О.В.МОСИН

КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ И ИНТЕРНЕТ.

ВВЕДЕНИЕ

Поступательно развивающийся научно-технический прогресс ставит важность компьютерных информационных технологий на первый план. Порой законодатель не успевает за все увеличивающимися темпами технократического и информационного развития общества. Изменения, происходящие в экономической жизни России – формирование и развитие частно-собственнических отношений, создание финансово-кредитной системы, предприятий различных форм собственности и т.п. - оказывают существенное влияние на вопросы правовой защиты информации, включая информацию компьютерную. Долгое время в нашей стране существовала только одна форма собственности - государственная, поэтому информация и секреты были исключительно прерогативой государства, охраняемыми мощными спецслужбами. Сейчас ситуация существенно изменилась, поскольку появилось множество различных объектов, источников и средств информации. Именно поэтому обеспечение правовой защиты компьютерной информации выступает на первый план деятельности любой фирмы, учреждения, гослужбы и т.п. Следует подчеркнуть, что отдельные сферы государственной деятельности (банковские и финансовые институты, промышленные национальные информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер правовой защиты и безопасности данных и предъявляют повышенные требования к надежности функционирования компьютерных информационных систем в соответствии с характером и важностью решаемых ими задач. Каждое противоправное посягательство в сфере компьютерной информации это не только сбой работы компьютерной сети и “моральный” ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, “безбумажного” документооборота и других, серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что может привести к значительному материальному ущербу и колоссальным убыткам. Не случайно поэтому защита данных в компьютерных сетях, борьба с компьютерной преступностью становится одной из актуальных проблем российского уголовного законодательства.

Термин **“компьютерная преступность”** возник в США в начале 70-х годов. В настоящее время под компьютерными преступлениями подразумеваются: **неправомерный доступ к компьютерной информации (статья 272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (статья 273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (статья 274 УК РФ); хищение, подделка, уничтожение компьютерной информации и др.** Характерной чертой преступлений в сфере компьютерной

информации является то, что компьютер может выступать и как предмет преступных посягательств, и как инструмент преступления. Если разделять два последних понятия, то термин компьютерное преступление как юридическая категория имеет двойной смысл. Действительно, если компьютер - только объект посягательства, то квалификация преступления может квалифицироваться существующими нормами уголовного права. Если же - только инструмент, то достаточен только такой признак, как “применение технических средств”. Впрочем, возможно объединение указанных понятий, когда компьютер одновременно и инструмент и предмет преступления. В частности, к этой ситуации относится факт хищения машинной информации. Если хищение информации связано с потерей материальных и финансовых ценностей, то данное деяние квалифицируется как уголовное преступление. Также если с данным деянием связываются нарушения интересов национальной безопасности, авторства, то уголовная ответственность предусмотрена уголовным кодексом РФ.

Уровень разработанности правовых способов регулирования компьютерной преступности коррелирует с научно-техническим прогрессом в обществе. При этом среди наиболее эффективным способов, направленных на предупреждение преступлений в сфере компьютерной информации выделяют **технические, организационные и правовые.**

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, принятие специальных конструкционных мер защиты от хищений, саботажа, диверсий, чрезвычайных ситуаций, терроризма, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и т.п..

К организационным мерам относится охрана вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение административной, дисциплинарной и уголовной ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы государственного контроля за разработчиками компьютерных программ и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран и др.

На сегодняшний день сформулировано три базовых правовых принципа информационной безопасности, которая должна обеспечивать:

целостность данных - защиту от сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных;

конфиденциальность (законность) информации;

доступность информации для всех авторизованных зарегистрированных пользователей;

защита компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка);

Таким образом, проблема компьютерной преступности составляет важную часть российского уголовного права. Уголовно-правовая ответственность в сфере защиты

компьютерной информации в российском уголовном законодательстве введена в новом Уголовном Кодексе 1996 г. впервые. Ранее, 23 сентября 1992 года, был принят Закон **"О правовой охране программного обеспечения для ЭВМ и баз данных"**[1] и 20 февраля 1995 года Федеральный Закон **"Об информации, информатизации и защите информации"**[2]. В этих нормативно-правовых актах был предусмотрен целый комплекс правовых мер по защите ЭВМ, баз данных, сетей в целом комплексной информации. В частности, в статье 20 ФЗ **"Об информации, информатизации и защите информации"** содержалось положение о том, что ***выпуск под своим именем чужой программы для ЭВМ или баз данных, либо незаконное воспроизведение, распространение таких произведений влечет за собой уголовную ответственность.*** Однако соответствующие уголовные нормы тогда еще не были приняты, за исключением статьи 141 старого Уголовного кодекса РСФСР. В настоящее время в различных отраслях российского законодательства идет процесс, связанный с принятием ряда нормативно-правовых актов, устанавливающих условия и принципы защиты компьютерной информации в соответствующих областях. Действует с 1995 года Федеральный закон **"Об информации, информатизации и защите информации"**[3]**,** устанавливающий основные принципы защиты информации; в 1994 году принят гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией.; сравнительно недавно вступил в силу новый Уголовный Кодекс РФ, где есть отдельная глава (гл. 28 "Преступления в сфере компьютерной информации") и статьи 272-274, предусматривающие основания уголовной ответственности за преступные деяния в названной сфере. Следует подчеркнуть, что разработка и совершенствование эффективной правовой основы, которая обеспечила бы нормальное функционирование механизма защиты компьютерной информации, представляет собой задачу на будущее. Но уже сегодня можно говорить о необходимости разработки нескольких правовых проблем в качестве составных частей правового механизма защиты компьютерной информации:

1. Установление контроля над несанкционированным, противоправным доступом к компьютерным информационным данным системы[4].
2. Ответственность за выполнение надлежащих технологических операций, связанных с защитой компьютерной информации.

ГЛАВА 1.
ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

ИСТОРИЯ РАЗВИТИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ.

1 См. Ведомости РФ, 1992 год, № 42, ст.2325
2 См. Сборник законодательства РФ, 1995, №8, ст.609
3 Российская газета. 1995г. 22 февраля
4 См. Венгеров А.Б. Право и информация в условиях автоматизации управления: теоретические вопросы. 1996. Стр. 12-14.

Человечеству потребовалось немало времени, чтобы от первых, примитивных счетных устройств XVII века перейти к использованию сверхбыстродействующих, с огромным объемом памяти (по нынешним меркам) электронно-вычислительных машин (ЭВМ), способных собирать, хранить, перерабатывать, передавать и выдавать любую информацию. Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между лини- и большими ЭВМ, дали возможность подключаться к мощным ин- формационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными. Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополни-тельным мерам безопасности, они стали активно использовать правовые, в том числе уголовно-правовые средства защиты. Так, Уголовный кодекс Франции (1992 г.) пополнил систему преступлений против собственности специальной главой **"О посягательствах на системы автоматизированной обработки данных",** где предусмотрел ответственность за незаконный доступ ко всей или части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы такой системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных. Не остались в стороне от этой проблемы и международные организации, в частности Совет Европы, который счел необходимым изучить и разработать проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации.

В 1992 году был принят Закон России **о правовой охране программ для электронно-вычислительных машин и баз данных**, в 1994 году — **Гражданский кодекс**, который содержит ряд норм, связанных с компьютерной информацией, в 1995 году — **Федеральный закон об информации, информатизации и защите информации**. Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в **УК РФ 1996 года** группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления.

Первые попытки осмысления компьютерных преступлений и конструирования в отечественной научной литературе были, однако, направлены на выработку необходимых рекомендаций по совершенствованию ранее действующего уголовного законодательства. Уяснению принципов, по которым формировалась закрепленная ныне в законе система компьютерных посягательств, способствует исследование, проведенное Ю.М. *Батуриным* и *А.М. Жодзишским.* Выделяя среди компьютерных преступлений два основных вида — связанные с вмешательством в работу компьютера и предполагающие его использование в качестве необходимого технического средства, авторы к первому отнесли: ***1) несанкционированный доступ к информации, хранящейся в компьютере; 2) ввод в программное обеспечение "логической бомбы", срабатывающей при определенных условиях и частично или полностью выводящей из строя компьютерную систему; 3) разработку и распространение компьютерных вирусов; 4) небрежность в разработке, изготовлении и эксплуатации программно-вычислительного комплекса, могущие вызывать тяжкие последствия; 5) подделку компьютерной информации; 6) ее хищение.*** Так как, по мнению этих авторов, статьями **УК РСФСР** 1960 года охватывалась только часть этих деяний (умышленное и неосторожное уничтожение или модификация компьютерной информации, небрежность в обращении с компьютерной системой), то предлагалось установить специальные основания уголовной ответственности за незаконное проникновение в вычислительные системы; похищение компьютерной информации; заражение компьютерным вирусом. Примечательно, что, увязывая

направленность значительной части компьютерных преступлений с общественной безопасностью, Ю.М. Батурин и А.М. Жодзишский считали целесообразным выделить в некоторых "обычных" преступлениях (хищении и т. д.) новый квалифицирующий признак: "совершение деяния с использованием средств компьютерной техники" (второй вид компьютерных вмешательств).

Разработчики проекта УК, ориентируясь на сходные представления об объекте уголовно-правовой охраны, предлагали объединить компьютерные посягательства в одну из глав раздела ***"Преступления против общественной безопасности",*** где нашли место почти все деяния, относимые указанными авторами вмешательству в работу компьютера.

