесения финансового ущерба государству. Так, в 1994 г. президент одного из сибирских коммерческих банков дал прямое указание оператору банка о внесении изменений в программное обеспечение системы электронных платежей через РКЦ. В результате банк незаконно получил 510 млн. руб.

Необходимо также учитывать, что по мере освоения компьютерной техники усложняется и механизм ее использования в различных правонарушениях. Увеличивается число преступлений «со взломом». В общем виде используемая компьютерными преступниками методика «взлома» или несанкционированного доступа сводится к двум разновидностям:

*•* **«Взлом изнутри»** преступник имеет физический доступ к терминалу, с которого доступна интересующая его информация, и может определенное время работать на нем без постороннего контроля.

*•* **«Взлом извне»**: преступник не имеет непосредственного доступа к компьютерной системе,но имеетвозможность проникнуть (обычно посредством удаленного доступа через сети) в защищенную систему для внедрения специальных программ, проведения манипуляций с обрабатываемой или хранящейся в системе информацией или осуществления других противозаконных действий.

Анализ подобных деяний свидетельствует, что разовые преступления по проникновению в системы со своих или соседних рабочих мест постепенно перерастают в сетевые компьютерные преступления путем «взлома» защитных систем организаций.

Оценка потерь от компьютерных преступлений, которые несет экономика в развитых странах Запада, составляет гигантские цифры - миллиарды долларов. Стоит напомнить, что Европа не имеет столь высокого уровня уголовных преступлений, как Россия, однако развитие технического прогресса прямо пропорционально бурному росту компьютерных мошенничеств.

Одно из первых криминальных использований компьютерной техники в СССР относится к 1979 г., когда в Вильнюсе было похищено свыше 78 тыс. руб., а в последние годы компьютеры применялись уже не только для хищений и разного рода мошенничеств, но и для изготовления поддельных денежных знаков, различных банковских платежных документов, кредитных, дебитных карт, различного рода карт-систем (для таксофонов, спутникового телевидения, сотовых радиотелефонов и пр.). В РФ отмечены случаи компьютерного хулиганства со значительным ущербом (заражение ЭВМ Игналинской АЭС вирусными программами в 1993 г.).

**Наиболее известные случаи из компьютерной криминалистики:**

1. Август 1994 г. Группа лиц, используя компьютерную связь, похитила в Мытищинском отделении «Уникомбанка» 150 тыс. дол.

2. Февраль 1995 г. Одно из отделений Московского Сбербанка РФ. Не установленные лица совершили несанкционированный доступ в систему передачи платежных документов из отделения банка в ОПЕРУ. Преступники, безусловно, хорошо знавшие технологию обработки данных «операционного дня» по всем филиалам отделения и их передачи для произведения расчетов, изготовили повторное сообщение, предварительно включив в общую сумму платежей дополнительную сумму в 2 млрд. руб., планируемую для хищения. Данное повторное сообщение было передано через некоторое время после первого сеанса. Во втором сеансе было передано на один (ложный) документ больше и на указанную сумму. Поскольку протокол связи с ОПЕРУ построен так, что каждый новый сеанс замешает данные предыдущего, то в ОПЕРУ были приняты последние документы и проведены по корсчету отделения. Для успешного завершения преступления были выведены из строя модемная связь отделения банка и сетевой компьютер повреждением кабеля связи с АТС; в связи с этим электронная выписка не была получена вовремя. Замечено, что несанкционированный вход осуществлен с не установленного места вне сети банка. Первичная передача данных произведена по сети «Искра», повторная - по сети «Инфотел». Хищение денежных средств предотвращено в результате обнаружения в коммерческом банке, куда был перечислены 2 млрд. руб., фальшивого платежного поручения.

3. Июль 1995 г. Ленинградское отделение Сбербанка г. Калининграда. Не установленные лица, используя систему международных денежных переводов «Вестерн Юнион» несанкционированно вошли в банковскую систему извне, внесли произвольные записи на сумму 100 тыс. дол. Ввели необходимые реквизиты для их перечисления и последующего обналичивания. В связи с установленными ограничениями сумм выплат, указанное количество валютных средств было распределено на суммы по 50 тыс. дол., которые переадресованы на счета банков Литвы, расположенных в двух городах, где и были сняты неким гражданином по предъявленному загранпаспорту.

