Ташкентский государственный
юридический институт

Компьютерная преступность и компьютерная безопасность

Выполнила:
Холиков Уткир Уктамович,

ТАШКЕНТ
2011 год

Содержание

Введение

Изменения происходящие в экономической жизни России – создание финансово-кредитной системы; предприятий различных форм собственности и т. п. – оказывают существенное влияние на вопросы защиты информации. Долгое время в нашей стране существовала только одна собственность – государственная, поэтому информация и секреты были тоже только государственные, которые охранялись мощными спецслужбами.

Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего вычислительных систем. Это даёт основание поставить проблему компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений. Объектом посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением. Квалификация правонарушения зависит от того, является ли компьютер только объектом посягательства или он выступает в роли инструмента.

Цель работы – *исследование компьютерной преступности и компьютерной безопасности.*

Данная цель определила основные задачи работы:

1. Осветить возможные способы компьютерных преступлений;
2. Выявить методы защиты от них.

Следует отметить, что хищение информации почти всегда связано с потерей материальных и финансовых ценностей. Каждый сбой работы компьютерной сети это не

только моральный ущерб для работников предприятий и сетевых администраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота и других, серьёзный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям. Не случайно, что защита данных в компьютерных сетях становится одной из самых острых проблем в современной информатике.

Необходимо также отметить, что отдельные сферы деятельности (банковские и финансовые институты, информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер безопасности данных и предъявляют повышенные требования к надёжности функционирования информационных систем, в соответствии с характером и важностью решаемых ими задач.

Глава 1

Компьютерная преступность и компьютерная безопасность

§1 Компьютерная преступность

Ещё совсем недавно ни в одном из уголовных кодексов союзных республик невозможно было найти главу под названием «Компьютерные преступления». Таким образом компьютерных преступлений, как преступлений специфических в юридическом смысле не существовало.

Уголовный Кодекс Российской Федерации (далее УК РФ), введённый в действие с 1-го января 1997 года содержит главу №28 «Преступления в сфере компьютерной информации»

Понятие компьютерной информации определено в комментируемой статье. Предметом компьютерной информации являются информационные ресурсы, которые в статье Федерального закона от 20 февраля 1995 года «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 статье 2 Закона содержат сведения о лицах, предметах, событиях, процессах, населении независимо от формы их представления. В законе далее даётся полная расшифровка их содержания.

Уголовно-правовая защита компьютерной информации в российском уголовном законодательстве введена впервые. Ранее, 23 сентября 1992 года, был принят закон «О правовой охране программ для электронно-вычислительных машин и баз данных»[1] и 20 февраля 1995 года – федеральный закон «Об информации,

[1] См. Ведомости РФ, 1992 г., №42, ст. 2325

информатизации и защите информации»[1]. В этих законах предусмотрен комплекс мер по защите ЭВМ, баз данных, сетей и в целом компьютерной информации. В статье 20 Закона от 23 сентября 1992 года содержалось положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных, либо незаконное воспроизведение или распространение таких произведений влечёт за собой уголовную ответственность в соответствии с законом. Однако соответствующие уголовно-правовые нормы тогда не были приняты. Очевидно, посчитали достаточной статью 141 УК РСФСР, хотя она ответственности за упомянутые деяния не предусматривала. Эти вопросы, по моему мнению, решены в статьях 146 и 147 УК (смотри комментарии к этим статьям).

Включение статьи 272, как и статей 273 и 274 УК, в раздел о преступлениях, посягающих на общественную безопасность и общественный порядок, определяет объект рассматриваемых преступлений. Но это был бы слишком общий подход. 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 отличить преступления, предусмотренные статьями 272-274 УК РФ, 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 её хищение, уничтожение или повреждение подлежит квалификации по статьям 158-168 УК РФ. Но дело в том, что информационная структура (программы и информация) не может быть предметом преступлений против собственности, поскольку машинная информация не отвечает ни одному из критериев предмета преступлений против собственности, в частности не обладает физическим

[1] См. СЗ РФ, 1995 г., №8, ст. 609

признаком. Что касается компьютера как орудия преступления, то его следует рассматривать в ряду таких средств, как оружие или транспортные средства. В этом смысле использование компьютера имеет прикладное значение при совершении преступления, например хищение денежных средств или сокрытие налогов. Такие действия не рассматриваются в качестве самостоятельных преступлений, а подлежат квалификации по другим статьям УК РФ в соответствии с объектом посягательства [1].