УК РФ не воспринял формулировки, предложенные разработчиками проекта, хотя суть задуманного в принципе была сохранена; однако некоторые законодательные недоработки могут вызвать трудности в правоприменительной практике. В первую очередь это касается ст. 272 УК, предусматривающей ответственность за неправомерный доступ к компьютерной ин- формации***, "... если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети"***. Термин "повлекло" дает основание полагать, что объективная сторона данного состава преступления складывается из деяния (неправомерного доступа), последствий (уничтожение информации и т. д.) и причинной связи между ними. Этот состав преступления образовался путем объединения трех названных в проекте самостоятельных составов: ***а) самовольное проникновение в автоматизированную компьютерную систему, если это повлекло ознакомление ненадлежащих пользователей с конфиденциальной информацией", б) "неправомерное копирование программ для ЭВМ, файлов или баз данных, занесенных в память ЭВМ, если это повлекло причинение существенного вреда", и в) "самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ***". Однако нельзя не признать, что уничтожение, блокирование, модификация и копирование информации не исключают совершения самостоятельных действий. Представляется, было бы правильнее рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ **сопряжен** с уничтожением, блокированием и т. д. (т. е. такому доступу следовало бы придать значение не только причины, но и необходимого условия).

Есть и другие соображения, которые позволяют констатировать, что в статьях, посвященных преступлениям в сфере компьютерной информации, решение вопроса о последствиях содеянного оказывается наиболее слабо проработанным. Сам факт уничтожения, блокирования, модификации, копирования охраняемой законом информации причиняет ущерб владельцу информации, которую законодатель не без оснований ставит под защиту. Но серьезные препятствия в пользовании владельцем своей информацией могут возникать и в результате нарушения работы ЭВМ, системы ЭВМ, их сети, а стало быть, и такие последствия незаконных деяний должны влечь уголовную ответственность, причем в одних случаях как за посягательство на собственность, в других — за совершение компьютерных преступлений (вирусные программы способны выводить из строя, скажем, электронную начинку ЭВМ), а в третьих — по совокупности преступлений. Вместе с тем применительно к наказуемости нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети упоминается о последствиях в виде уничтожения, блокирования или модификации информации, но ничего не говорится о нарушении работы ЭВМ, системы ЭВМ, их сети. Не совсем понятно, почему при нарушении данных правил, если оно повлекло уничтожение информации, виновный может быть привлечен к уголовной ответственности, а при последствиях в виде нарушения работы ЭВМ — не может.

Единый подход к решению данного вопроса диктуется не столько формальными

соображениями, сколько тем, что при совершении любого компьютерного преступления возможны последствия второго уровня. Из периодической и научной печати многим стали известны случаи использования ЭВМ для взлома электронной банковской системы безопасности с целью похищения огромных денежных сумм или умышленной либо неосторожной дезорганизации работы систем национальной безопасности, крупнейших предприятий, диспетчерских служб и т. д. В конечном счете не так уж важно, почему именно (в результате "взлома", "шалости", появления компьютерного вируса, небрежности программиста) произошел сбой в работе компьютерной сети какого-либо технологического процесса: в любом случае последствия могут быть катастрофическими. Это, собственно, и есть одна из причин, по которой компьютерные преступления следует считать посягательствами не столько на интеллектуальную собственность, сколько на безопасность общества. Вряд ли последовательным нужно признать такой подход, при котором неосторожное причинение тяжких последствий в результате, например, нарушения правил эксплуатации ЭВМ должно признаваться квалифицирующим обстоятельством, в то время как наступление такого рода последствий, вызванных неправомерным доступом к охраняемой законом компьютерной информации, —, не может.

Наличие двух уровней последствий содеянного в составах компьютерных преступлений накладывает свой отпечаток на характеристику их субъективной стороны. Не касаясь ее специфики при наступлении последствий первого уровня, заметим, что психическое отношение лица в отношении последствий второго уровня законодатель допускает лишь в форме неосторожности. Умышленное их причинение должно образовывать самостоятельное преступление и квалифицироваться по совокупности.

ГЛАВА 2.
ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Уголовный Кодекс Российской Федерации установил нормы, объявляющие общественно опасными деяниями конкретные действия в сфере компьютерной информации и устанавливающие уголовную ответственность за их совершение. Такие нормы появились в российском законодательстве впервые. К уголовно-наказуемым отнесены *1)* ***неправомерный доступ к компьютерной информации (ст. 272 УК РФ), 2) создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ) и 3) нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ).***

Видовым объектом преступлений в сфере компьютерной информации являются ***информационные отношения, т. е. отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.*** Из этого определения следует, что и информационные отношения стали новым объектом преступления. Конкретно эти преступления направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации.

Выяснение данного обстоятельства важно для того, чтобы отграничить преступления, предусмотренные статьями 272 — 274 УК, от других преступлений, связанных с использованием ЭВМ, системы ЭВМ и их сети для совершения других преступлений. В тех случаях, когда компьютерная аппаратура является предметом преступлений против собственности, соответственно ее хищение, уничтожение или повреждение подлежат квалификации по ст. 158 — 168 УК. Информационная же структура (программы и информация) не может быть предметом преступления против собственности, поскольку машинная информация не отвечает ни одному из основных при- знаков предмета преступлений против собственности, в частности не обладает физическим признаком.

Предметом компьютерной информации являются информационные ресурсы, которые в ст. 2 Федерального закона от 20 февраля 1995 г. «Об информации, информатизации и защите информации» рассматриваются как *отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности в банках данных*. Эти ресурсы согласно ст. 2 Закона содержат сведения о лицах, предметах, событиях, процессах, населении независимо от формы их представления.

ГЛАВА 3.
ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В ДЕЙСТВУЮЩЕМ РОССИЙСКОМ УГОЛОВНОМ ЗАКОНОДАТЕЛЬСТВЕ

3.1. Неправомерный доступ к компьютерной информации *(Статья 272)*

Объектом преступления являются отношения в сфере охраны компьютерной информации.

Объективную сторону преступления образует неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать самовольное получение информации без разрешения ее собственника или владельца. В связи с тем, что речь идет об охраняемой законом информации, неправомерность доступа к ней потребителя характеризуется еще и нарушением установленного порядка доступа к этой информации. Если нарушен установленный порядок доступа к охраняемой законом информации, согласие ее собственника или владельца не исключает неправомерности доступа к ней. Собственником ин- формационных ресурсов, информационных систем, технологии и средств их обеспечения является субъект, в полном объеме реализующий права владения, пользования распоряжения указанными объектами. Владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения является субъект, осуществляющий владение и пользование указанными объектами и реализующий права распоряжения в пределах, установленных законом. Пользователем (потребителем) информации является субъект, обращающийся к информации.

Информация (сведения различного характера) содержится в базе данных, которая является объективной формой представления и организации совокупности данных, систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ.

Гибкие диски (дискеты), жесткие диски и компакт-диски позволяют переносить документы и программы с одного компьютера на другой, хранить информацию, не используемую постоянно на компьютере, делать архивные копии информации, содержащейся на жестком диске.

Доступ к информации на машинном носителе имеют **законные пользователи**, т. е. лица, имеющие разрешение пользоваться компьютерными системами., Такое разрешение может. быть дано, например, администратором базы данных.

Неправомерным следует признать доступ в закрытую информационную систему лица, не являющегося законным пользователем либо не имеющего разрешения для работы с данной информацией. Способы такого доступа: использование чужого имени, модификация программного **и** информационного обеспечения, изменение физических адресов технических устройств в результате системной поломки компьютера, установка аппаратуры записи, подключаемой к каналам передачи данных, и т. п.

Обязательный элемент объективной стороны данного **состава— последствия.**

Уничтожение информации заключается в удалении файла (поименованной области на диске или другом машинном носителе) без технической возможности восстановления.

Модификация — внесение любых изменений, за исключением необходимых для функционирования программы или базы. данных на конкретных технических средствах пользователя или под управлением его конкретных программ.

Блокирование информации — это создание препятствий к свободному доступу; при этом информация не подвергается уничтожению.

Копирование информации — создание копий файлов и системных областей дисков.

Нарушение работы ЭВМ (систем ЭВМ, их сети) выражается в снижении работоспособности отдельных звеньев ЭВМ, отключении элементов компьютерной сети.

Преступление **окончено** с момента осуществления неправомерного доступа к информации, повлекшего ее уничтожение, модификацию, блокирование, копирование либо нарушение работы ЭВМ (систем ЭВМ, их сети).

С субъективной стороны преступление характеризуется только **умышленной** формой, вины. При этом по отношению к действию умысел может быть только прямым, о чем свидетельствует и использование законодателем термина "неправомерный", а к факту наступления последствий — как прямым, так и косвенным.

Субъектом преступления, предусмотренного ч. 1 ст. 272 УК, могут быть лица, достигшие 16 лет, в том числе и законный пользователь, который не имеет разрешения для работы с информацией определенной категории.

Частью 2 ст. 272 УК предусмотрена уголовная ответственность за данное преступление, совершенное **группой** лиц **по** предвари тельному **сговору** или **организованной группой** либо лицом с **использованием своего служебного положения,** а равно имеющим **доступ** к ЭВМ, системе ЭВМ или их сети.

Совершение преступления **группой** лиц по предварительному сговору будет иметь место, когда неправомерный доступ осуществили два лица, заранее договорившиеся о совместном его совершении.

Признак **организованной группы** вменяется при совершении преступления двумя или более лицами, вне зависимости от формы соучастия — простое (соисполнительство) или сложное (с функциональным распределением ролей); причем действия виновных квалифицируются без ссылки на ст. 33 УК .

Лицо, **использующее свое служебное положение** или **имеющее доступ** к ЭВМ, системе ЭВМ, их сети, — это законный пользователь, обладающий правом доступа и обработки определенного рода информации в связи с выполнением своих служебных обязанностей, вытекающих из трудовых отношений (заключенного контракта).