4. Несколько слов о «деле Левина». По классификации Интерпола оно квалифицируется как «транснациональное сетевое компьютерное преступление». «Дело» явилось первым зарегистрированным случаем в России, по которому правоохранительными органами велась разработка.

*В связи с тем, что данное преступление является на сегодня в своем роде уникальным, оно представляет большой общественный интерес. В то же время многие обстоятельства до конца не установлены, и информация по «делу» достаточно противоречива. Однако соответствующие специалисты подготовили анализ основных моментов «дела».*

*Владимир Левин работал в одной из фирм Санкт-Петербурга, которая занималась распространением и обслуживанием компьютерной техники. В составе группы лиц Левин, используя телекоммуникационные линии связи, несанкционированно входил в систему управления наличными фондами Ситибанка и вводил команды о переводе с различных счетов этого финансового учреждения на необходимые счета различных сумм денег.*

*В результате Левин в течение нескольких месяцев осуществил не менее сорока переводов на общую сумму свыше 10 млн. дол., из которых несколько сотен тысяч преступникам удалось похитить.*

*Несанкционированный вход в систему Ситибанка и ввод команд осуществлялся из офиса санкт-петербургской фирмы. Несмотря на большой период «работы» Левина, служба безопасности банка не смогла его вычислить сразу, хотя, подозревая о наличии проблемы, неоднократно вносила изменения в систему защиты, которую группа Левина* ***все*** *равно «взламывала».*

*География совершенного преступления охватывала страны, откуда изымались крупные суммы денег со счетов клиентов (Аргентина, Гонконг, Индонезия, Канада, Колумбия, Мексика, Новая Зеландия, Уругвай) и страны, куда деньги переводились и где похищались (Россия, Нидерланды, Швейцария, Израиль).*

Приведенные примеры касаются использования компьютерной техники для хищений и мошеннических операций. Однако этим криминальное применение компьютеров не ограничивается.

В последние годы компьютеры применялись также для изготовления поддельных денежных знаков, различных банковских платежных документов - кредитных и дебитных карт, различного рода карт-систем.

*Например, в июне 1995 г. в Таганроге (Ростовская обл.) была задержана преступная группа, изготовлявшая и распространявшая фальшивые купюры достоинством в 50 тыс. руб. Для их изготовления использовалась компьютерная техника с программным обеспечением и принтеры.*

*В 1995-1996 гг. в Москве и Санкт-Петербурге были задержаны несколько групп лиц, которые для совершения различных мошеннических операций использовали поддельные* кредитные карты, изготовленные с помощью специального программного обеспечения.

Как указывают компетентные эксперты, наряду со «специалистами» в области компьютерной техники и программирования, в данной сфере незаконного бизнеса появляется все больше любителей. Последние умело производят декодирование паролевой системы защиты карты с последующим перепрограммированием имеющейся микросхемы («чипа») или установлением новой с записью необходимой информации для совершения мошенничества. После подобной модификации переделанные или вновь изготовленные поддельные пластиковые карты или другие их типы и виды реализуются среди недобросовестных клиентов.

Данный вид незаконного бизнеса уже получил широкое распространение, и теперь активно внедряется в России.

Таким образом, очевидно, что помимо традиционных мер безопасности в технической сфере (организационные, материальные, программные), необходимо вносить в повестку дня проблему соответствующей подготовки сотрудников служб безопасности. Речь идет прежде всего о подготовке специалистов в области компьютерной безопасности, основной функцией которых должно стать предупреждение, выявление и пресечение деятельности по нанесению информационного и финансового ущерба.

Привлекает внимание тот факт, что компьютерные преступления не исключены и в сфере деятельности самой полиции. Приведем примеры.

