РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

(КАФЕДРА УГОЛОВНОГО ПРАВА И ПРОЦЕССА)

Написал:

студент юридического факультета

группы юю-208

Константинопольский Василий

Принял: старший преподаватель

А.К. Манна

МОСКВА 2000

**Оглавление**

1. Введение

2. Общая характеристика преступлений в сфере компьютерной информации.

*2.1 Неправомерный доступ к компьютерной информации*

*2.2 Создание, использование и*

*распространение вредоносных программ для ЭВМ*

*2.3 Нарушение правил эксплуатации ЭВМ, системы ЭВМ*

*или их сети*

3. КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА И ФАКТОР, ОПРЕДЕЛЯЮЩИЙ ОСОБЕННОСТИ ЛИЧНОСТИ КОМПЬЮТЕРНОГО ПРЕСТУПНИКА

*3.1 Несанкционированный доступ к информации, хранящейся в компьюте­ре.*

*3.2 Хищение компьютерной информации.*

*3.3 Разработка и распространение компьютерных вирусов.*

##### *3.4 Уничтожение компьютерной информации*

*3.5 Подделка компьютерной информации.*

## 4. Способы совершения компьютерных

## преступлений

## 5. Предупреждение компьютерных преступлений

6. Международный и отечественный опыт

борьбы и предупреждения компьютерных

преступлений и вновь возникающие

проблемы.

7. Доказательство в судебных делах по

компьютерным преступлениям

8. Заключение

"По-настоящему безопасной можно считать лишь систему, которая выключена, замурована в бетонный корпус, заперта в помещении со свинцовыми стенами и охраняется вооруженным караулом, - но и в этом случае сомнения не оставляют меня".

#### Юджин Х. Спаффорд эксперт по информационной безопасности

**Введение**

Изменения происходящие в экономической жизни России – создание финансово-кредитной системы; предприятий различных форм собственности – 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.

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.

В наше время, когда наступает эпоха интернета и компьютерных технологий, компьютерная преступность стала реальностью общественной жизни.

Негативные тенденции в значительной степени обусловлены бурным процессом развития научно-технической революции (НТР). Эта революция повлекла за собой появление нового вида общественных отношений и ресурсов – информационных. Существует целый ряд особенностей, которые отличают информационные ресурсы от других видов ресурсов:

они непотребляемы и подвержены не физическому, а моральному износу

они по своей сути нематериальны и несводимы к физическому носителю, в котором воплощены

их использование позволяет резко сократить потребление остальных видов ресурсов, что в конечном итоге приводит к колоссальной экономии средств

процесс их создания и использования осуществляется с помощью компьютерной техники

Информация становится продуктом общественных отношений, начинает приобретать товарные черты и становится предметом купли-продажи. Следствием информационных процессов является возникновение и формирование новых общественных отношений и изменение уже существующих. Сейчас можно зафиксировать большой объем договорных отношений, связанных с изготовлением, передачей, накоплением и использованием информации в различных ее формах. Такого рода общественные отношения закреплены в Федеральном Законе «Об информации, информатизации и защите информации», вступившем в действие с января 1995 года. В соответствии со статьей 2 которого:

под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления

документированной информацией (документом) признается зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать

информационным процессом считается процесс сбора, обработки, накопления, хранения, поиска и распространения информации

информационным ресурсом являются отдельные документы и отдельные массивы документов в информационных системах

под информационной системой понимается упорядоченная совокупность документов и информационных технологий.

В пункте 6 статьи 6 данного закона информация и информационные ресурсы признаются товаром со всеми вытекающими отсюда последствиями.

В связи с этим новые информационные технологии дали толчок не только в плане прогресса общества, но и стимулировали возникновение и развитие новых форм преступности. Революция в области компьютерной техники предоставила преступникам широкие возможности в плане доступа к новым техническим средствам. В современных российских условиях преступные элементы не испытывают недостатка в кадрах, способных эффективно использовать новейшие электронные средства, технологические новшества, свои профессиональные знания и умения для подготовки, совершения, маскировки преступлений и активного противодействия работе правоохранительных органов. Этими профессиональными кадрами являются сокращенные высококвалифицированные специалисты, обслуживавшие структуры военно-промышленного комплекса, различные научно-исследовательские центры, лаборатории и институты, а также реорганизованного в недавнем прошлом КГБ. Рост безработицы сразу же повлиял на изменение криминогенной ситуации в России.