3.2. Создание, использование и распространение вредоносных программ для ЭВМ *(Статья 273)*

Объектом преступления являются отношения в сфере обеспечения компьютерной безопасности.

Обьективная сторона преступления выражается в: создании программ для ЭВМ или внесении изменений в существующие программы, заведомо приводящих к несанкционирован- ному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; использовании таких программ; распространении таких программ или машинных носителей с такими программами.

В данной статье речь идет о разработке, распространении компьютерных вирусов путем создание программ для ЭВМ или внесения изменений в существующие программы. Опасность компьютерного вируса состоит в том, что он может привести к полной дезорганизации системы компьютерной информации и при этом, по мнению специалистов в данной области, может бездействовать достаточно длительное время, затем неожиданно «проснуться» и привести к катастрофе. Вирус может оказаться причиной катастрофы в таких областях использования компьютерной информации, как оборона, космонавтика, государственная безопасность, борьба с преступностью и т. д. К тяжким последствиям, наступившим по неосторожности, могут быть отнесены, например, гибель людей, причинение вреда их здоровью, дезорганизация производства на предприятии или отрасли промышленности, осложнение дипломатических отношений с другим государством, возникновение вооруженного конфликта.

Программа для ЭВМ — это объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью по- лучения определенного результата. Под программой подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.

Под **созданием** и **распространением вредоносных программ** для ЭВМ следует понимать воздействие вирусов, т. е. программ, преднамеренно и без санкции соответствующих лиц изменяющих хранящиеся в компьютере данные или программы.

Под **использованием программы** понимается воспроизведение, распространение (предоставление экземпляров программы неопределенному кругу лиц) и иные действия по ее введению в оборот.

Распространением программы признается предоставление доступа к воспроизведенной в любой материальной форме программе, в том числе сетевым и иным способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.

Окончено это преступление с момента совершения действий, указанных в диспозиции статьи.

С субъективной стороны преступление может быть совершенно как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям. При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели,

которую перед собой ставил виновный, а когда наступили последствия, к достижению которых он стремился, — и зависимости от наступивших последствий. Лицо сознает, что создает программу, зараженную "вирусом", либо внедряет "вирус" в чужую программу или распространяет и использует его, и желает совершить эти действия. В этом случае действия, предусмотренные ст. 273 УК, оказываются лишь способом достижения поставленной цели. Совершенное деяние подлежит квалификации по совокупности совершенных преступлений.

Субъект преступления — лицо, достигшее **16** лет. Квалифицирующим обстоятельством данного преступления является наступление **тяжких последствий** (ч. 2 ст. 273 УК). При фиксации последствий в данном составе преступления законодатель использует оценочное понятие. Следовательно, их тяжесть должна определяться с учетом конкретных обстоятельств дела: имущественный ущерб, сопряженный с восстановлением информации; упущенная выгода при срыве заключения крупного контракта или соглашения; дезорганизация работы предприятий или учреждений и т. п. Форма вины по отношению к тяжким последствиям может быть только **неосторожной.**

3.3. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети *(Статья 274)*

Объектом преступления являются отношения в сфере обеспечения безопасности.

Объективную сторону преступления образует нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом ин- формации ЭВМ, если это причинило существенный вред.

К такого вида нарушениям можно отнести несоблюдение общих средств защиты информации, а также нарушение режима эксплуатации ЭВМ. Выделяют два основных средства защиты: копирование. информации и ограничение доступа к информации. Нарушение режима эксплуатации ЭВМ образуют, например, несанкционированные изменение, уничтожение или передача информации. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит в несоблюдении правил режима их работы, предусмотренных инструкциями, исходящими из технических характеристик, правил внутреннего распорядка, а также правил обращения с компьютерной информацией, установленных собственником или владельцем информации либо законом или иным нормативным актом. Под охраняемой законом информацией следует понимать информацию, изъятую из публичного оборота на основании закона, других нормативных актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования. Представляется, что частные фирмы, включая коммерческие банки, вправе устанавливать ограничительные грифы в целях сохранения коммерческой или банковской тайны.

Под **существенным вредом** (оценочное понятие) следует пони- мать причинение как материального, так и нематериального вреда.

Обязательным признаком объективной стороны преступления является наличие прямой (непосредственнной) **причинной связи** между уничтожением, модификацией или блокированием охраняемой законом информации и наступлением последствий в виде причинения существенного вреда.

С субъективной стороны преступление может быть совершено как **умышленно** так и по **неосторожности** в виде как небрежности, так и легкомыслия. При установлении умысла на нарушение правил эксплуатации ЭВМ, системы ЭВМ и сети деяние, предусмотренное ст. 274 УК, становится лишь способом совершения преступления. Преступление в этом случае подлежит квалификации по наступившим последствиям, которые предвидел виновный, по совокупности с преступлением,

предусмотренным данной статьей **УК.**

Субъект преступления специальный — лицо, имеющее законный доступ к эксплуатации упомянутых технических средств, достигший 16 лет. Это могут быть программисты, операторы ЭВМ, техники-наладчики и другие лица, имеющие к ним доступ по работе. О тяжких последствиях, наступивших по неосторожности, сказано выше в ст. 273

Квалифицирующим признаком ч. 2 ст. 274 УК является наступление **тяжких последствий,** а **субъективная сторона** характеризуется **неосторожной** формой вины по отношению к этим последствиям.

ГЛАВА 4.
КОМПЬЮТЕРНАЯ ПРЕСТУПНОСТЬ И ЕЕ ОСНОВНЫЕ ХАРАКТЕРИСТИКИ.

Характеристика компьютерных преступлений. Попытаемся охарактеризовать преступное явление, которое как уголовная категория получила на Западе название **“компьютерная преступность”.** Впервые мир узнал о компьютерных преступлениях в начале 70-х годов, когда в США правоохранительными органами было выявлено довольно большое количество аналогичных преступлений. Как правило, эта категория уголовных преступлений носит экономический характер. Например, неправомерное обогащение путем злоупотребления с компьютерными информационными системами, экономический шпионаж, кража компьютерной информации и программного обеспечения, так называемого "компьютерного времени", а также традиционные экономические преступления, совершаемые с помощью компьютера как средства преступлений. Изначально, как показывает судебная практика, правоохранительные органы боролись с ней при помощи уголовно-правовых норм о преступлениях против собственности: краже, присвоении, мошенничестве, злоупотреблении доверием и др. Однако вскоре уголовная практика показала, что такой правовой подход не отвечает требованиям сложившейся ситуации, поскольку многие преступления в сфере компьютерной информации не охватываются традиционными составами уголовных преступлений. Во многих преступлениях отсутствовал материальный состав преступления, так как предмет отсутствует как материальная вещь, существующая в реальном физическом мире. "Обман компьютера" – понятие эфемерное, поскольку это всего лишь механизм и обмануть его в принципе невозможно. С таким же успехом можно обманывать дверной замок. Уничтожение имущества тоже не подходит под данный состав преступления, поскольку нет уничтожения как такового. Хотя подобные действия и могут принести значительный имущественный ущерб – без физического повреждения компьютера такой состав попросту не имеет смысла. Поэтому преступления в сфере компьютерной информации требуют более пристального изучения в уголовном праве. Действующий российский уголовный кодекс содержит главу 28, посвященную преступлениям в сфере компьютерной информации, включающую в себя три статьи 272-274, предусматривающие уголовную ответственность. Однако, следует отметить, что они устарели по смысловому значению, и требуют существенных дополнений.

Компьютерные преступления условно можно подразделить на две основные категории - ***преступления, связанные с вмешательством в работу компьютеров, и,***

преступления, использующие компьютеры как необходимые технические средства преступлений.

Перечислим основные виды преступлений, связанных с противоправным вмешательством в работу компьютеров.

4.1. Неправомерный доступ к компьютерной информации.

Неправомерный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры "электронные корсары", "компьютерные пираты" - так называют компьютерных правонарушителей, осуществляющих противоправный несанкционированный доступ в чужие информационные сети. Техника правонарушения проста – набирая один номер за другим, они дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственной ЭВМ и устанавливается автоматическая связь и необходимый код. Таким образом можно внедриться в чужую компьютерную систему.

Несанкционированный противоправный доступ к файлам и информации законного пользователя осуществляется также нахождением слабых мест в компьютерной защите системы. Однажды обнаружив их, преступник может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, подобно покупателю, изучающему товары на витрине.

Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей компьютерной логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению возможности совершения противоправного деяния. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что правонарушитель проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого способа преступления. Самый простейший путь его осуществления – это получить коды и другие идентифицирующие шифры законных пользователей. Это возможно:

- **приобретением** (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- **обнаружением такого документа в организациях**, где не налажен достаточный контроль за их хранением;
- **незаконным, несанкционированным подслушиванием через телефонные линии.**

Иногда случается, как например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение

определенного времени и таким образом незаконно получить некоторую ценную информацию, в частности коды.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог инструкций и приспособлений, помещаемых в транспорте под надписью “разбить стекло в случае аварии”. Такая программа - мощный и опасный инструмент в руках преступника. Несанкционированный доступ также может осуществляться в результате системной поломки компьютера. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к непринадлежащим ему частям банка данных. Говоря фигурально, все происходит так словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В результате он может проникнуть в чужие сейфы и похитить все, что в них хранится.

4. 2. Ввод в программное обеспечение вредоносных программ (“логических бомб”).