Попытаемся кратко обрисовать явление, которое как социологическая категория получило название «Компьютерная преступность». Компьютерные преступления условно можно разделить на две больших категории – преступления, связанные с вмешательством в работу компьютеров, и, преступления, использующие компьютеры как необходимые технические средства.

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

1. Неправомерный доступ к компьютерной информации (статья 272), хранящейся в компьютере.

Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать самовольное получение информации без разрешения её собственника или владельца. В связи с тем, что речь идёт об охраняемой законом информации, неправомерность доступа к ней потребителя характеризуется ещё и нарушением установленного порядка доступа к этой информации. Если нарушен установленный порядок доступа к охраняемой законом информации, согласие её собственника или владельца не исключает, по моему мнению, неправомерности доступа к ней.

Собственником информационных ресурсов, информационных систем, технологии и средств их обеспечения является субъект, в полном объёме

[1] См. подробнее: Новое уголовное право. Особенная часть, М., 1996 г., с. 271-274

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.

Неправомерный доступ осуществляется, как правило, с использованием чужого имени, фиктивных документов, изменением физических адресов, технических устройств, использованием информации, оставшейся после решения задач, модификации программного и информационного обеспечения, хищение носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных, нарушением средств или систем защиты информации.

Хакеры, «электронные корсары», «компьютерные пираты» – так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети для забавы. Набирая наудачу один номер за другим, они терпеливо дожидаются пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приёмник сигналов в собственной ЭВМ, и связь установлена. Если теперь угадать код (а слова, которые служат паролем часто банальны), то можно внедриться в чужую компьютерную систему.

Несанкционированный доступ к файлам законного пользователя осуществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может не спеша исследовать содержащуюся в системе информацию, копировать её, возвращаться к ней много раз, как покупатель рассматривает товары на витрине.

Программисты иногда допускают ошибки в программах, которые не удаётся обнаружить в процессе

отладки. Авторы больших, сложных программ могут не заметить некоторых слабостей логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небрежности, ошибки приводят к появлению «брешей».

Обычно они всё-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что некто проникает в компьютерную систему, выдавая себя за законного пользователя системы, которые не обладают свойствами аутентичной идентификации (например по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого приёма. Самый простейший путь его осуществления: - получить коды и другие идентифицирующие шифры законных пользователей. Это может делаться:

- Приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;
- Обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;
- Подслушиванием через телефонные линии.

Иногда случается, как например, с ошибочными телефонными звонками, что пользователь с удалённого 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 течении определённого времени и таким образом получить некоторую 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 приспособлений, помещаемых в транспорте под надписью «разбить стекло в случае аварии». Такая программа – мощный и опасный инструмент в руках злоумышленника.

Несанкционированный доступ может осуществляться в результате системной поломки. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Всё 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 всё, что в них хранится.

Ответственность по статье 272 УК РФ наступает в том случае, если деяние повлекло указанные в части 1 этой статьи последствия.

Под уничтожением информации следует понимать её утрату при невозможности её восстановления.

Блокирование информации – это невозможность её использования при сохранности такой информации.

Модификация информации означает изменение её содержания по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя.

Под копированием информации следует понимать её переписывание, а также иное тиражирование при сохранении оригинала. Представляется, что копирование может означать и её разглашение.

Нарушение работы ЭВМ, системы ЭВМ или их сети может выразиться в их произвольном отключении, в отказе выдать информацию, в выдаче искажённой информации при сохранении целостности ЭВМ, системы ЭВМ и их сети.

Неправомерный доступ к компьютерной информации считается оконченным с момента наступления в результате

этого неправомерного доступа к ней одного или нескольких из упомянутых последствий.

Представляется, что к лицам, как указывается в части 2 статьи 272 УК РФ, «равно имеющим доступ» к ЭВМ, системе ЭВМ, или их сети, положение части первой этой статьи о несанкционированном доступе к компьютерной информации относится в тех случаях, когда они вышли за пределы определённых им обязанностей по работе и вторглись в ту сферу компьютерной информации, на которую их обязанности не распространяются. Полагаю, что о других случаях несанкционированного доступа к компьютерной информации для лиц, уже имеющих доступ, говорить вряд ли можно.