*• Служащие Нью-Йоркской автоинспекции добавили больше тысячи имен в машинные списки на получение водительских прав. Эти имена принадлежали, в основном, эмигрантам, не владеющим английским языком. Водительские лицензии этим лицам выписываются на основе компьютерных списков. Работая в частных автошколах, служащие инспекции брали 200-400 дол. за каждое незаконно выданное удостоверение. В результате они получили 3 млн. дол. (См.:Computer fraund and Ssecurity Dulletin -1989. -N 5. -Р.4-6; Times, Мау 30. 1989. -Р.3.)*

*• Сотрудник налогового управления продал копию документации, основанной на секретной компьютерной логике. В этих документах описаны машинные методы, используемые в налоговом управлении для контроля деклараций о доходах налогоплательщиков. Знание этой информации позволяет налогоплательщикам избежать* *правильного обложения налогами.*

*• Офицера полиции штат. Массачусетс обвинили в продаже полицейских записей частному детективу. В г. Чикаго полицейский офицер предстал перед федеральным судом по обвинению в незаконном программировании компьютера, принадлежащего национальному центру уголовной информации ФБР, для получения информации в личных целях. '(См.:inforsystem, 1978, 26. N 6. Р.18.; Chriscian Seiene, 1979, 26. 03. Р.8.; Congressional Record - Senate, 1977,. Sept. 27 Р.1754.)*

Эти примеры свидетельствуют о том, что вероятность компьютерных преступлении в самой политической среде требует подготовки профилактических мер по их предотвращению. По приблизительным данным ФБР, в США потери от преступлений, совершаемых с помощью вычислительной техники, составляют млрд. дол. ежегодно при этом средняя сумма одной кражи составляет 430 тыс. дол. Шансы найти преступника чрезвычайно малы: согласно оценкам, один случай из 25 тыс.

**Правовая защита программного обеспечения**

*Программное обеспечение (software) состоит из трех компонент:*

*замысла (основания, подосновы);*

*собственно программ;*

*сопровождающей документации.*

*Замысел (подоснова) - это идеи, концепции, алгоритмы, соображения по реализации и т.п.*

*Программа может выступать в одной из трех форм: исходный, объектный или исполняемый коды.*

*К документации относятся: руководство по использованию, блок диаграммы, книги по обучению; иногда сложное программное изделие, такое, как операционная система, сопровождается специальным аудиовизуальным курсом обучения.*

Мы не рассматриваем здесь аппаратных и программных средств защиты программных изделий (аппаратные ключи, вставляемые в параллельный порт, ключевые дискеты, прожигание отверстий лазером, привязка к аппаратному идентификатору машины и пр.). В поле зрения только правовая защита.

Имеется два основных подхода к правовой защите программного обеспечения:

**защита на основе уже существующей правовой системы;**

**использование нового законодательства, независимо от существующего**.

Правовая защита программного обеспечения по своей проблематике во многом совпадает с более широкой задачей - правовой защитой интеллектуальной собственности.

В настоящее время имеется пять основных правовых механизмов защиты программного обеспечения:

**авторское право;**

**патентное право;**

**право промышленных тайн;**

**право, относящееся к недобросовестным методам конкуренции;**

**контрактное право.**

Два основных игрока на этой арене - авторское и патентное право. Три последних механизма защиты часто объединяют в одну группу.

Сменяемость компьютерных систем составляет характерную для рынка аппаратных средств величину: 40 мес. При сдаче компьютерной системы в аренду помесячная оплата составляет 1/40 от стоимости системы; эта цифра приводится, например в таких справочниках, как GML Corporation booklet. Через 40 мес. система устаревает и должна быть заменена новой моделью. Никто, по-видимому, не проводил анализа, который позволил бы выяснить, какова «постоянная времени» для сменяемости программных изделий. За 14 лет существования (1976-1990гг.) операционной системы VAX/VMS (корпорация ДЭК) она прошла путь от первой версии до версии 5.3 через многие промежуточные версии (4.5, 4.7 и т.д.). Во всяком случае она претерпела за это время четыре крупных перехода и около 20 мелких. По-видимому, правильной «постоянной времени» для сменяемости программных издалий является 24-30 мес. Эта оценка важна потому, что срок патентования составляет несколько лет (до 5 и более). Так что даже если бы не было никаких правовых трудностей с патентованием программного обеспечения, механизм патентной защиты плохо подходил бы к программному обеспечению.

Прежде всего, рассмотрим вопрос о защите программного обеспечения авторским правом.

**Авторское право** восходит к британскому законодательству начала XVIII века, когда Парламентом был принят так называемый «Статус Анны» (1710), в котором говорилось о «поощрении ученых мужей составлять и писать полезные книги». Летом 1787 г. на Конституциональном конвенте в Филадельфии была принята Конституция Соединенных Штатов (ратифицирована а июне 1788 г.). В ней было заложено будущее патентное и авторское право. Согласно Конституции, Конгресс имеет право «поощрять развитие наук и полезных искусств, обеспечивая на определенный срок авторам и изобретателям исключительное право на их произведения и открытия» (Конституция США).