Вредоносные программы для ЭВМ по типу **“логическая бомба”** срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему. Вредоносная программа по типу **“временная бомба”** - разновидность “логической бомбы”, которая срабатывает по достижении определенного момента времени. Этот преступный способ состоит в несанкционированном введении в лицензионную программу таких вредоносных программ, позволяют осуществлять новые, не планировавшиеся авторизованным законным владельцем программы функции, но одновременно сохранять и прежнюю работоспособность. С помощью этого метода преступники, например, отчисляют на свой счет определенную сумму денег с каждой операции. Компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен, тысяч, а иногда и миллионов команд. Поэтому вредоносная программа из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Имеется еще одна разновидность вредоносных программ. Ее особенность заключается в том, что в безобидно выглядящей кусок программы вставляются команды, формирующие другие команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти вредоносную программу, необходимо искать не его самого, а команды его формирующие. Развивая эту идею, можно представить себе вредоносные команды, которые создают команды и т.д. (сколь угодно большое число раз), создающие вредоносную программу по типу **“троянского коня”.**

В настоящее время в США получила распространение форма компьютерного преступления, при котором вредоносная программа разрушает через какой-то промежуток времени все программы, хранящиеся в машинной памяти. Во многих поступивших в продажу компьютерах оказалась вредоносная программа, которая выполняется в самый неожиданный момент, разрушая всю библиотеку данных. Не следует думать, что вредоносные программы по типу “логические бомбы” - это экзотика, несвойственная нашему обществу.

4. 3. Разработка и распространение компьютерных вирусов.

Вряд ли найдется хотя бы один пользователь персонального компьютера, который ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведенного фирмой Creative Strategies Research (США), 64 % из 451 опрошенного специалиста компании испытали на себе действие вирусов. На сегодняшний день по оценкам западных специалистов дополнительно к тысячам уже известных вирусов появляется 100-150 новых видов ежемесячно.

Позволю себе небольшое отступление и скажу, что в процессе разработки настоящей курсовой работы, на компьютер "просочился" один из вирусов и парализовал работу программного обеспечения. А если представить все это в масштабах большого предприятия, отрасли? В действующем российском законодательстве РФ существуют статья 273 о создании, использовании и распространении вредоносных программ для ЭВМ, которая определяет основание уголовной ответственности для подобного рода преступлений. Опасность компьютерного вируса состоит в том, что он может привести к полной дезорганизации работы компьютера и программного обеспечения и при этом, по мнению специалистов в данной области, может бездействовать достаточно длительное время, затем неожиданно активизироваться и привести к катастрофе[5]. Вирус может оказаться причиной неустранимых нарушений в работе программного обеспечения и компьютерных сетей в таких важных национальных областях использования компьютерной информации, как оборона, космонавтика, государственная безопасность, банковская система, организованная борьба с преступностью. Именно высокой степенью общественной опасности объясняется, что УК РФ преследует достаточно строго за сам факт создания, распространения и использования вредоносных компьютерных программ для ЭВМ, не оговаривая наступления каких-либо тяжких последствий. При этом преступление считается оконченным, когда вредоносная программа создана или были внесены изменения. Под использованием (распространением) вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в компьютер, систему, сеть компьютеров, а также продажа, обмен, дарение, безвозмездная передача. Можно предположить, что под распространением следует понимать и их копирование. Российским уголовным законодательством предусмотрены квалифицирующие признаки: такое преступление может иметь тяжкие последствия – гибель людей, моральный и материальный вред, причинение тяжкого вреда здоровью, дезорганизация производства на предприятии или в отрасли промышленности, осложнение дипломатических отношений, вплоть до возникновения вооруженного конфликта. Яркий пример этому - произведение американского писателя Дэвида Бишофа под названием "Военные игры", написанного на основе реально происходивших событий. Чрезвычайно одаренный подросток взломал компьютерную сеть Пентагона и едва не развязал Третью мировую войну. Вирусы, действующие по принципу: "сотри все данные этой программы, перейди в следующую и сделай то же самое" обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как самое настоящее вирусное заболевание. Причем выявляется вирус не сразу: первое время компьютер "вынашивает ин-фекцию", поскольку для маскировки вирус нередко используется в комбинации с вредоносной программой типа **"логической бомбы"** или **"временной бомбы"**. Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Все происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека. Начиная действовать (перехватывать управление), вирус дает команду компьютеру, чтобы

5 См. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность., М., 1999 г., стр. 34-47.

тот записал зараженную версию программы. После этого он возвращает программе управление. Пользователь персонального компьютера ничего не заметит, так как его компьютер находится в состоянии "здорового носителя вируса". Обнаружить этот вирус можно, только обладая чрезвычайно развитой программистской интуицией, поскольку никакие нарушения в работе ЭВМ в данный момент не проявляют себя. А в один прекрасный день компьютер "заболевает". Все вирусы можно разделить на две разновидности, обнаружение которых различно по сложности: **"вульгарный вирус"** и **"раздробленный вирус"**. Программа "**вульгарного вируса**" написана единым блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить ее в самом начале эпидемии (размножения). Эта операция требует, однако, крайне тщательного анализа всей совокупности операционной системы ЭВМ. Программа **"раздробленного вируса"** разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции которые указывают компьютеру как собрать их воедино, чтобы воссоздать и, следовательно, размножить вирус. Таким образом, он почти все время находится в "распределенном" состоянии, лишь на короткое время своей работы собираясь в единое целое. Как правило, создатели вируса указывают ему число репродукций, после достижения которого он становится агрессивным. Подобные вирусы называют еще "невидимками".

Варианты вирусов зависят от противоправных целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея. Признаки могут быть эволютивными, и "болезнь" будет обостряться по мере своего течения. Так по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения. Каковы же способы распространения компьютерного вируса? Они основываются на способности вируса использовать любой носитель передаваемых данных в качестве "средства передвижения". То есть с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется зараженной. Таким образом, дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И наоборот, когда "здоровая" лицензионная дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных вирусных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения - это копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы. Специалисты предостерегают от копирования нелицензированных ворованных программ. Иногда, однако, и официально поставляемые программы могут быть источником заражения. Часто с началом компьютерной эпидемии связывают имя Роберта Морисса студента Корнеллского университета (США), в результате действий которого зараженными оказались важнейшие компьютерные сети восточного и западного побережий США. Вредоносная программа охватила более 6 тысяч компьютеров и 70 компьютерных систем. Пострадавшими оказались, в частности, компьютерные центры НАСА, Дивермарской лаборатории ядерных исследований, Гарвардского, Питсбургского, Мэрилендского, Висконсинского, Калифорнийского, Стэнфордского университетов. Масштаб впечатляет. Однако, на мировом рынке

все большую популярность завоевывают антивирусные программы, написанные российскими разработчиками. А изобретателем вируса является, некий студент Калифорнийского университета Фред Коуэн, который в 1994 году выступая на одной из конференций, рассказал про свои опыты с тем, что один его друг назвал "компьютерным вирусом". Когда началось практическое применение вирусов, неизвестно, ибо банки, страховые компании, предприятия, обнаружив, что их компьютеры заражены вирусом, не допускали, чтобы сведения об этом просочились наружу. Компьютерный вирус можно сравнить с вирусом СПИД ("AIDS"). Только упорядоченная жизнь с одним или несколькими партнерами способна уберечь от этого вируса. Беспорядочные связи со многими компьютерами почти наверняка приводят к заражению. Однако, пожелание ограничить использование непроверенного программного обеспечения скорее всего так и останется практически невыполнимым. Это связано с тем, что фирменные лицензионные программы на "стерильных" носителях стоят немалых денег в конвертируемой валюте. Поэтому избежать их неконтролируемого копирования в настоящее время практически невозможно. Справедливости ради следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается любым антивирусным тестом. Это служит достаточно надежной действующей гарантией, что никто не рискнет незаконно копировать и модернизировать такую дискету.

Американскими экспертами собрано досье писем от шантажистов требующих перечисления крупных сумм денег в одно из отделений американской фирмы “ПК Сиборг”; в случае отказа преступники грозятся вывести компьютеры из строя. По данным журнала “Business world”, дискеты-вирусоносители получены десятью тысячами организаций, использующих в своей работе компьютеры. Для поиска и выявления компьютерных преступлений созданы специальные отряды американских детективов.

По оценке западных специалистов в настоящее время в “мировом обращении” находится более 100 типов вредоносных программ-вирусов. Но все их можно разделить на две разновидности, обнаружение которых различно по сложности: **“вульгарный вирус”** и **“раздробленный вирус”**. Программа “вульгарного вируса” написана единым блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить ее в самом начале эпидемии (размножения). Эта операция требует, однако, крайне тщательного анализа всей совокупности операционной системы ЭВМ. Программа “раздробленного вируса” разделена на части, на первый взгляд, не имеющие между собой связи. Эти части содержат инструкции, которые указывают компьютеру, как собрать их воедино чтобы воссоздать и, следовательно, размножить вирус. Таким образом, он почти все время находится в “распределенном” состоянии, лишь на короткое время своей работы собираясь в единое целое. Как правило создатели вируса указывают ему число репродукций, после достижения которого он становится агрессивным. Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер. Варианты вирусов зависят от целей, преследуемых их создателем. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея (т. н. “итальянский попрыгунчик”). Признаки могут быть эволютивными, и “болезнь” будет обостряться по мере своего течения. Так, по непонятным причинам программы начинают переполнять магнитные диски, в результате чего существенно увеличивается объем программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения.

По-видимому, в будущем следует ожидать появление принципиально новых видов вирусов. Например, можно себе представить вредоносной программы вирусного типа в логических электронных схемах компьютера. В самом деле, пока речь идет только о заражении компьютеров. А почему бы - не микросхем? Ведь они становятся все более мощными и превращаются в некое подобие мини-ЭВМ. И их также необходимо программировать. Конечно, ничто не может непосредственно “заразить” микросхему. Но ведь можно заразить компьютер, используемый как программатор для тысячи микросхем.