С субъективной стороны преступление может быть совершено только с прямым умыслом. Мотивами преступления могут быть корыстные или хулиганские побуждения, месть, зависть и т. д.

Субъектом преступления, предусмотренного частью 1 статьи 272 УК РФ, а также при совершении его группой лиц могут быть любые лица достигшие 16 лет. При совершении преступления, предусмотренного частью 2 этой статьи, при других обстоятельствах, субъектами могут быть лишь лица, занимающие определённое служебное положение или имеющие доступ к ЭВМ, системе ЭВМ или их сети, т. е. субъект специальный.

2. Ввод в программное обеспечение «логических бомб» (статья 273 «Создание, использование и распространение вредоносных программ для ЭВМ»), которые срабатывают при выполнении определённых условий и частично или полностью выводят из строя компьютерную систему.

«Временная бомба» - разновидность «логической бомбы», которая срабатывает по достижении определённого момента времени. Способ «троянский конь» состоит в тайном введении в чужую программу таких команд,

которые позволяют осуществлять новые, не планировавшиеся владельцем программные функции, но одновременно сохраняют и прежнюю работоспособность.

С помощью «троянского коня» преступники, например, отчисляют на свой счёт определённую сумму с каждой операции.

Компьютерные командные 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.

Есть ещё одна разновидность «троянского коня». Её особенность состоит в том, что в безобидно выглядящий кусок программы вставляются не команды, собственно, выполняющие «грязную» работу, а команды, формирующие эти команды и после выполнения уничтожающие их. В этом случае программисту, пытающемуся найти «троянского коня», необходимо искать не его самого, а команды его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т. д. (сколько угодно большое количество раз), создающие «троянского коня».

В США получила распространение форма компьютерного вандализма, при которой «троянский конь» разрушает через какой-то промежуток времени все программы, хранящиеся в памяти машины. Во многих поступивших в продажу компьютерах оказалась «временная бомба», которая "взрывается" в самый неожиданный момент, разрушая всю библиотеку данных. Не следует думать, что «логические бомбы» – это экзотика, несвойственная нашему обществу.

3. Разработка и распространение компьютерных вирусов (статья 273)

В статье 273 УК РФ речь идёт о разработке и распространении компьютерных вирусов путём создания программ для ЭВМ или внесения изменений в существующие программы. Опасность компьютерного вируса состоит в том, что он может привести, как следует из текста комментируемой статьи, 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.

Именно высокой степенью общественной опасности объясняется то, что уголовный закон преследует достаточно строго за сам факт создания программ для ЭВМ или внесения изменений в существующие программы, не оговаривая наступления каких-либо последствий.

Преступление предусмотренное статьёй 273 УК РФ, считается оконченным, когда программа создана или внесены изменения в существующую программу, независимо от того, была ли она использована или распространена.

Под использованием, либо распространением вредоносных программ или машинных носителей к ним понимается, соответственно, введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам.

Представляется, что под распространением вредоносных программ следует понимать и их копирование.

С субъективной стороны преступление может быть совершено 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

ставит виновный, а когда наступили последствия, к достижению которых он стремился, - и в зависимости от наступивших последствий. В этом случае действия, предусмотренные статьёй 273 УК РФ, оказываются лишь способом достижения поставленной цели. Совершённое деяние подлежит квалификации по совокупности совершённых преступлений.

К тяжким последствиям, наступившим по неосторожности (часть 2), могут быть отнесены, например, гибель людей, причинение вреда их здоровью, дезорганизация производства на предприятии или в отрасли промышленности, осложнение дипломатических отношений с другим государством, возникновение вооружённого конфликта. При этом необходимо иметь ввиду, что наступившие последствия по совокупности с другими преступлениями в зависимости от характера последствий и отнесения заведомости к легкомыслию или к косвенному умыслу в виде безразличного отношения к последствиям.

Субъектом преступления может быть любое лицо, достигшее 16 лет.

«Троянские кони» типа «сотри все данные этой программы, перейди в следующую и сделай тоже самое» обладают свойствами переходить через коммуникационные сети из одной системы в другую, распространяясь как вирусное заболевание.