Отсутствие четкого определения компьютерной преступности, единого понимания сущности этого явления значительно затрудняют определение задач правоприменительных органов в выработке единой стратегии борьбы с ней.

До недавнего времени считалось, что компьютерная преступность существует только в зарубежных капиталистических странах, а в России, по причине слабой компьютеризации, отсутствует вообще. На мой взгляд, именно это обстоятельство и привело к недостаточному изучению этой проблемы. Само появление компьютерной преступности в нашей стране приводит к выводу о том, что это явление свойственно всем государствам, которые в силу своего научного прогресса вступают в период широкой компьютеризации своей деятельности.

Впервые о проблемах борьбы с компьютерной преступностью в России отечественная криминалистическая наука официально заявила в июле 1992 года с момента создания межведомственного семинара «Криминалистика и компьютерная преступность». Он организован научно-исследовательским институтом проблем укрепления законности и правопорядка Генеральной прокуратуры Российской Федерации и Экспертно-криминалистическим центром МВД России. В течение последних 15-20 лет по мере компьютеризации хозяйственно-управленческой и финансово-коммерческой деятельности появились новые виды преступлений, которые стали называться компьютерными, исходя из терминологии зарубежной юридической практики. Первое преступление подобного типа в бывшем СССР было зарегистрировано в 1979 году в городе Вильнюсе. Тогда ущерб государству составил около 80 тысяч рублей. Этот случай явился определенной отправной точкой в развитии и исследовании нового вида преступлений в нашей стране.

В настоящее время все больше применяется межбанковская система электронных платежей, которая не может быть абсолютно надежной. Этим пользуются преступные элементы, которые получают несанкционированный доступ к банковским компьютерным сетям для совершения противоправных действий. Можно сказать, что процесс компьютеризации общества приводит к увеличению количества компьютерных преступлений. Причем материальные потери от этого вида преступлений постоянно возрастают. Между тем в отечественной криминалистике не существует четкого определения понятия компьютерного преступления. Некоторые считают, что правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в особую группу преступлений. Существуют и другие точки зрения по этому вопросу, но я бы выделил одно определение. Его придерживается А.Н. Караханьян. Под компьютерными преступлениями он понимает противозаконные действия, объектом или орудием совершения которых являются электронно-вычислительные машины.

В настоящее время существуют два основных течения научной мысли. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательств. В этом случае кража компьютера тоже является компьютерным преступлением. Другая часть исследователей утверждает, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства. Надо сказать, что законодательство многих стран, в том числе и в России, стало развиваться именно по этому пути.

В главе 28 Уголовного кодекса Российской Федерации определяются следующие общественно опасные деяния в отношении средств компьютерной техники:

* Неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.
* Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.
* Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ.

С криминалистической точки зрения, по моему мнению, компьютерное преступление следует понимать в широком смысле этого слова. Так, в марте 1993 года на заседании постоянно действующего межведомственного семинара «Криминалистика и компьютерная преступность» была сделана попытка дать первое отечественное определение понятия «компьютерное преступление». Согласно этому определению, под компьютерным преступлением следует понимать **«… предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства»**.

Подводя итоги, можно выделить следующие характерные особенности этого социального явления:

1. Неоднородность объекта посягательства
2. Выступление машинной информации, как в качестве объекта, так и в качестве средства преступления
3. Многообразие предметов и средств преступного посягательства
4. Выступление компьютера либо в качестве предмета, либо в качестве средства совершения преступления.

На основе этих особенностей можно сделать вывод, что компьютерное преступление – это предусмотренное уголовным законом общественно опасное действие, совершенное с использованием средств электронно-вычислительной (компьютерной) техники. Первая часть определения, по моему мнению, не нуждается в дополнительных пояснениях. Вторая же часть требует детализации.