Каковы способы распространения компьютерного вируса? Они основываются на способности вируса использовать любой носитель передаваемых данных в качестве “средства передвижения”. То есть с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется зараженной. Таким образом, дискета или магнитная лента, перенесенные на другие ЭВМ, способны заразить их. И наоборот, когда “здоровая” дискета вводится в зараженный компьютер, она может стать носителем вируса. Удобными для распространения обширных эпидемий оказываются телекоммуникационные сети. Достаточно одного контакта, чтобы персональный компьютер был заражен или заразил тот, с которым контактировал. Однако самый частый способ заражения - это противоправное копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы.

Специалисты предостерегают от копирования несанкционированных, поддельных программ. Иногда, однако, и официально поставляемые программы могут быть источником заражения. В этом плане весьма показательна параллель между компьютерным вирусом и вирусом “AIDS”. Только упорядоченная жизнь с одним или несколькими партнерами способна уберечь от этого вируса. Беспорядочные связи со многими компьютерами почти наверняка приводят к заражению.

Наиболее распространенными методами защиты от компьютерных вирусов в настоящее время являются различные антивирусные программы (Norton antivirus, антивирус Касперского и др.).

Защитные антивирусные программы подразделяются на три вида:

Фильтрующие (препятствующие проникновению вируса),

противоинфекционные (постоянно контролирующие процессы в системе)

противовирусные (настроенные на выявление отдельных вирусов).

Следует подчеркнуть, что в качестве перспективного подхода к защите от компьютерных вирусов в последние годы все чаще применяется сочетание программных и аппаратных методов защиты. Среди аппаратных устройств такого плана можно отметить специальные антивирусные платы, которые вставляются в стандартные слоты расширения компьютера. Корпорация Intel в 1994 году предложила перспективную технологию защиты от вирусов в компьютерных сетях. Flash-память сетевых адаптеров Intel EtherExpress PRO/10 содержит антивирусную программу, автоматически сканирующую все системы компьютера еще до его загрузки.

Заметим, что пожелание ограничить использование нелицензированного сомнительного программного обеспечения скорее всего так и останется практически невыполнимым. Это связано с тем, что фирменные программы на лицензионных носителях стоят значительных денег в валюте. Поэтому избежать их несанкционированного противоправного копирования почти невозможно.

Следует отметить, что распространение компьютерных вирусов имеет и некоторые положительные стороны. В частности, они являются, по-видимому, лучшей защитой от похитителей программного обеспечения. Зачастую разработчики сознательно заражают свои дискеты каким-либо безобидным вирусом, который хорошо обнаруживается

любым антивирусным тестом. Это служит достаточно надежной гарантией, что никто не рискнет копировать такую дискету.

4.4. Преступная небрежность в нарушении правил эксплуатации ЭВМ, систем ЭВМ или их сетей.

Проблема неосторожности в области компьютерной техники аналогична неосторожной вине при использовании любого другого вида техники, транспорта и т.п. Особенностью компьютерной неосторожности является то, что безошибочных программ в принципе не бывает. Если проект практически в любой области техники можно выполнить с огромным запасом надежности, то в области программирования такая надежность весьма условна. а в ряде случаев почти не достижима.

4.5. Неправомерный доступ к компьютерной информации.

Понятие компьютерной информации определено в статье 272 УК РФ. **Предметом компьютерной информации** являются **информационные ресурсы**, которые в статье 2 Федерального закона от 20 февраля 1995 года **"Об информации, информатизации и защите информации"** рассматриваются как отдельные массивы документов в информационных системах. Эти ресурсы, согласно статье 2 Закона содержат сведения о лицах, предметах, событиях, процессах, населении независимо от формы их представления. В Законе дается полная расшифровка их содержания.

Особенность компьютерной информации – в ее относительно простых пересылке, преобразовании и размножении; при изъятии информации в отличии от изъятия вещи. Она легко сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут иметь одновременно практически неограниченное количество пользователей. Еще в 1982 году в предпринятом Верховным Судом СССР обзоре судебной практики были отражены условия использования компьютерной информации в уголовном судопроизводстве.[6] Чаще всего противоправный несанкционированный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов, технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных. Прогресс породил абсолютно новую категорию компьютерных преступников – хакеры[7]. По непроверенным данным в мире существуют целые преступные сообщества хакеров, где они обмениваются информацией, данными и тому подобным. В большинстве случаев преступления в сфере компьютерной информации совершаются ими. Хакеры. Для некоторых взлом и попытка разобраться в украденной в информации развлечение, для других бизнес. Они могут месяцами "стучаться" в закрытые паролями, системами защиты от копирования "двери" сетей или компьютеров конкретных людей перебирая простые слова в качестве пароля. И это не так глупо как кажется (по крайней мере было до недавнего времени). Есть еще несколько довольно простых и эффективных способов

6 См. Бюллетень Верховного Суда СССР, 1982, №6, стр. 22.
7 От английского hucker - взломщик

незаконного подключения к удаленным компьютерам. По этому поводу пишутся целые трактаты, их можно найти в неограниченном количестве в Интернете – глобальной всемирной компьютерной сети. Противоправный несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, преступник может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз как покупатель рассматривает товары на витрине или читатель выбирает книгу, просматривая полки библиотек. Программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Это создает возможности для нахождения "бре-шей". Авторы больших сложных программ могут не заметить некоторых сла-бостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавиться от них невозможно. Бывает, что программисты намеренно делают "бреши" для последующего использования. Прием "брешь" можно развить. В найденной (созданной)"бреши" программа "разрывается" и туда дополнительно вставляют одну или несколько команд. Этот "люк" "открывается" по мере необходимости, а встроенные команды автоматически осуществляют свою задачу. Чаще всего этот прием используется проектантами систем и работниками организаций, занимающихся профилактикой и ремонтом систем. Реже - лицами, самостоятельно обнаружившими "бреши". Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приема. Самый простой путь его осуществления - получить коды и другие идентифицирующие шифры законных пользователей. Здесь способов – великое множество, начиная с простого мошенничества. Иногда случается, как, например, с ошибочными телефонными звонками, что пользователь сети с удаленного компьютера подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеривался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом получить некоторую информацию, в частности кода. В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе ЭВМ, своеобразный аналог приспособлений, помещаемых в транспорте под надписью "Разбить стекло в случае аварии". Такая программа - мощный и опасный инструмент в руках злоумышленника.

Совсем недавно в России начали создаваться высшие учебные заведения для обучения специалистов в области информационной безопасности. Несанкционированный противоправный доступ может осуществляться и в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к непринадлежащим ему частям банка данных. Все происходит так, словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В таком случае он может проникнуть в чужие сейфы и похитить все, что в них хранится. Также под понятие "несанкционированного доступа" попадают такие частности, как ввод в программное обеспечение "логических бомб", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему. Способ "троянский конь" состоит в тайном введении в чужую программу таких команд, которые позволяют осуществить новые, не планировавшиеся владельцем программы функции, но одновременно

сохранять и прежнюю работоспособность. С помощью "троянского коня" преступники, например, отчисляют на свой счет определенную сумму с каждой операции. На самом деле все обстоит довольно просто: компьютерные программные тексты обычно чрезвычайно сложны. Они состоят из сотен тысяч, а иногда и миллионов команд. Поэтому "троянский конь" из нескольких десятков команд вряд ли может быть обнаружен, если, конечно, нет подозрений относительно этого. Но и в последнем случае экспертам-программистам потребуется много дней и недель, чтобы найти его.

Обратимся к истории компьютерных преступлений. Здесь, в частности, явно лидирует США, поскольку именно эта страна является местом прогрессивного развития современных компьютерных технологий и программного обеспечения. В этом плане показателен случай использования вредоносной программы по типу "троянского коня" одним американским программистом. Он вставил в программу компьютера фирмы, где работал, команды, не отчисляющие деньги, а не выводящие на печать для отчета определенные поступления. Эти суммы, особым образом маркированные, "существовали" только в системе. Украв бланки, он заполнял их с указанием своей секретной маркировки и получал эти деньги, а соответствующие операции по прежнему не выводились на печать и не могли подвергнуться ревизии. Есть еще одна разновидность вредоносной программы. Ее особенность состоит в том, что в безобидно выглядящую часть программы вставляются не команды, собственно выполняющие всю непосредственную работу. а команды, формирующие эти команды и после выполнения уничтожающие их. В это случае программисту, пытающемуся найти вредоносную программу необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе вредоносные программы, которые создают команды и т. д.(сколь угодно большое число раз), которые в свою очередь создают вредоносную программу "троянского коня".

4.6. Хищение компьютерной информации.

Темпы хищения компьютерной информации в современной России достигли небывалой величины, попытки повернуть на правовой путь распространения програмного обеспечения практически ни к чему не приводят. Хотя в последнее время видны ощутимые сдвиги: в частности в Москве работниками милиции и налоговыми инспекторами периодически проводятся рейды и проверки торговых точек, торгующих нелицензионной продукцией, конфискуется и уничтожается большое количество пиратских копий лазерных дисков, в 2002 году возбуждены 100 уголовных дел и т. п.[8]. Однако, если "обычные" хищения подпадают под действие существующего УК РФ, то проблема хищения информации значительно более сложна. Присвоение машинной информации, в том числе программного обеспечения, путем несанкционированного противоправного копирования не квалифицируется как хищение, поскольку хищение сопряжено с изьятием ценностей из фондов организации. Не очень далеко от истины утверждение, что в России все программное обеспечение распространяется только путем краж и обмена краденым. При неправомерном обращении в собственность машинная информация может не изыматься из фондов, а копироваться. Следовательно, как уже отмечалось выше, машинная информация должна быть выделена как самостоятельный предмет уголовно-правовой охраны.