Выявляется вирус не сразу: первое время компьютер «вынашивает инфекцию», поскольку для маскировки вирус нередко используется в комбинации с «логической бомбой» или «временной бомбой». Вирус наблюдает за всей обрабатываемой информацией и может перемещаться, используя пересылку этой информации. Всё происходит, как если бы он заразил белое кровяное тельце и путешествовал с ним по организму человека.

Начиная действовать (перехватывать управление), вирус даёт команду компьютеру, чтобы тот записал зараженную версию программы. После этого он возвращает

программе управление. Пользователь ничего не заметит, т. к. 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».

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 злоумышленников созданы специальные отряды английских детективов.

По оценке специалистов, в «обращении» находится более 100 типов вирусов.

Но все их можно разделить на две разновидности, обнаружение которых различно по сложности: «вульгарный вирус» и «раздробленный вирус». Программа «вульгарный вирус» написана одним блоком, и при возникновении подозрений в заражении ЭВМ эксперты могут обнаружить его 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, воссоздать и, следовательно, размножить вирус. Таким образом, он почти всё время находится в «распределённом» состоянии, лишь на короткое время своей работы собираясь в единое целое. Как правило, создатели вирусов указывают ему число репродукций, после достижения которого он становиться агрессивным.

Вирусы могут быть внедрены в операционную систему, прикладную программу или в сетевой драйвер.

Варианты вирусов зависят от целей, преследуемых их создателями. Признаки их могут быть относительно доброкачественными, например, замедление в выполнении программ или появление светящейся точки на экране дисплея (как например «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 объём программных файлов. Наконец, эти проявления могут быть катастрофическими и привести к стиранию файлов и уничтожению программного обеспечения.

По-видимому, в будущем будут появляться принципиально новые виды вирусов. Например, можно себе представить (пока подобных сообщений не было) своего рода «троянского коня» вирусного типа в электронных цепях. В самом деле, пока речь идёт только о заражении компьютеров. А почему бы – не микросхем? Ведь они становятся всё более мощными и превращаются в подобие ЭВМ. И их 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». Т. е. с начала заражения имеется опасность, что ЭВМ может создать большое число средств передвижения и в последующие часы вся совокупность файлов и программных средств окажется заражённой. 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. Удобным 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 копирование программ, что является обычной практикой у пользователей персональных ЭВМ. Так, скопированными оказываются и заражённые программы.

Специалисты предостерегают от копирования ворованных программ. Иногда, однако, и официально поставляемые программы могут быть источником заражения.

В печати часто проводится параллель между компьютерным вирусом и вирусом “AIDS”. Только упорядоченная жизнь с одним или несколькими партнёрами способна уберечь от этого вируса. Беспорядочные связи со многими компьютерами почти наверняка приводят к заражения.

Естественно, что против вирусов были приняты чрезвычайные меры, приведшие к созданию текстовых программ – антивирусов. Защитные программы подразделяются на три вида: ***ФИЛЬТРУЮЩИЕ*** (препятствующие проникновению вируса), ***ПРОТИВОИНФЕКЦИОННЫЕ*** (постоянно контролирующие процессы в системе) и ***ПРОТИВОВИРУСНЫЕ*** (настроенные на выявление отдельных вирусов). Однако развитие этих программ пока не успевает за развитием компьютерной эпидемии.

4. Преступная небрежность в разработке, изготовлении и эксплуатации программно-вычислительных комплексов, приведшая к тяжким последствиям (статья 274 УК РФ "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети")

Проблема неосторожности в области компьютерной техники сродни 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 надёжности, то в области программирования такая надёжность весьма условна, а в ряде случаев почти недостижима.

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит в несоблюдении правил режима их работы, предусмотренных инструкциями, исходящими из их технических характеристик, правил внутреннего распорядка, а также правил обращения с компьютерной информацией, установленных собственником или владельцем информации либо законом или иным нормативным актом.

Статья 274 распространяется на охраняемую законом информацию. Под охраняемой законом информацией следует понимать информацию, изъятую из публичного (открытого) оборота на основании закона, других нормативных (включая ведомственные) 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.

Для наступления ответственности по статье 274 УК РФ необходимо установить, что упомянутое нарушение правил эксплуатации повлекло уничтожение, блокирование или модификацию охраняемой законом информации при условии причинения существенного ущерба.