Средства компьютерной техники можно разделить на 2 группы:

1. Аппаратные средства
2. Программные средства

***Аппаратные средства*** – это технические средства, используемые для обработки данных. Сюда относятся: Персональный компьютер (комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач).

Периферийное оборудование (комплекс внешних устройств ЭВМ, не находящихся под непосредственным управлением центрального процессора).

Физические носители машинной информации.

***Программные средства*** – это объективные формы представления совокупности данных и команд, предназначенных для функционирования компьютеров и компьютерных устройств с целью получения определенного результата, а также подготовленные и зафиксированные на физическом носителе материалы, полученные в ходе их разработок, и порождаемые ими аудиовизуальные отображения. К ним относятся:

Программное обеспечение (совокупность управляющих и обрабатывающих программ). Состав:

1. Системные программы (операционные системы, программы технического обслуживания)
2. Прикладные программы (программы, которые предназначены для решения задач определенного типа, например редакторы текстов, антивирусные программы, СУБД и т.п.)
3. Инструментальные программы (системы программирования, состоящие из языков программирования: Turbo C, Microsoft Basic и т.д. и трансляторов – комплекса программ, обеспечивающих автоматический перевод с алгоритмических и символических языков в машинные коды)
4. Машинная информация владельца, собственника, пользователя.

Подобную детализацию я провожу, чтобы потом более четко понять суть рассматриваемого вопроса, чтобы более четко выделить способы совершения компьютерных преступлений, предметов и орудий преступного посягательства, а также для устранения разногласий по поводу терминологии средств компьютерной техники. После детального рассмотрения основных компонентов, представляющих в совокупности содержание понятия компьютерного преступления, можно перейти к рассмотрению вопросов, касающихся основных элементов криминалистической характеристики компьютерных преступлений.

**Общая характеристика преступлений в сфере компьютерной информации.**

Развитие современного общества, основанного на использовании огромного количества самой разнообразной информации, немыслимо без широкого внедрения во все сферы жизни общества электронно-вычислительной техники. Она служит не только для хранения и обработки соответствующей информации на уровне отдельных управленческих или хозяйственных единиц или использования как средства связи между гражданами, но и широко внедряется в целях обеспечения внутренней и внешней безопасности государства.

Но развертывание научно-технической революции обусловливает не только коренные прогрессивные изменения в составе факторов экономического развития России, но и негативные тенденции развития преступного мира, приводит к появлению новых форм и видов преступных посягательств. Это ярко проявляется в том, что преступные группы и сообщества начинают активно использовать в своей деятельности новейшие достижения науки и техники.

Особую тревогу в этом плане вызывает факт появления и развития в России нового вида преступных посягательств, ранее неизвестных отечественной юридической науке и практике и связанный с использованием средств компьютерной техники и информационно-обрабатывающих технологий компьютерных преступлений. Последние потребовали от российского законодателя принятия срочных адекватных правовых мер противодействия этому новому виду преступности.

Первыми шагами в этом направлении были: принятие Закона РФ “О правовой охране программ для ЭВМ и баз данных“ от 23.09.1992; Федерального закона “Об информации, информатизации и защите информации“ от 20.02.1995; включение в новый Уголовный кодекс специальной главы 28 “Преступления в сфере компьютерной информации”.

Преступления, содержащиеся в этой главе, представляют собой деяния, сущность которых заключается отнюдь не в использовании самой по себе электронно-вычислительной техники в качестве средства для совершения преступлений. Эта глава включает общественно-опасные деяния, посягающие на безопасность информации и систем обработки информации с использованием ЭВМ.

Последствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т. д. Поэтому совершенно оправданно то, что преступления данного вида помещены в раздел IX “ Преступления против общественной безопасности и общественного порядка “.