Однако, что же это – компьютерная программа? Вещь? Материальный объект? Нематериальная ценность? Или нечто другое? На мой взгляд, компьютерная программа отличается главным образом тем, что поддается

8 Данные взяты из средств массовой информации и журнальных статей издательства "Компьютеруволд".

свободному копированию, не теряя при этом своих свойств. При этом виртуальные пространства позволяют размещать огромную информацию на ничтожно малом месте. За последние два года в правовой жизни нашего общества в сфере создания и использования произведений науки, литературы и искусства произошли существенные изменения. С принятием 9 июля 1993 года закона РФ "Об авторском праве и смежных правах" завершилось формирование российской системы авторского права как системы норм, предусматривающих защиту и охрану прав авторов соответствующий требованиям Бернской Конвенции об охране литературных и художественных произведений, являющейся своеобразным мировым эталоном защиты авторских прав. Вопросы, относящиеся к авторскому праву в информатике, к которым относятся и вопросы передачи прав на программу ЭВМ или базу данных из-за специфичности свойств объекта авторских прав в действующем российском законодательстве рассмотрены отдельно. Закон РФ “О правовой охране программ для электронных вычислительных машин и баз данных” (от 23 сентября 1992 г.) в статье 1 определяет следующие понятия:

программа для ЭВМ — это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения;

база данных — это объективная форма представления и организации совокупности данных (например: статей, расчетов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ;

адаптация программы для ЭВМ или базы данных — это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя;

модификация (переработка) программы для ЭВМ или базы данных - это любые их изменения, не являющиеся адаптацией;

декомпилирование программы для ЭВМ — это технический прием, включающий преобразование объектного кода в исходный текст в целях изучения структуры и кодирования программы для ЭВМ;

воспроизведение программы для ЭВМ или базы данных — это изготовление одного или более экземпляров программы для ЭВМ или базы данных в любой материальной форме, а также их запись в память;

распространение программы для ЭВМ или базы данных — это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей:

выпуск в свет (опубликование) программы для ЭВМ или базы данных - это предоставление экземпляров программы для ЭВМ или базы данных с согласия автора неопределенному кругу лиц (в том числе путем записи в память ЭВМ и выпуска печатного текста), при условии, что количество таких экземпляров должно удовлетворять потребности этого круга лиц, принимая во внимание характер указанных произведений;

использование программы для ЭВМ или базы данных - это выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модифицированной форме). Не признается использованием программы для ЭВМ или базы данных передача средствами

массовой информации сообщений о выпущенной в свет программе для ЭВМ или базе данных.

Правообладатель - автор, его наследник, а также любое физическое или юридическое лицо, которое обладает исключительными имущественными правами, полученными в силу закона или договора. Вышеназваный закон регулирует отношения, связанные с созданием, правовой охраной и использованием программ для ЭВМ и баз данных, в том числе и такую, во многих случаях решающую, их область, как передача прав на программу и базу данных. В соответствии с законом, имущественные права могут быть переданы автором полностью или частично любому физическому или юридическому лицу. Имущественные права на программу или базу данных переходят по наследству в установленном законом порядке, и их можно реализовать в течение срока действия авторского права. Передача имущественных прав должна быть оформлена на основании договора или контракта, который заключается в письменном виде. В договоре должны обязательно присутствовать следующие основные условия: объем и способы использования, порядок выплаты вознаграждения и срок действия договора, а также территория, на которой используется данный продукт[9]

Каждый законный пользователь информации имеет право использовать только тот программный продукт, который он получил на основании лицензионного договора либо приобрел путем покупки, взял в аренду или в прокат и т.д. В настоящее время в России существует достаточно эффективная законодательная база для реальной охраны и регулирования вопросов в сфере авторства. Но к сожалению, эти законы не подкреплены реальными действиями со стороны государства. Что же касается государства, то оно не предпринимает в этом направлении каких-либо эффективных действенных мер, поэтому от России отворачиваются многие перспективные иностранные партнёры. Думается, существенную роль в регулировании вопросов охраны информации стоит отвести органам МВД и специальным комиссиям[10]. Учитывая западный опыт следует подчеркнуть, что во многих странах мира, в органах полиции и прокуратуры существуют специальные отделы которые занимаются только вопросами охраны интеллектуальной собственности. Думается, государство не должно упускать те огромные суммы денег, которое оно недополучает в виде налогов, из-за нарушений в области охраны авторских и смежных прав. Неправомерный несанкционированный доступ к программному обеспечению для ЭВМ, к первичным документам баз данных и иной подобной информации, выполненной в виде рукописных записей, отпечатанной на принтере и иным типографским способом, не подразумевается в статье 272 и может в соответствующих случаях повлечь ответственность лишь по статьям Особенной части[11]. Овладение компьютером, не имеющим источников питания, а также машинным носителем как вещью, не рассматривается как доступ к компьютерной информации и в соответствующих случаях может повлечь ответственность по статьям о преступлениях против собственности. Точно так же не образует объективной стороны данного преступления уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитным излучением, ударами и иными подобными способами. Также стоит упомянуть о том, что правила обращения с компьютерной информацией могут устанавливаться собственником либо владельцем информации, законом, иным нормативным актом. Информация охраняется законом, то есть существует информация, изъятая из публичного открытого оборота на основании закона, или иных нормативных (включая ведомственные) актов. Существует так

9 См. ст. №1 Закона "О правовой охране программ для электронных вычислительных машин и баз данных."

10 См. ст.146 УК РФ “Нарушение авторских и смежных прав.”

11 См. ст. 137, 138, 183 УК РФ

называемый "гриф ограниченного пользования". Из толкования закона также можно судить, что частные фирмы, включая коммерческие банки, вправе самостоятельно устанавливать ограниченные грифы в целях сохранения коммерческой, банковской, и иных тайн.

4.7. Уничтожение компьютерной информации.

Под термином уничтожения информации понимается стирание из логической памяти ЭВМ. Одновременный перевод информации на другой носитель не считается в контексте уголовного закона уничтожением компьютерной информации лишь в том случае, если в результате этих действий доступ правомерных пользователей не оказался существенно затруднен, а то и вовсе исключен. Имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от других пользователей, не освобождает виновного от уголовной ответственности. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое "вытеснение" старых версий файлов новыми. Блокирование информации – искусственное затруднение доступа пользователей к компьютерной информации, не связанной с ее уничтожением. От уничтожения и блокирования следует отличать вывод из строя компьютерной программы; в последнем случае программа для компьютера может быть доступна как организованная в виде файла информация, но не как объект взаимодействия с пользователем.

4. 8. Подделка компьютерной информации.

По-видимому этот метод компьютерной преступности является одним из наиболее распространенным. Он является разновидностью несанкционированного доступа с той разницей, что пользоваться им может, как правило, не посторонний пользователь, а сам разработчик причем имеющий достаточно высокую профессиональную квалификацию.

Состав преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удается сдать заказчику заведомо неисправную продукцию. К подделке информации можно отнести также искажение результатов выборов, голосований, референдумов и т. п. Ведь если каждый голосующий не может убедиться, что его голос зарегистрирован правильно, то всегда возможно внесение искажений в итоговые протоколы. Естественно, что подделка информации может преследовать и другие цели.

Рассмотрим теперь категорию компьютерных преступлений, в которых компьютер является **"средством" достижения преступных целей**. В тех случаях, когда компьютерная аппаратура является предметом преступления против собственности, соответственно ее хищение, уничтожение или повреждение подлежит квалификации по статьям 158-168 УК РФ. Но дело в том, что информационная структура (например программы и информация) не может быть преступлением против собственности, поскольку машинная информация не отвечает ни одному из основных принципов предмета преступления против собственности, в частности, она не обладает физическим признаком (другими

словами ее просто нет в реальном мире, она эфемерна).

Что же касается компьютера как **орудия преступления**, то его следует рассматривать в ряду таких средств, как оружие или транспортное средство. В этом смысле использование компьютера имеет уже прикладное значение при совершении преступления, то есть хищения денежных средств, сокрытие налогов. Кроме того, компьютер может использоваться в целях хранения какой-либо информации, он может служить типографским станком, аппаратурой для неправомерного доступа в базы данных, копирования информации и так далее. Такие противоправные действия не рассматриваются в качестве самостоятельных преступлений, а подлежат квалификации по иным статьям в соответствии с объектом посягательства[12]. Проблема заключается в том, что компьютер по сути своей универсален, и позволяет выполнять практически любую работу очень широкого круга назначения[13]. Здесь также можно выделить разработку сложных математических моделей, входными данными в которых являются возможные условия проведения преступления, а выходными данными - рекомендации по выбору оптимального варианта действий преступника.

Другой вид преступлений с использованием компьютеров получил название **"воздушный змей"**[14]. Преступный метод заключается в следующем. В простейшем случае требуется открыть в двух банках по небольшому счету. Далее деньги переводятся из одного банка в другой и обратно с постепенно повышающимися суммами. Хитрость заключается в том, чтобы до того, как в банке обнаружится, что поручение о переводе не обеспечено необходимой суммой, приходило бы извещение о переводе в этот банк так чтобы общая сумма покрывала требование о первом переводе . Этот цикл повторяется большое число раз ("воздушный змей" поднимается все выше и выше) до тех пор, пока на счете не оказывается приличная сумма (фактически она постоянно "перескакивает" с одного счета на другой, увеличивая свои размеры). Тогда деньги быстро снимаются и фиктивный владелец счета исчезает. Этот способ требует очень точного расчета, но для двух банков его можно сделать и без компьютера. На практике в такую игру включают большое количество банков: так сумма накапливается быстрее и число поручений о переводе не достигает подозрительной частоты. Но управлять этим процессом можно только с помощью мощного компьютера.