Что касается существенности ущерба, причинённого нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, то это оценочное понятие, которое зависит в каждом конкретном случае от многих показателей, относящихся к применяемым техническим средствам (ЭВМ и др.), к содержанию информации, степени повреждения и многим другим показателям, которые должны оцениваться следователем и судом. В всяком случае существенный вред

должен быть менее значительным, чем причинение тяжких последствий, о которых говорится в части 2 данной статьи.

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

Субъект преступления специальный - лицо, имеющее доступ к эксплуатации упомянутых технических средств. Это могут быть программисты, операторы ЭВМ, техники-наладчики, другие лица, по работе имеющие к ним доступ.

5. Подделка компьютерной информации

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

Идея преступления состоит в подделке выходной информации компьютеров с целью имитации работоспособности больших систем, составной частью которых является компьютер. При достаточно ловко выполненной подделке зачастую удаётся сдать заказчику заведомо неисправную продукцию.

К подделке информации можно отнести также подтасовку результатов выборов, голосования, 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.

6. Хищение компьютерной информации (статья 272)

Не очень далеко от истины шутка, что у нас программное обеспечение распространяется только путём краж и обмена краденным.

Теперь собственность на информацию закреплена в законодательном порядке. Машинная информация выделена как самостоятельный предмет уголовно-правовой охраны. На мой взгляд, последствия этого не замедлят сказаться. В пункте 1, среди других последствий неправомерного доступа к компьютерной информации, мною было рассмотрено её хищение путём копирования.

Рассмотрим теперь вторую категорию преступлений, в которых компьютер является "средством" достижения цели. Здесь 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".

В простейшем случае требуется открыть в двух банках по небольшому счёту. Далее деньги переводят 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 всё выше и выше) до тех пор, пока на счёте не оказывается приличная сумма (фактически она постоянно "перескакивает" с одного счёта на другой, увеличивая свои размеры). Тогда деньги быстро снимаются, а владелец счёта

исчезает. Этот способ требует очень точного расчёта, 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 компьютера.

Можно представить себе создание специализированного компьютера-шпиона, который будучи подключен к разведуемой сети, генерирует всевозможные запросы, фиксирует и анализирует полученные ответы. Поставить преграду перед таким хакером практически невозможно. Не трудно предположить, что организованная преступность давно приняла на вооружение вычислительную технику.

§2 Предупреждение компьютерных преступлений

При разработке компьютерных систем, выход из строя или ошибки в работе которых могут привести к тяжелым последствиям, вопросы компьютерной безопасности становятся первоочередными. Известно много мер, направленных на предупреждение преступления. Выделим из них 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, установку оборудования и тушения пожара, оборудование для обнаружения воды, принятия конструкционных мер защиты от хищений, саботажа, диверсий, оснащение помещений замками, установку сигнализации и многое другое.

К организационным мерам отнесем охрану 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 и создание норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и

гражданского законодательства, а также судопроизводство. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие международных договоров об их ограничениях, если они влияют, или могут повлиять на военные, экономические и социальные аспекты жизни стран, заключающих соглашения.

Защита от стихийных бедствий

Основной и наиболее распространенный метод защиты информации и оборудования от различных стихийных бедствий (пожаров, землетрясений наводнений и т.п.) – 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 в другом районе города (другом городе).

§3 Защита данных в компьютерных сетях

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 ПО:
   - -потеря или изменение данных при ошибках ПО;
   - -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 обеспечения

В зависимости от возможных видов нарушений работы сети (под нарушениями работы я также понимаю и

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.
- -программные средства защиты, в том числе: антивирусные программы, системы разграничения полномочий, программные средства контроля доступа.
- -административные методы защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и др.

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 др.,

Концентрация информации в компьютерах – аналогично концентрации наличных денег в банках – заставляет все более усиливать контроль в целях защиты информации. Юридические вопросы, частная тайна, национальная безопасность – все эти соображения требуют усиления внутреннего контроля в коммерческих и правительственных организациях. Работы 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.

Сложность создания системы защиты информации определяется тем, что данные могут быть похищены из компьютера и одновременно оставаться на месте; целостность 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 появления нарушений работы, ущерб от коммерческих потерь, снижение коэффициента системы, общественные отношения, юридические проблемы) и представить 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 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, некоторые наиболее солидные компании начинают использовать возможности, предоставляемые шифрованием для обеспечения конфиденциальности информации.