Основные положения авторского права устанавливают баланс между общественным интересом и зашитой прав автора. С одной стороны, общество нуждается в работах «ученых мужей» во имя процветания, с другой - права автора должны быть защищены для того, чтобы поощрить его к дальнейшей работе. Такую балансировку может обеспечить только очень хорошо продуманное, взвешенное законодательство.

Задолго до принятия Акта об авторском праве 1976 г. были установлены следующие два требования к «произведению», необходимые для защиты его авторским правом: оригинальность и реализация в материальной форме. Степень «художественности» произведения не играет роли, важно, чтобы оно было собственным произведением автора.

Здесь, однако, возникает вопрос о единственности представления идеи, точнее о запасе возможных представлений идеи. Если идея представляется единственным выражением, то защита выражения равносильна запрету использования идеи. Простая идея имеет небольшой запас выражений, ее представляющих, и они, как

таковые, не могут защищаться авторским правом. Поэтому должна быть установлена некая граница, начиная с которой «произведение» защищаемо авторским правом. Это особенно актуально применительно к программам. Ассемблерная программа перемножения двух чисел с фиксированной точкой вряд ли может быть защищена авторским правом. Однако правовое определение границы, начиная с которой программы защищаемы авторским правом, представляет собой непреодолимую трудность.

*Провести четкую демаркационную линию между выражением и идеей нельзя. Известно следующее рассуждение судьи Л.Хэнда, так называемый «Абстракционный тест»:*

*«Любое произведение, особенно пьесу, можно хорошо уложить в последовательность схем, общность которых будет возрастать по мере того, как все больше эпизодов опускается. Последняя из них может, пожалуй, оказаться не более чем общим утверждением, о чем эта пьеса, а иногда может попросту состоять из ее названия; однако в этой серии абстракций имеется пункт, начиная с которого они уже не защищаемы, ибо в противном случае драматург мог бы воспрепятствовать использованию его «идей», на которые, в отличие от их выражения, его собственность никогда не распространялась». Ни законодательно, ни прецедентно указать эту* демаркационную линию не удалось.

Авторское право обеспечивает автоматическую защиту. Защита авторским правом возникает вместе с созданием произведения независимо от того, предоставил ли автор копию произведения в Бюро по авторскому праву для регистрации. Однако без регистрации держатель авторского права не может реализовать свои права. Например, он не может возбудить иск о нарушении его права и не может получить возмещение.

Закон подробно оговаривает, в каком виде должны представляться « копии» программ или баз данных для их регистрации. В случае опубликованной или неопубликованной программы требуется представить один экземпляр «идентифицирующей порции» программы, воспроизведенной в форме, визуально воспринимаемой без помощи машины или какого-либо устройства, на бумаге или на микроформе. Оговаривается, какова эта «порция». После установления, что представленное произведение защищаемо авторским правом, и просмотра сопровождающих (несложных!) документов Регистр Авторского Права (Register of Copyright*)* регистрирует требование и выдает автору свидетельство о регистрации.

Авторское право защищает произведение от копирования, но не запрещает независимого создания эквивалентов. Таким образом, риск монополизации знания при использовании авторского права существенно меньше, чем при использовании патентного права и, как следствие, стандарты защиты авторским правом не столь строги, как стандарты защиты патентным правом.

Авторское право США предоставляет автору следующие пять прав:

воспроизведение;

подготовка производных произведений;

распространение копий или звукозаписей;

публичное исполнение;

выставка (display).

Авторское право, как уже говорилось, защищает не идею, а ее выражение, конкретную форму представления. Поэтому в основу защиты программ авторским правом кладутся следующие соображения.

**Последовательность команд.** Программа - это последовательность команд, поэтому она может рассматриваться как «выражение» идеи автора, т.е. как его произведение.

**Копирование.** Это понятие, используемое в авторском праве, может быть распространено на перенос программ с одного носителя на другой, в том числе - на носитель другого типа (с ленты на диск, в ПЗУ (КОМ) и т.п.). Математически это понятие формализуется следующим образом. Пусть имеются виды носителей А и В и процессы «перехода» с одного носителя на другой:

А--->В и В---->А.