Таким образом, если исходить из учения о четырехзвенной структуре объекта преступления, общим объектом компьютерных преступлений будет совокупность всех общественных отношений, охраняемых уголовным законом, родовым - общественная безопасность и общий порядок; видовым - совокупность общественных отношений по правомерному и безопасному использованию информации; непосредственный объект трактуется исходя из названий и диспозиций конкретных статей.

Компьютерные преступления, посягая на основной объект, всегда посягают и на дополнительный объект, поскольку поражаются блага конкретного свойства: личные права и неприкосновенность частной сферы, имущественные права и интересы, общественную и государственную безопасность, конституционный строй. Эти подлежащие правовой охране интересы личности, общества и государства являются дополнительным объектом посягательства компьютерных преступлений. Отсутствие посягательства на эти общественные отношения (либо незначительность такого посягательства) исключает уголовную ответственность в силу ч. 2 ст. 14 УК РФ. Дополнительный объект, как правило, более ценный, чем объект основной. Это отражено и в названии гл. 28 УК, которое говорит не о посягательстве на объект, а о посягательствах в определенной “сфере”.

Преступлениями в сфере компьютерной информации являются:

Неправомерный доступ к компьютерной информации (ст.272 УК РФ);

Создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ);

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ);

Особенностью конструкции составов этих преступлений является то, что они сконструированы по типу материальных - предусматривают наступление общественно-опасных последствий в виде вреда для пользователей ЭВМ, который в целом состоит в нарушении нормального функционирования ЭВМ или сетей ЭВМ.

Физическое повреждение или уничтожение компьютерной техники, незаконное завладение ею, а равно машинными носителями (дискетами, CD-R дисками), как предметами, обладающими материальной ценностью, квалифицируются по статьям главы 21 УК РФ. В принципе, можно предположить случаи, когда вредоносное воздействие на ЭВМ осуществляется путем непосредственного влияния на нее информационных команд. Это возможно, когда преступнику удается ввести движущиеся части машины (диски, принтер) в резонансную частоту, увеличить яркость дисплея или его части для прожигания люминофора, зациклить работу компьютера таким образом, чтобы при использовании минимального количества его участков произошел их разогрев и выход из строя. В этих случаях квалификация содеянного должна проводиться по совокупности статей глав о преступлениях против собственности и компьютерной безопасности, поскольку страдают два объекта уголовно-правовой охраны. Равно и при использовании в качестве орудия при совершении противоправного деяния не информационной, а аппаратно-технической части (нанесение телесных повреждений принтером и т. п.), последнюю можно расценивать наряду с такими предметами как нож, пистолет, веревка и другие вещи материального мира. В целом же, гл. 28 УК РФ имеет своей целью охрану именно информационной безопасности - и только в силу этого защиту и аппаратно-технических средств, которые являются материальными носителями информационных ресурсов.

**Объективная сторона** компьютерных преступлений характеризуется как действием, так и бездействием. Действие (бездействие) сопряжено с нарушением прав и интересов по поводу пользования компьютерной информацией.

Компьютерные преступления имеют материальные составы. Действие (бездействие) должно причинить значительный вред правам и интересам личности, общества или государства (исключением является преступление с формальным составом, предусмотренное ч. 1 ст.273 УК: создание, использование и распространение вредоносных программ для ЭВМ). Преступные последствия конкретизируются в законе применительно к конкретным видам компьютерных преступлений. Между деянием и последствиями обязательно должна быть установлена причинная связь.

**Субъективная сторона** компьютерных преступлений характеризуется умышленной виной. В ч. 2 ст. 24 сказано, что деяние совершенное по неосторожности признается преступлением только тогда, когда это специально предусмотрено соответствующей статьей Особенной части УК. Неосторожная форма вины названа в Особенной части лишь применительно к квалифицированным видам компьютерных преступлений, предусмотренных в ч. 2 ст. 273 и ч.2 ст. 274 УК.

**Субъект** компьютерного преступления общий - лицо, достигшее 16 лет. В ст. 274 и в ч. 2 ст. 272 УК формулируются признаки специального субъекта: лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети.