Финансовые службы компаний (прежде всего в США) 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

Шифрование данных может осуществляться в режимах On-line (в темпе поступления информации) и Off-line (автономно). Остановимся подробнее на первом типе, представляющем большой интерес. Наиболее распространены два алгоритма:

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 бит проверки на четность и требует от злоумышленника перебора 72 квадриллионов возможных ключевых комбинаций, обеспечивая высокую степень защиты при небольших расходах. При частой смене ключей алгоритм

утвердительно решает проблему превращения конфиденциальной информации в недоступную.

Алгоритм RSA был изобретен Ривестом, Шамиром и Альдерманом 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,** т.е. он использует разные ключи при шифровании и дешифровании. Пользователи имеют два ключа и могут широко распространять свой открытый ключ. Открытый ключ используется для шифрования 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 процесс шифрования и де шифрования). 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.

§4 Физическая защита данных

1. Кабельная система

Кабельная система остается главной "ахиллесовой пятой " большинства локальных вычислительных сетей: по данным различных исследований именно кабельная система является причиной более чем половины всех отказов сети. В связи с этим кабельной системе должно уделяться особое внимание с самого момента проектирования сети.

Наилучшим способом избавить себя от "головной боли" по поводу неисправностей прокладки кабеля является использование получивших широкое распространение в последнее время так называемых структурированных кабельных систем, использующих одинаковые кабели для передачи данных в локальной вычислительной сети, локальной телефонной сети, передачи видеоинформации или сигналов от датчиков пожарной безопасности или охраны систем. К структурированным кабельным системам относятся, например, SYSTIMAX SCS фирмы AT&T, OPEN DECconnect компании DIGITAL, кабельная система корпорации IBM.

Понятие “структурированность” означает, что кабельную систему здания можно разделить на несколько уровней в зависимости от назначения и местоположения компонентов кабельной системы. Например кабельная система SYSTIMAX SCS состоит из:

- -внешней подсистемы (campus subsystem);
- -аппаратных (equipment room);
- -административной подсистемы (administrative subsystem);
- -магистрали (backbone cabling);
- -горизонтальной подсистемы (Horizontal subsystem);
- -рабочих мест (work location subsystem);

Внешняя подсистема состоит из медного оптоволоконного кабеля, устройств электрической защиты и заземления и связывает коммуникационную и обрабатывающую аппаратуру в здании (или комплексе зданий). Кроме того, в эту подсистему входят и устройства сопряжения внешних кабельных линий с внутренними.

Аппаратные служат для размещения различного коммуникационного оборудования, предназначенного для обеспечения работы административной подсистемы.

Административная подсистема предназначена для быстрого и легкого управления кабельной системы SYSTIMAX SCS при изменении планов размещения персонала и отделов. В ее состав входят кабельная система (неэкранированная витая пара и оптоволокно), устройства коммутации и сопряжения магистрали и горизонтальной подсистемы, соединительные шнуры, маркировочные средства и т.д.

Магистраль состоит из медного кабеля или комбинации медного и оптоволоконного кабеля и вспомогательного оборудования. Она связывает между собой этажи здания или большие площади одного и того же этажа.

Горизонтальная система на базе второго медного кабеля расширяет магистраль от входных точек административной системы этажа к розеткам на рабочем месте.

И, наконец, оборудование рабочих мест включает в себя соединительные шнуры, адаптеры, устройства сопряжения и обеспечивает механическое и электрическое соединение между оборудованием рабочего места и горизонтальной кабельной подсистемы.

Наилучшим способом защиты кабеля от физических (а иногда температурных и химических воздействий, например в производственных цехах) является прокладка кабелей с использованием в различной степени защищенных коробов. При прокладке сетевого кабеля

вблизи источников электромагнитного излучения необходимо выполнять следующие требования:

1) Неэкранированная витая пара должна стоять минимум на 15-30 см от электрического кабеля, розеток, трансформаторов и т.д.

2) Требования к коаксиальному кабелю менее жесткие – расстояние до электрической линии или электроприборов должно быть не менее 10-15 см.

Другая важная проблема правильной инсталляции и безотказной работы кабельной системы – соответствие всех ее компонентов требованиям международных стандартов.

Наибольшее распространение в настоящее время получили следующие стандарты кабельных систем:

Спецификации корпорации IBM, которые предусматривают девять различных типов кабелей. Наиболее распространенный среди них является кабель IBM type 1 – экранированная витая пара (STP) для сетей Token Ring.