Если объект а при переходе с А на В преобразуется в объект Ь, который при переходе с В на А переходит в прежний объект а, то такой «переход» считается копированием.

Судить об «идентичности» программ на носителях А и В можно по многим признакам, например по их одинаковым функциональным свойствам; однако совпадение функциональных свойств не защищается авторским правом; одинаковость функциональных свойств, как таковая, еще не свидетельствует о воспроизведении «формы», т.е. о копировании.

***Творческая активность.*** Подобно другим формам фиксации, защищаемым авторским правом, компьютерная программа есть результат творчества. Хотя эта форма выражения или фиксации все еще не является общеизвестной, уровень творческой активности, искусности и изобретательности, необходимый для создания программы, позволяет утверждать, что программы подлежат защите авторским правом не менее, чем любые другие произведения, им защищаемые. Тот факт, что компьютерные программы имеют утилитарное назначение, этого не меняет.

***Стиль.*** Творчество, искусность и изобретательность автора проявляются в том, как создается программа. Необходимо поставить задачи, подлежащие решению. Затем проанализировать, как достичь решения, выбрать цепочки шагов, ведущих к решению; все это должно быть зафиксировано написанием текста программы. Способ, которым все это проделывается, придает программе ее характерные особенности и даже стиль.

***Алгоритм.*** Собственно шаги представляют собой элементы, с помощью которых строится программа, т.е. алгоритмы, не могут защищаться от неавторизованного воспроизведения. Это - аналоги слов в литературе или - мазков кистью в живописи.

***Отбор и сопряжение элементов.*** Как и в случае других произведений, в частности литературных, защита компьютерных программ рассматривается с точки зрения отбора и сопряжения автором этих базовых элементов, в чем и проявляется его творчество и искусность, и что отличает его произведение от произведений других авторов. Случай, когда два автора независимо друг от друга написали бы для одной и той же цели две идентичные программы, практически исключен. Однако субрутины, которыми пользуются программисты, в основном общеизвестны ( их берут в одной и той же операционной среде из единой библиотеки).

***Оригинальность программ -*** первое основное требование авторского права - часто основана на отборе и сопряжении этих общеизвестных элементов.

***Удачность.*** Успех в решении задачи в значительной степени определяется тем отбором элементов, который автор произвел на каждом шаге построения. Поэтому программа может работать быстрее; она проще и надежнее в обращении, легче воспринимается и в целом более производительна, чем ее предшественница или конкуренты.

Эти и другие соображения были положены в основу защиты программ авторским правом. Здесь необходимо было обсудить ряд специфических положений:

кто является автором произведения;

что именно защищается (замысел, программа, документация);

какие именно права гарантируются авторским правом;

каким должен быть срок действия авторского права применительно к программе;

в чем должна состоять процедура «регистрации» произведения;

какие процедуры следует применять в случае нарушения авторского права и др.

Мы не останавливаемся на этих вопросах, а также на вопросах сравнения законодательства по защите программ авторским правом в разных странах и на сравнении этого законодательства с основными международными конвенциями (UСС – Universal Copyright Converntien - Всеобщая конвенция по авторскому праву; Буэнос-Айресская и Бернская конвенции).

Детальное рассмотрение их проблем требует отдельной работы. Имеются и более специфические вопросы, хуже осмысленные на сегодня в правовом отношении. К ним относятся: вопрос о форматах данных, используемых при вводе/выводе информации и вопрос об интерфейсе пользователь/программа; а также о структуре и организации программы.

Первая проблема состоит в следующем. Является ли нарушением авторского права использование форматов данных, особенно графических форматов - «экранов», примененных в программах другого автора. Графические форматы сегодня широко распространены, например в связи с вводом оперативной экономической информации (системы key-to-disk в банковском деле и т.п.).

Вопрос об интерфейсе пользователь/программа получил название «look and feel» - «облик и ощущение». В какой мере пользовательский интерфейс новой программы выглядит как интерфейс более ранней программы, в какой степени он создает такое же ощущение? Эти вопросы важны, поскольку «удачность» программы связана в первую очередь с «приятным ощущением пользователя».

Вопрос о структуре и организации программ связан с тем, что сегодня большая работа выполняется по переносу программ и программных систем с одного типа машин на другой. Например, с машин 1ВМ на ОЕС.