**Преступление в сфере компьютерной информации** - это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

**Неправомерный доступ к компьютерной информации ( ст. 272 УК)**

**Непосредственным объектом** преступления является право владельца компьютерной системы на неприкосновенность содержащейся в ней информации

**Объективная сторона** данного преступления состоит в неправомерном доступе к охраняемой законом компьютерной информации, т.е. к информации на машинном носителе, в ЭВМ, системе ЭВМ или их сети, если это деяние повлекло уничтожение. Блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под информацией в данном случае понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащиеся в информационных системах. Эта информация должна быть чужой для осуществляющего неправомерный доступ лица и защищенной от произвольного копирования.

“Доступ” к охраняемой законом компьютерной информации - это приобретение и использование лицом возможности получать информацию, вводить ее либо влиять на процесс обработки информации.

“Неправомерным” следует считать такой доступ, когда лицо действует без разрешения владельца этой системы или сети или другого законного полномочия.

Обязательным признаком объективной стороны этого преступления является наступление вредных последствий для собственника или хранителя информации в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Это означает, что сам по себе просмотр информации, хранящейся в оперативной памяти компьютера или на машинном носителе (дискете, CD-R диске), состава преступления не образует.

Под уничтожением информации понимается не простое удаление файлов, а только такое, которое приведет к невозможности их восстановления.

Модификация информации - существенное ее видоизменение, совершенное без согласия собственника информации и затрудняющее законное пользование ею.

Блокирование информации - это создание препятствий к свободному ее использованию при сохранности самой информации.

Нарушение работы ЭВМ, системы ЭВМ или их сети имеет место в случае, если компьютерная система не выполняет своих функций, выполняет их не должным образом или в случае заметного уменьшения производительности системы. Между действиями и последствиями обязательно должна быть установлена причинная связь.

Вопрос о том, когда окончено данное деяние, должен решаться так - моментом его окончания является момент отсылки пользователем последней интерфейсовой команды вызова хранящейся информации, независимо от наступления дальнейших последствий. Однако преступлением это деяние станет лишь при наличии последнего условия. При ненаступлении указанных последствий, все совершенные до этого действия будут подпадать под признаки неоконченного преступления.

**Субъективная сторона** преступления характеризуется виной в форме умысла: лицо сознает, что осуществляет неправомерный (несанкционированный) доступ к охраняемой законом компьютерной информации, предвидит, что в результате производимых им действий могут наступить или неизбежно наступят указанные в законе вредные последствия, и желает (прямой умысел) или сознательно допускает (косвенный умысел) их наступления либо относится к ним безразлично.

Мотивы и цели этого преступления могут быть разными: корыстный мотив, желание получить какую-либо информацию либо желание причинить вред. Мотив и цель не являются признаками состава данного преступления и не влияют на квалификацию.

**Субъект** - лицо, достигшее 16-летнего возраста.

Квалифицирущие признаки:

совершение данного преступления группой лиц по предварительному сговору;

совершение данного преступления организованной группой;

совершение данного преступления лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Если описание первых двух признаков дано в ст. 35 УК, то специальный субъект двух последних можно трактовать как отдельных должностных лиц, программистов, операторов ЭВМ, наладчиков оборудования, специалистов-пользователей специализированных рабочих мест и т.д.

Лицом, “имеющим доступ к ЭВМ, системе ЭВМ или их сети” является как лицо, которому в силу разрешения владельца системы или служебного полномочия разрешено получать информацию в компьютерной системе, вводить ее или производить с ней операции, так и лицо, осуществляющее техническое обслуживание компьютерного оборудования и на иных законных основаниях имеющее допуск к компьютерной системе. Лицо, имеющее допуск к компьютерной системе может совершить это преступление лишь в случае доступа к информации, допуска к которой оно не имеет. В случае, когда существенный вред причиняется действиями лица имеющего правомерный доступ имеющее допуск к компьютерной информации, ответственность наступает по ст. 274 УК.

**Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК)**

**Непосредственным объектом** данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Состав ч. 1 формальный и предусматривает совершение одного из следующих действий:

Создание программ для ЭВМ, заведомо для создателя приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части.