Система категорий Underwriters Labs (UL), представлена этой лабораторией совместно с корпорацией ANIXTER. Система включает 5 уровней кабелей. В настоящее время система UL приведена в соответствии с системой категорий EIA/TIA.

Стандарт EIA/TIA 568 был разработан совместными усилиями UL, American National Standards Institute (ANSI), Electronic Industry Association, Telecommunications Industry Association, под группой TR 41.8.1 для кабельных систем в витой паре (UTR)

В дополнение к стандарту EIA/TIA 568 существует документ DIS 11801 разработанный International Standard Organization (ISO) и International Electrotechnical Commission (IEC). Данный стандарт использует термин «категория» для отдельных кабелей и термин «класс» для кабельных систем.

Необходимо также отметить, что требования стандарта EIA/TIA 568 относятся только к сетевому кабелю. Но реальные системы, помимо кабеля, включают также соединительные разъемы, розетки, распределительные панели и другие элементы. Использование только кабеля категории 5 не гарантирует создание кабельной системы этой категории. В связи с этим все вышеперечисленное оборудование должно быть также сертифицировано на соответствие данной категории кабельной системы.

2. Системы электроснабжения

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии является установка источников бесперебойного питания, Различные по своим технологическим и потребительским характеристикам, подобные устройства могут обеспечить питание по всей локальной сети или отдельных компьютеров в течение промежутка времени, достаточного для восстановления подачи напряжения или для сохранения информации на магнитные носители. Большинство источников бесперебойного питания одновременно выполняет функцию и стабилизатора напряжения, что является дополнительной защитой от скачков напряжения в сети. Многие современные сетевые устройства – серверы, концентраторы, мосты и др. – оснащены собственными дублированными системами электропитания.

За рубежом корпорации имеют собственные аварийные электрогенераторы или резервные линии электропитания. Эти линии подключены к разным подстанциям, и при выходе из строя одной из них, электроснабжение осуществляется с резервной подстанции.

3. Системы архивирования и дублирования информации

Организация надежной и эффективной системы архивации данных является одной из важнейших задач по обеспечению сохранности информации в сети. В небольших сетях, где установлены один-два сервера, чаще

всего применяется установка системы архивации непосредственно в свободные слоты серверов. В крупных корпоративных сетях наиболее предпочтительно организовать выделенный специализированный архивационный сервер.

Хранение архивной информации, представляющей особую ценность, должно быть организовано в специальном охраняемом помещении. Специалисты рекомендуют хранить дубликаты архивов наиболее ценных данных в другом здании, на случай пожара или стихийного бедствия.

§5 Программные и программно-аппаратные методы защиты

1. Защита от компьютерных вирусов

Вряд ли найдётся хотя бы один пользователь или администратор сети, который бы ни разу не сталкивался с компьютерными вирусами. По данным исследования, проведённого фирмой Creative Strategies Research, 64% из 451 опрошенного специалиста испытали "на себе" действие вирусов. На сегодняшний день дополнительно к тысячам уже известных вирусов появляется 100-150 новых штампов ежемесячно. Наиболее распространёнными методами защиты от вирусов по сей день остаются антивирусные программы.

Однако в качестве перспективного подхода к защите от компьютерных вирусов в последние годы всё 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 перспективную технологию защиты от вирусов в компьютерных сетях. Flash - память сетевых адаптеров Intel EtherExpress Pro/10 содержит антивирусную программу, сканирующую все системы компьютера ещё до его разгрузки.

2. Защита от несанкционированного доступа

Проблема защиты информации от 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 элементы. 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 используют встроенные средства сетевых операционных систем. Так, крупнейший производитель сетевых ОС - корпорация Novell - в своём 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 тоже время в такой системе организации защиты всё равно остаётся слабое место: уровень доступа и возможность входа в систему определяются 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 глаз или отпечатков пальцев, размерами 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 несанкционированного доступа. В этом случае для доступа к компьютеру 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 надёжнее применения паролей, поскольку, если пароль подглядели, пользователь об этом может не узнать, 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 запроса доступа к ресурсам, использования запрещённых утилит, программ, команд DOS.