ГЛАВА 5.
ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИТИИ.

В предыдущих главах было аргументировано показано, что в результате создания, распространения и использования вредоносной программы, а также выхода из строя или ошибки в работе компьютерного обеспечения могут привести к тяжелым последствиям. Именно поэтому вопросы компьютерной безопасности становятся первоочередными. Среди наиболее эффективным мер, направленных на

12 См. Новое уголовное право России. Особенная часть, М., 1996 года, страница 241 – 274.

13 В частности, стоит упомянуть открытый эффект "двадцать пятого кадра", который якобы позволят осуществлять на человека внушающее воздействие на уровне подсознания. Ученые утверждают, что таким способом вполне можно воздействовать на сознание и психику человека.

14 Пример взят из книги Д.Ведеева Защита данных в компьютерных сетях М., 1999, № 3, стр. 12

предупреждение преступлений в сфере компьютерной информации выделяют **технические, организационные и правовые.**

1) К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

2) К организационным мерам относится охрана вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

3) К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы государственного контроля за разработчиками компьютерных программ и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран и др.

ГЛАВА 6.
СПОСОБЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ.

Концентрация информации в машинной памяти компьютеров - аналогично концентрации наличных денег в банках - заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, частная тайна, национальная безопасность - все эти положения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Исследования в этом направлении привели к появлению новой дисциплины: безопасность информации. Специалист в области безопасности информации отвечает за разработку, реализацию и эксплуатацию системы обеспечения информационной безопасности, направленной на поддержание целостности, пригодности и конфиденциальности накопленной в организации информации. В его функции входит обеспечение физической (технические средства, линии связи и удаленные компьютеры) и логической (данные, прикладные программы, операционная система) защиты информационных ресурсов.

При рассмотрении проблем защиты данных в сети прежде всего возникает вопрос о классификации сбоев и нарушений прав доступа, которые могут привести к уничтожению или нежелательной модификации данных. Среди таких потенциальных “угроз” можно выделить :

1. Сбои оборудования :

- сбои кабельной системы;

- перебои электропитания;
- сбои дисковых систем;
- сбои систем архивации данных;
- сбои работы серверов, рабочих станций,сетевых карт и т.д.

2. Потери информации из-за некорректной работы оборудования:

- потеря или изменение данных при ошибках оборудования;
- потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом :

- несанкционированное копирование, уничтожение или подделка информации;
- ознакомление с конфиденциальной информацией, составляющей тайну, посторонних лиц;

4. Потери информации, связанные с неправильным хранением архивных данных.

5. Ошибки обслуживающего персонала и пользователей :

- случайное уничтожение или изменение данных;
-некорректное использование программного и аппаратного обеспечения, ведущее к уничтожению или изменению данных;

В зависимости от возможных видов нарушений работы сети (под нарушением работы подразумевается и противоправный несанкционированный доступ) многочисленные виды защиты информации объединяются в три основных класса :

- **средства физической защиты**, включающие средства защиты кабельной системы, систем электропитания, средства архивации, дисковые массивы и т.д.

-**средства защиты от стихийных бедствий -** пожаров, землетрясений, наводнений и т.д. - состоит в хранении архивных копий информации или в размещении некоторых сетевых устройств, например, серверов баз данных, в специальных защищенных помещениях, расположенных, как правило, в других зданиях или, реже, даже в другом районе города или в другом городе.

- **программные средства защиты,** в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.

- **административные меры защиты**, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.

Следует отметить, что подобное деление достаточно условно, поскольку современные технологии развиваются в направлении сочетания программных и аппаратных средств защиты. Наибольшее распространение такие **программно-аппаратные средства** получили, в частности, в области контроля доступа, защиты от вирусов и т.д.

Проблема защиты информации от противоправного несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей. Необходимо также отметить, что зачастую ущерб наносится не из-за “злого умысла”, а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем. Так, крупнейший производитель сетевых ОС - корпорация Novell - в своем последнем продукте NetWare 4.1 предусмотрел помимо стандартных средств ограничения доступа, таких, как система паролей и разграничения полномочий, ряд новых возможностей, обеспечивающих первый класс защиты данных. Новая версия NetWare предусматривает, в частности, возможность кодирования

данных по принципу “открытого ключа” (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов. В то же время в такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются специальным известным законным пользователем паролем. Не секрет, что пароль можно подсмотреть или подобрать. Для исключения возможности неавторизованного входа в компьютерную сеть в последнее время используется комбинированный подход - пароль + идентификация пользователя по персональному “ключу”. В качестве “ключа” может использоваться пластиковая карта (магнитная или со встроенной микросхемой - smart-card) или различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза или отпечатков пальцев, размерам кисти руки и так далее.

Оснастив сервер или сетевые рабочие станции, например, устройством чтения смарт-карточек и специальным программным обеспечением, можно значительно повысить степень защиты от противоправного несанкционированного доступа. В этом случае для доступа к компьютеру законный пользователь должен вставить смарт-карту в устройство чтения и ввести свой персональный код. Программное обеспечение позволяет установить несколько уровней безопасности, которые управляются системным администратором. Возможен и комбинированный подход с вводом дополнительного пароля, при этом приняты специальные меры против “перехвата” пароля с клавиатуры. Этот подход значительно надежнее применения паролей, поскольку, если правонарушитель каким-то образом узнал специальный пароль, законный пользователь об этом может не знать, если же пропала карточка, можно принять меры немедленно. Смарт-карты управления доступом позволяют реализовать, в частности, такие функции, как контроль входа, доступ к устройствам персонального компьютера, доступ к программам, файлам и командам. Кроме того, возможно также осуществление контрольных функций, в частности, регистрация попыток нарушения доступа к ресурсам, использования запрещенных утилит, программ, команд DOS.

Одним из удачных примеров создания комплексного решения для контроля доступа к компьютерной информации в открытых системах, основанного как на программных, так и на аппаратных средствах защиты, стала система Kerberos. В основе этой схемы авторизации лежат три компонента:

- **База данных**, содержащая информацию по всем сетевым ресурсам, пользователям, паролям, шифровальным ключам и т.д.
- **Авторизационный сервер** (authentication server), обрабатывающий все запросы пользователей на предмет получения того или иного вида сетевых услуг. Авторизационный сервер, получая запрос от пользователя, обращается к базе данных и определяет, имеет ли пользователь право на совершение данной операции. Примечательно, что пароли пользователей по сети не передаются, что также повышает степень защиты информации.
- **Ticket-granting server** (сервер выдачи разрешений) получает от авторизационного сервера “пропуск”, содержащий имя пользователя и его сетевой адрес, время запроса и ряд других параметров, а также уникальный сессионный ключ. Пакет, содержащий “пропуск”, передается также в зашифрованном по алгоритму DES виде. После получения и расшифровки “пропуска” сервер выдачи разрешений проверяет запрос и сравнивает ключи и затем дает “добро” на использование сетевой аппаратуры или программ.

Среди других подобных комплексных схем можно отметить разработанную Европейской Ассоциацией Производителей Компьютеров (ECMA) систему Sesame (Secure European System for Applications in Multivendor Environment), предназначенную для использования в крупных гетерогенных сетях.

По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов, возникает необходимость доступа удаленных пользователей (или групп пользователей) к вычислительным и информационным

ресурсам главного офиса компании. Компания Datapro свидетельствует, что уже в 1995 году только в США число работников постоянно или временно использующих удаленный доступ к компьютерным сетям, составит 25 миллионов человек. Чаще всего для организации удаленного доступа используются кабельные линии (обычные телефонные или выделенные) и радиоканалы. В связи с этим защита информации, передаваемой по каналам удаленного доступа, требует особого подхода. В частности, в маршрутизаторах удаленного доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям,- что делает невозможным "перехват" данных при незаконном несанкционированном подключении правонарушителя "хакера" к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможности расшифровки "перехваченных" данных. Кроме того, маршрутизаторы удаленного доступа могут быть запрограммированы таким образом, что удаленные пользователи будут ограничены в доступе к отдельным ресурсам сети главного офиса.

Также разработаны и специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой AT&T предлагается модуль Remote Port Security Device (PRSD), представляющий собой два блока размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удаленного пользователя. RPSD Key и Lock позволяют установить несколько уровней защиты и контроля доступа, в частности:

- **шифрование данных**, передаваемых по линии при помощи генерируемых цифровых ключей;
- **контроль доступа** в зависимости от дня недели или времени суток (всего 14 ограничений).

Широкое распространение радиосетей в последние годы поставило разработчиков радиосистем перед необходимостью защиты информации от "хакеров", вооруженных разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиосети компании RAM Mobil Data информационные пакеты передаются через разные каналы и базовые станции, что делает практически невозможным для посторонних собрать всю передаваемую информацию воедино. Активно используются в радио сетях и технологии шифрования данных при помощи алгоритмов DES и RSA.

Шифрование компьютерной информации. Сложность создания системы защиты информации определяется тем, что данные могут быть похищены преступником из компьютера и одновременно оставаться на месте; ценность некоторых данных заключается в обладании ими, а не в уничтожении или изменении. Обеспечение безопасности информации - дорогое дело, и не столько из-за затрат на закупку или установку средств, сколько из-за того, что трудно квалифицированно определить границы разумной безопасности и соответствующего поддержания системы в работоспособном состоянии. Если локальная сеть разрабатывалась в целях совместного использования лицензионных программных средств, дорогих цветных принтеров или больших файлов общедоступной информации, то нет никакой потребности даже в минимальных системах шифрования/дешифрования информации.