Внесение в существующие программы изменений, обладающих аналогичными свойствами.

Использование двух названных видов программ.

Их распространение.

Использование машинных носителей с такими программами.

Распространение таких носителей.

Создание и изменение программы - это изготовление и преобразование написанного на языке ЭВМ машинного алгоритма. Использование и распространение программы - употребление ( применение ) и расширение сферы применения ее за пределы рабочего места создателя.

Последствия всех этих действий ( равно как и момент окончания деяния) аналогичны таковым для предыдущей статьи, однако в данном случае для признания деяния преступлением не обязательно их наступление.

Преступление является оконченным с момента создания программы-”вируса” либо ее использования или распространения.

Обязательными признаками **объективной стороны** ч.1 ст.273 будут два, характеризующих способ и средство совершения преступления. Это во-первых то, что последствия должны быть несанкционированными, во-вторых, наличие самой вредоносной программы либо изменения в программе.

ч.2 ст. 273 криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия. Это - преступление с материальным составом и двумя формами вины: по отношению к действиям присутствует умысел, а к общественно-опасным последствиям - неосторожность, легкомыслие или небрежность.

В случае умышленного причинения общественно-опасных последствий ответственность наступает по совокупности ч. 1 ст. 273 УК и других статей УК в зависимости от того, на наступление каких последствий был направлен умысел преступника. При совершении преступления, предусмотренного ч.2 ст. 273 УК, лицо осознает, что создает вредоносную программу, использует либо распространяет такую программу или ее носители и либо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит возможности наступления тяжких последствий, хотя при необходимой внимательности и предусмотрительности могло и должно было их предвидеть.

“Тяжкие последствия “ - оценочное понятие, наличие их в каждом конкретном случае определяется из особенностей дела. Хотя разработчики УК попытались ввести определенную упорядоченность в содержание понятий разных видов общественно-опасных последствий ( “тяжкие“ - для организационного вреда, “ущерб“ - для материального, “вред“ - для физического ), все они, конечно, не укладываются в эту схему. Так, в данном случае, под тяжкими последствиями можно понимать смерть одного или нескольких человек, причинение тяжкого вреда здоровью, катастрофы, серьёзную дезорганизацию работы, крупный материальный ущерб и т.п.

**Субъективная сторона** преступления характеризуется прямым умыслом. Лицо сознает, что создает программу-”вирус” или модифицирует, доводя до такого качества обычную программу, предвидит возможность или неизбежность наступления при ее использовании другими пользователями ЭВМ вредных последствий и желает их наступления.

Мотив и цель не являются признаками состава этого преступления и не влияют на его квалификацию.

**Субъект преступления** - лицо, достигшее 16-летнего возраста. Законодательство РФ предусматривает возможность применения в административном порядке к лицам, совершившим общественно-опасные деяния, но не достигшим возраста, с которого может наступать уголовная ответственность, принудительных мер воспитательного характера.

**Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК)**

Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации, если это деяние причинило существенный вред.

**Непосредственным объектом** этого преступления является интерес владельца компьютерной системы или сети относительно правильной эксплуатации системы или сети.

**Объективная сторона** преступления характеризуется действием или бездействием, заключающемся в нарушении правил эксплуатации компьютерной системы или сети, последствием в виде существенного вреда и причинной связью между действием и последствием (материальный состав). Фактически это выражается в несоблюдении или прямом игнорировании определенных правил, обеспечивающих безопасность компьютерной системы или сети (например непроверке вновь используемых машинных носителей на наличие “вирусных” программ).

Под “правилами эксплуатации компьютерной системы” следует понимать как правила, которые могу быть установлены компетентным государственным органом (“Общероссийские временные санитарные нормы и правила для работников вычислительных центров”), так и правила технической эксплуатации и правила работы с программами, установленные изготовителями ЭВМ и иного компьютерного оборудования, правила, установленные продавцами и разработчиками программ, а также правила, установленные владельцем компьютерной системы или по его полномочию, конкретные, принимаемые в одном учреждении ил и организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Нарушение правил эксплуатации компьютерной системы должно повлечь уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, и, кроме того, существенный вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства. “Охраняемая законом информация” определяется в ст. 272 как “информация на машинном носителе, в ЭВМ, системе ЭВМ или их сети”.