Может ли считаться нарушением авторского права ситуация, когда разработчик получил доступ к исходному коду программной системы для машины А, например, по контракту с автором этого кода. Разработчик использовал исходный код для машины А, чтобы написать аналогичную систему для машины В. Например, разработчик адаптировал фортранный код для А к Фортрану на машинах В. Может ли этот разработчик считаться автором программной системы на машине В?

Эти вопросы, а также ряд других не получили законодательного разрешения.

**Промышленный шпионаж и законодательство**

Многие специалисты отмечают слабость юриспруденции развитых стран в отношении защиты предприятий и фирм от промышленного шпионажа. Американский специалист по этому поводу высказался так: «Нет еще законов, обеспечивающих надлежащую защиту от похитителей секретных знаний и данных. Те, кто крадет эту ценную собственность, находятся в выгодном положении по сравнению с теми, кто крадет материальное имущество, так как первые не подпадают под действие «Национального закона о хищении имущества». «Кроме того, - как утверждает Бержье,-промышленный шпион, как правило, рискует получить шесть месяцев тюрьмы за то, за что военный шпион был бы расстрелян, а вознаграждение промышленного шпиона в случае удачи было бы в несколько раз больше вознаграждения военного шпиона».

*К тому же западные законодательства довольно громоздки и похищение промышленного секрета трудно доказуемо. «Неадекватные законы - по словам американского юриста - ограничивают суды и дают им мало шансов в преследовании преступников, занимающихся промышленным шпионажем.» Так, в США для того, чтобы потребовать законодательной защиты в случае разглашения торгового секрета требуется доказать:*

*1. Что предмет,.рассматриваемый как торговый секрет, является таковым фактически;*

*2. Право собственности на него;*

*3. Что действия лица, раскрывающего торговый секрет, относятся к одной из следующих категории;*

*а) торговый секрет получен нечестным путем;*

*6) разглашение или использование торгового секрета представляет собой нарушение доверительных отношений между лицами;*

в) лицо узнало секрет (в том числе и от третьего лица) и знало о том, что это секрет.

**Лучше защищена запатентованная информация**, хотя и здесь много слабых мест. Так, закон США предусматривает запрет на публикацию сведений в печати в течение года до подачи заявки на патентование. В других странах, как правило (кроме Франции и Голландии), простого запрета на разглашение информации хватает для того, чтобы доказать, что она секретная. Однако и здесь законодательство несовершенно.

Но ни в какое сравнение с законами развитых стран не могут идти законы (а точнее, их полное отсутствие) на территории стран СНГ. Такое положение шокирует западных бизнесменов и вызывает у них боязнь инвестирования новых технологий в СП, действующих на территории СНГ.

**Коммерческой тайной не являются следующие документы и сведения:**

• учредительные документы, документы, позволяющие заниматься предпринимательской или хозяйственной деятельностью или ее отдельными видами;

• информация по всем установленным формам государственной отчетности;

• данные, необходимые для проверки начисления и уплаты налогов и других обязательных платежей, сведения о численности и составе работающих, их заработной плате в целом, по профессиям и должностям, а также о наличии свободных мест;

• документы об уплате налогов и обязательных платежей;

• информация о загрязнении окружающей природной среды, не обеспечении безопасности условий труда, реализации продукции, которая приносит вред здоровью, а также о других нарушениях законодательства и размерах нанесенных при этом убытков;

• документы о платежеспособности;

• сведения об участии должностных лиц предприятия в кооперативах, малых предприятиях, союзах, объединенияхи других организациях, которые занимаются предпринимательской деятельностью;

• сведения, которые в соответствии с действующим законодательством подлежат оглашению.

Указанные сведения предприятия обязаны предоставлять контролирующим органам государственной власти, и правоохранительным органам, а также другим юридическим лицам по их требованию, согласно действующему законодательству.

Говорят, что успешно проведенные акции промышленного шпионажа ведут к получению незаконных преимуществ над конкурентами. Однако следует ли считать промышленный шпионаж таким ужасным преступлением в мире рыночных отношений, где правит конкуренция и где каждый с неизбежностью становится победителем или побежденным.