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ. Анализ риска должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь, снижение коэффициента готовности системы, общественные отношения, юридические проблемы) и предоставить информацию для определения подходящих типов и уровней безопасности. Коммерческие организации все в большей степени переносят критическую корпоративную информацию с больших вычислительных систем в среду открытых систем и встречаются с новыми и сложными

проблемами при реализации и эксплуатации системы безопасности. Сегодня все больше организаций разворачивают мощные распределенные базы данных и приложения клиент/сервер для управления коммерческими данными. При увеличении распределения возрастает также и риск неавторизованного доступа к данным и их искажения.

Шифрование данных традиционно использовалось правительственными и оборонными департаментами, но в связи с изменением потребностей и некоторые наиболее солидные компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

Практика экономически развитых стран, прежде всего США показывает, что финансовые службы компаний представляют важную и большую пользовательскую базу и часто специфические требования предъявляются к алгоритму, используемому в процессе шифрования. Опубликованные алгоритмы, например DES (см. ниже), являются обязательными. В то же время, рынок коммерческих систем не всегда требует такой строгой защиты, как правительственные или оборонные ведомства, поэтому возможно применение продуктов и другого типа, например PGP (Pretty Good Privacy).

Шифрование данных может осуществляться в режимах **On-line** (в темпе поступления информации) и **Off-line** (автономном). Наибольший интерес и практическое применение имеет первый тип с его основными алгоритмами.

Стандарт шифрования данных DES (Data Encryption Standart) был разработан фирмой IBM в начале 70-х годов и в настоящее время является правительственным стандартом для шифрования цифровой информации. Он рекомендован Ассоциацией Американских Банкиров. Сложный алгоритм DES использует ключ длиной 56 бит и 8 битов проверки на четность и требует от злоумышленника перебора 72 квадрилионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм удовлетворительно решает проблему превращения конфиденциальной информации в недоступную.

Алгоритм RSA был изобретен Ривестом, Шамиром и Альдеманом в 1976 году и представляет собой значительный шаг в криптографии. Этот алгоритм также был принят в качестве стандарта Национальным Бюро Стандартов DES, технически является СИММЕТРИЧНЫМ алгоритмом, а RSA -- АСИММЕТРИЧНЫМ, то есть он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Открытый ключ используется для шифрованием сообщения пользователем, но только определенный получатель может дешифровать его своим секретным ключом; открытый ключ бесполезен для дешифрования. Это делает ненужными секретные соглашения о передаче ключей между корреспондентами. DES определяет длину данных и ключа в битах, а RSA может быть реализован при любой длине ключа. Чем длиннее ключ, тем выше уровень безопасности (но становится длительнее и процесс шифрования и дешифрования). Если ключи DES можно сгенерировать за микросекунды, то примерное время генерации ключа RSA - десятки секунд. Поэтому открытые ключи RSA предпочитают разработчики программных средств, а секретные ключи DES - разработчики аппаратуры.

ВЫВОДЫ, РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ.

Проведенное в настоящей работе исследование российского уголовного законодательства в сфере компьютерной информации, раскрытие понятия, состава преступлений в сфере компьютерной информации, рассмотрение отдельных видов

компьютерных преступлений и способов защиты компьютерной информации от преступных посягательств позволяет сделать следующие выводы:

1) В настоящее время в нашей стране накоплена богатая научно-теоретическая база, которая свидетельствует о складывающемся устойчивом правовом механизме, нацеленным на защиту компьютерной информации. В 1992 году был принят Закон России **о правовой охране программ для электронно-вычислительных машин и баз данных,** в 1994 году **— Гражданский кодекс**, который содержит ряд норм, связанных с компьютерной информацией, в 1995 году **— Федеральный закон об информации, информатизации и защите информации.** Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в **УК РФ 1996 года** группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления.

2) Однако, в действующем российском законодательстве пока еще нет четкого представления о правовом механизме защиты компьютерной информации как целостной разработанной правовой системы. Компьютерная преступность не знает границ, она выходит за пределы российской действительности. Это международное понятие и бороться с ней надо согласованно и сообща. С внедрением в человеческую жизнь новых компьютерных технологий, когда обмен информацией стал быстрым, дешевым и эффективным, преступность в информационной сфере переросла за рамки тех уголовно-правовых норм, направленных для борьбы с ней. Компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства.

3) Проблемы информационной безопасности постоянно усугубляется процессами незаконного несанкционированного проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего компьютерных вычислительных систем. Не случайно поэтому защита компьютерной информации становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано три базовых принципа информационной безопасности, которая должна обеспечивать:

целостность данных - защиту от несанкционированных сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных.

конфиденциальность (законность) информации

доступность для всех авторизованных зарегистрированных пользователей

защита компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка);

Анализ действующего российского уголовного законодательства в сфере компьютерной информации позволяет говорить о необходимости нескольких правовых проблем, которые могут быть рассмотрены в качестве составных частей правового механизма защиты компьютерной информации:

1. Установление контроля над несанкционируемым, противоправным доступом к компьютерным информационным данным системы[15].

2. Ответственность за выполнение технологических операций, связанных с правовой защитой компьютерной информации.

Среди наиболее эффективным мер, направленных на предупреждение преступлений в сфере компьютерной информации выделяют **технические, организационные и правовые.**

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в

15 Венгеров А.Б. Право и информация в условиях автоматизации управления: теоретические вопросы. М. Норма, 1999, стр. 14-21.

случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам относится охрана вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.

К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы государственного контроля за разработчиками компьютерных программ и принятие международных договоров об их ограничениях, если они влияют или могут повлиять на военные, экономические и социальные аспекты стран и др.

В заключении следует подчеркнуть, что даже самые современные аппаратные, программные и любые другие научные методы, по-видимому, не смогут гарантировать абсолютную надежность и безопасность компьютерной безопасности. В то же время свести риск потерь к минимуму возможно лишь при комплексном правовом подходе к вопросам защиты компьютерной безопасности.

Список использованной литературы и нормативно-правовых актов и материалов судебной практики.

Литература

1. *Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. - М., 2001г, стр. 29-32.*
2. *Беляев В.С. Безопасность в распределительных системах. – М., 1999г, стр. 89-91.*
3. *Борзенков Г.Н. Крмиссаров В.С. Уголовное право Российской Федерации. – М.: Олимп, 1998г, стр. 33-42.*
4. *Ведеев Д.В. Защита данных в компьютерных сетях. - М., 1998, стр. 55-78.*
5. *Здравомыслов Б.В. Уголовное право России. Особенная часть. – М.: Юристъ, 1996, стр. 98-105*
6. *Копылов В.А. Информационное право. – М.:Юристъ, 2002г, стр. 40-43.*
7. *Наумов А.В. Комментарий к Уголовному кодексу. – М.:Юристъ, 1997г, стр. 23-48.*
8. *Скуратов Ю.И. Лебедев В.М. Комментарий к Уголовному кодексу. – М., 1996г, стр. 45-67.*
9. *М. Рааб (M. Raab) Защита сетей: наконец-то в центре внимания // Компьютерволд Москва, 1996, № 29, стр. 18.*

10. *Д. Векслер (J.Wexler) Наконец-то надежно обеспечена защита данных в радиосетях // Компьютеруорлд Москва, 1998, № 17, стр. 13-14.*
11. *С.В.Сухов Система безопасности NetWare//"Сети", 2001, № 4, стр. 60-70.*
12. *В. Беляев Безопасность в распределительных системах // Открытые системы Москва, 2002, № 3, стр. 36-40.*
13. *Д.Ведеев Защита данных в компьютерных сетях // Открытые системы Москва, 2001, № 3, стр. 12-18.*
14. *А. Б. Венгеров. Право и информация в условиях автоматизации управления. Теоретические вопросы. М. Норма., 1999г, стр. 14-21.*
15. *Борьба с компьютерной преступностью за рубежом-научно-аналитический обзор, М. Академия МВД РФ, 1995г, стр. 1- 173.*
16. *Гоилейчук В.Д., Зубань М.А. Компьютерные преступления: социально-правовой и криминолого-криминалистический аспекты, Киев, 1994, стр. 101-112.*
17. *Ю. Гульбин. Преступления в сфере компьютерной информации // Российская юстиция, 1997, № 10.*
18. *Д. Ляпунов, В. Максимов. Ответственность за компьютерные преступления // Законность, 1997, № 1.*
19. *И. Никифоров, Уголовные меры борьбы с компьютерной преступностью // Защита информации, 1995, № 5.*
20. *В. Федоров. Компьютерные преступления: выявление, расследование и профилактика. // Законность. 1994, № 6.*
21. *А.Б. Мельниченко, С.Н. Радачинский. Уголовное право. Особенная часть. Ростов-на-Дону, 2002г, стр. 298-300.*
22. *Уголовное право. Особенная часть. / ред. И.Я. Казаченко, М. Норма, 2001, стр. 554-560.*

Нормативно-правовые акты

1. *Уголовный Кодекс Российской Федерации*
2. *Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ // СЗ РФ 1995, №6, стр. 609.*
3. *Закон Российской Федерации "Об авторском и смежных правах" от 9 июля 1993 года №5351-1*
4. *Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" от 23 сентября 1992 года №3523-1 // Ведомости РФ, 1992, № 42, стр. 2325.*
5. *Гражданский Кодекс Российской Федерации, М. Ось, стр. 104-108.*
6. *Ведомости РФ, 1992 г, № 42, стр. 2325*

Материалы судебной практики

1. *Бюллютень Верховного суда СССР, 1982 г, № 6, стр. 22.*
2. *Бюллетень Верховного суда РФ, 1993г, № 11, стр. 89.*
3. *Журнальные статьи издательства "Компьтеруволд" .*