Одним из удачных примеров создания комплексного решения для контроля доступа 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 ключ. Пакет, содержащий "пропуск", передаётся также в зашифрованном по алгоритму DAS виде. После получения и расшифровки "пропуска" сервер выдачи разрешений проверяет запрос и сравнивает ключи и затем даёт "добро" на использование сетевой аппаратуры и программ.

Среди других подобных комплексных систем 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.

3. Защита информации при удалённом доступе

По мере расширения деятельности предприятий, роста численности персонала и появления новых филиалов, возникает необходимость доступа удалённых 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 удалённый доступ к компьютерным сетям, составит 25 млн. человек. Чаще всего для организации удалённого доступа используются кабельные линии (обычные телефонные или выделенные) и радиоканалы. В связи с этим защита информации, передаваемой по каналам удалённого доступа, требует особого подхода.

В частности, в мостах и маршрутизаторах удалённого доступа применяется сегментация пакетов - их разделение и передача параллельно по двум линиям - что делает невозможным "перехват" данных при незаконном подключении "хакера" к одной из линий. К тому же используемая при передаче данных процедура сжатия передаваемых пакетов гарантирует невозможность расшифровки "перехваченных" данных. Кроме того, мосты

и маршрутизаторы удалённого доступа могут быть запрограммированы таким образом, что удалённые пользователи будут ограничены в доступе к отдельным ресурсам сети главного офиса.

Разработаны и специальные устройства контроля доступа к компьютерным сетям по коммутируемым линиям. Например, фирмой AT&T предлагается модуль Remote Port Security Device (RPSD), представляющий собой 2 блока размером с обычный модем: RPSD Lock (замок), устанавливаемый в центральном офисе, и RPSD Key (ключ), подключаемый к модему удалённого 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 радиосетей перед необходимостью защиты информации от "хакеров", вооружённых разнообразными сканирующими устройствами. Были применены разнообразные технические решения. Например, в радиостанции 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 используется в радиосетях и технология шифрования данных при помощи алгоритмов DES и RSA.

Заключение

Итак, в работе освещены и исследованы возможные способы компьютерных преступлений, а также выявлены методы защиты от них.

Проследив это в работе, я сделала вывод о том, что все компьютерные преступления условно можно подразделить на две большие категории - преступления, связанные с вмешательством в работу компьютеров, и преступления, использующие компьютеры как необходимые технические средства. В российском уголовном законодательстве уголовно-правовая защита компьютерной информации введена впервые. Уголовный кодекс РФ, введённый в действие с 1 января 1997 года, содержит главу №28 "Преступления в сфере компьютерной информации".

Хакеры, "электронные корсары", "компьютерные пираты" - так называют людей, осуществляющих несанкционированный доступ в чужие информационные сети. Сомнения в необходимости существования уголовно-правовой защиты компьютерной информации нет. Уголовный закон достаточно строго преследует за совершение компьютерных преступлений. Это связано с высокой степенью общественной опасности.

Так же хотелось бы подчеркнуть, что абсолютную надёжность и безопасность в компьютерных сетях не смогут гарантировать никакие аппаратные, программные и любые другие решения. В то же время свести риск потерь возможно лишь при комплексном подходе к вопросам безопасности.

Литература

1. Уголовный кодекс РФ.
2. Комментарий к УК РФ.
3. М.Рааб (M.Raab) Защита сетей: наконец-то в центре внимания \\ Компьютеруолд Москва, 1994, №29.
4. С.В.Сухова. Система безопасности Net Ware \\ "Сети", 1995, №4.
5. Д.Векслер (J/Wexler) Наконец-то надёжно обеспечена защита данных в радиосетях \\ Компьютеруолд, М., 1994 г., №17.
6. В.Беляев. Безопасность в распределительных системах \\ Открытые систмы, М., 1995 г., №3.
7. Д.Ведеев. Защита данных в компьютерных сетях \\ Открытые системы, М., 1995 г., №3.
8. Федеральный закон от 20 февраля 1995 года "Об информации, информатизации и защите информации".
9. Ведомости РФ, 1992 г., №42
10. Новое уголовное право России. Особенная часть. М., 1996 г.
11. Батурин Ю.М., Жодзишкий А.М. Кмпьютерная преступность и компьютерная безопасность, М., 1991 г.
12. Китов И. Компьютерные вирусы. \\ Монитор №28(42) 21-27 мая 1997 г.