Существенный вред - оценочное понятие, однако он должен быть прямым следствием уничтожения, блокирования, или модификации охраняемой законом информации ЭВМ, произошедших по вине пользователя. При установлении признака “существенного вреда” следует учитывать законодательство и судебную практику по сходным преступлениям против общественной безопасности.

**Субъективная сторона** преступления характеризуется умышленной виной (исходя из положения, установленного ч. 2 ст. 24 УК). Виновный сознает, что нарушает правила эксплуатации, предвидит возможность или неизбежность уничтожения, блокирования или модификации охраняемой законом информации и причинения существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично. Часть 2 ст. 274 предусматривает ответственность за те же деяния, повлекшие по неосторожности тяжкие последствия. Понятие таких последствий раскрывалось при анализе ч. 2 ст. 273 УК.

**Субъект преступления** - специальный, то есть лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети (законный пользователь).

Итак, сделана первая попытка реализации уголовно-правовой политики в новой для нее области - сфере компьютерных правоотношений. Насколько она окажется успешной, как сможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц - будет зависеть от многих факторов политического, экономического, научно-технического, организационного характера. Ближайшая задача правоведов состоит теперь в том, чтобы во взаимодействии со специалистами в области программирования разработать по возможности более подробные рекомендации по применению главы 28 УК.

**КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ КАК ОБЪЕКТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА И ФАКТОР, ОПРЕДЕЛЯЮЩИЙ ОСОБЕННОСТИ ЛИЧНОСТИ КОМПЬЮТЕРНОГО ПРЕСТУПНИКА**

Этот заголовок не случаен, ведь действительно, нельзя рассматривать преступника как нечто, обособленное от всего мира, в том числе и от объекта его посягательств, ведь особенности объекта в определённой степени формируют особенности субъекта.

Итак, компьютерная информация. Как часть информации вообще, она имеет следующие основные свойства:

общедоступность, при условии отсутствия особых ограничений на доступ;

инвизуальность, т.е. отсутствие способа для человека без специальных инструментов в естественном виде наблюдать и анализировать информацию. Любая информация абстрактна вне привязки к носителю и системе визуализации;

100% идентичность копии и оригинала, т.е. одинаковая информационная ценность исходной информации и её копии на любом носителе при одинаковом конечном методе визуализации.

И эти свойства напрямую определяют то, какими качествами должен обладать преступник, посягающий на компьютерную информацию. Рассмотрим их все.

Начнём, пожалуй, со второго свойства – с инвизуальности. Средством визуализации компьютерной информации является собственно компьютер, инструмент не простой в обращении и требующий от человека, работающего с ним, определённых навыков. Соответственно, можно сделать промежуточный вывод о том, что компьютерный преступник обладает определённой совокупностью знаний и умений по части общения с компьютерами, программным обеспечением, компьютерными системами и сетями.

Теперь затронем тему общедоступности. Действительно, компьютерная информация, при условии, что индивид овладел основными навыками общения с инструментом визуализации, становится ему доступной. А так как основные навыки в общении с компьютерной техникой может в настоящее время приобрести практически каждый, то компьютерная информация является общедоступной. Но этот тип информации как никакой другой может быть выведен из разряда общедоступных путём обычных, но многократно усиленных вычислительной мощью компьютеров методов парольной зашиты, аутентичной верификации и шифрования (криптографии). При этом доступ к ней лицам, не знающим пароля, шифра или алгоритма защиты, блокируется практически намертво. Но именно «практически», что в русском языке последних лет стало синонимом слова «почти». Почти намертво. При наличии у индивида специальных знаний и навыков, представляется возможным преодоление любых защитных преград на пути к получению информации. Отсюда сам собой напрашивается ещё один вывод: компьютерный преступник обладает не просто знаниями в области компьютерных технологий, он обладает специальными, достаточно глубокими знаниями, позволяющими ему прокладывать себе путь сквозь любые защитные и оградительные механизмы. Но детально об этом чуть позже.