*«Проколы « безопасности фирм на Западе нередки, однако руководство обычно стремится быстро замять дело, чтобы избежать огласки и не ставить под удар свою репутацию. Обычная позиция руководителя фирмы: «Со мной это никогда не случится», - очень часто подводит его самого, его работников, клиентов и акционеров. На фирмах редко* *проявляют серьезное отношение к угрозам со стороны спецслужб других государств, причем спецслужб даже «дружественных» стран.*

Руководство фирм игнорирует возможность шпионажа со стороны конкурентов, не интересуется методами негласного сбора информации, а безопасность до сих пор считается объектом накладных расходов и не рассматривается в качестве объекта инвестиций в защиту ценностей и ресурсов. Когда проблема все же возникает, от нее стараются отделаться одним ударом.

Политическая философия 80-х годов внесла большой вклад в разрушение лояльности, гордости и самодисциплины сотрудников фирм. Некогда сильный «корпоративный дух» сегодня сгорает в котле индивидуализма рыночных отношений. Работник, затаивший обиду на своего начальника, представляет собой наибольшую угрозу информационной безопасности, однако это в наименьшей степени осознается руководством компаний.

В наши дни **размеры «информационной биржи»**, где люди занимаются куплей-продажей информации, **значительно расширились**, причем продажа нелегально добытых сведений не является чем-то совсем необычным. О деятельности брокеров на такой бирже по понятным причинам мало что известно, но то, что описано ниже, весьма характерно для сегодняшней действительности.

Оценивая правовой аспект промышленного шпионажа, журнал International Security reverw отмечает, что **во всех странах Европейского союза нет законов, напрямую трактующих промышленный шпионаж в качестве противоправного деяния**. Так, в Великобритании парламенту еще только предстоит признать промышленный шпионаж преступлением, хотя в этой стране существует с десяток законодательных актов, регулирующих те или иные стороны информационной безопасности. Однако попытки принять закон «О промышленной информации» в 1968 г. и «О злоупотреблении доверием» в 1981 г., в которых были даны определения понятий «промышленный шпионаж» и «угроза выведывания путем инсценированного интервью», успехом не увенчались. В то же время в ряде штатов США промышленный шпионаж законодательно считается преступлением.

*В январе 1993 г. за мошенничество в отношении фирмы British Petroleum (ВР) были задержаны и оштрафованы два преступника. В деле были замешаны одна немецкая и одна японская фирма, которые работали вместе с целью получения прибыльного контракта в Северном море. Главными фигурантами в этом деле были Жрайбар и Сорелли. Жрайбар занимался упомянутыми фирмами, а Сорелли подготавливал контракты от лица фирмы ВР.*

*Руководство ВР было уверено в том, что ему удалось создать надежную систему обеспечения информационной безопасности при заключении контрактов. Согласно установленному порядку, предложения участников торгов должны были подаваться в запечатанных конвертах. Для работников был жестко разграничен доступ к информации, а соответствии со служебной необходимостью. Однако если одному из участников торгов удавалось разузнать больше, чем другим, то вся система торгов сразу же становилась скомпрометированной.*

*Заведенный на фирме порядок проведения торгов редко изменялся, многие процедуры не были защищены от действий нелояльных по отношению к фирме и недобросовестных сотрудников. Работники имели доступ к картотекам, оставленным на рабочих столах или в незапертых шкафах. Добытую информацию они передавали Сорелли, а тот - Жрайбару. Последний продавал ее участникам торгов.*

*Указанные лица попались после проведения специальной операции фирмой 5епоих Рша 0№се против «информационных брокеров» в нефтяной промышленности. Фирме ВР был нанесен ущерб в несколько миллионов фунтов стерлингов. (International Security* Revierw- *1994/1995 Winter .-Р. 20-22.)*

Основной движущей силой промышленного шпионажа в рыночном обществе всегда была конкуренция. Все конкурирующие между собой фирмы располагают сведениями, которые обычно бывает легко узнать из отраслевых периодических изданий, газет, в ходе обычных деловых контактов. Однако некоторые данные фирмы всегда стремятся сохранить в тайне. Это сведения, за которыми охотятся конкуренты: **технологические процессы, стратегии маркетинга, результаты научно-исследовательских и опытно-конструкторских** **работ** - обычные цели промышленного шпионажа. Именно эти сведения должны быть четко определены и надежно защищены от хищений и несанкционированного доступа. Чем больше такой информации, тем острее стоит проблема обеспечения безопасности.