Последнее названное мной основное свойство компьютерной информации – полная идентичность копии и оригинала – вроде бы никаких прямых выходов на личность преступника не имеет. Но, так как копия имеет в большинстве случаев ценность, эквивалентную ценности оригинала, необходимость в завладении собственно оригиналом отпадает. Достаточно лишь любым способом сделать копию. При этом факт копирования может быть вообще никак не зафиксирован, поэтому и факт посягательства как бы отсутствует. Так и бывает в большинстве реальных случаев посягательства на компьютерную информацию. Следовательно, налицо повышенная безнаказанность подобного рода преступлений и, соответственно, преступников, их совершающих. Поэтому компьютерному преступнику практически не надо в бояться подозрений, неожиданных визитов представителей «органов» и тому подобных неприятностей. Компьютерный преступник - это человек, профессионально занимающийся своей деятельностью практически без риска быть уличённым в чём-либо незаконном. Он свободен от сонма страхов, которые преследуют воров, убийц и иных «мирских», некомпьютерных криминальных элементов.

Сложновато… Но это – «технический» портрет компьютерного преступника, отвлечённый от конкретной личности. Он – как вступление. Компьютерная преступность – явление настолько новое в жизни человечества, что говорить что-либо конкретное просто невозможно – не накопилось ещё достаточно информации и практического опыта. Но этот «портрет» вполне может стать ориентиром в борьбе с компьютерной преступностью, он позволяет выделить основные черты, присущие личности компьютерного преступника независимо от того, кто его родители, в какой социальной среде он вырос, сколько ему лет или был ли он ранее судим за иные преступления. И это только начало …

**НЕМНОГО О ЛИЧНОСТНЫХ ОСОБЕННОСТЯХ КОМПЬЮТЕРНЫХ ПРЕСТУПНИКОВ …**

Общий портрет – это, конечно, хорошо, иногда даже полезно – хоть какая-то информация. Но – он расплывчатый. И в очень широких пределах. Обычно же, требуется нечто более конкретное и не настолько общее. Да, это уже не универсальный портрет, это «репродукция с корректировками», с поправками на время, место и социально-политическую ситуацию. Особенности, так сказать, «национального» компьютерного преступника. Для России эти «корректировки» наиболее актуальны, так уж повелось, что у нас всё нуждается в корректировке соответственно российскому менталитету. И это не просто «рассуждения для заполнения пустого места в курсовой работе» (почему – станет ясно чуть позднее).

Начнём с того, что и у обывателей, и у работников следственных органов давно сложился яркий такой стереотип компьютерного преступника «made in USSR». Это выросший в семье среднестатистического советского инженера юнец лет 18-ти – 20-ти отроду, с тёмными, длинными, чуть косматыми волосами, в очках, молчаливый, замкнутый, рассеянный, с блуждающим взглядом, помешанный на компьютерах, днями и ночами просиживающий за своей «адской машиной», напрочь игнорирующий события в окружающем мире и девочек. Нельзя сказать, что данный стереотип не имеет права на существование и ни в чём с оригиналом не схож. Самое интересное, что, как показывает статистика и независимые исследования, проведённые, как ни странно, российскими специалистами (и не-специалистами), 20 из 100 «обитателей» преступного мира с «компьютерным уклоном» являют собой стопроцентно «чистых» стереотипных компьютерных преступников. Но только 20 из 100. Остальные 80 в это стереотип не вписываются либо вообще (самый интересный и, кстати, опасный случай), либо частично (это, в основном, промежуточная стадия между стереотипом и его крайней противоположностью).

Стереотипы, как известно, не рождаются на пустом месте. И действительно, в России, так уж исторически сложилось, самое большое число инженеров на душу населения. И, также является бесспорным тот факт, что особым достатком семьи инженеров не отличаются (очевидно, вследствие высокой конкуренции …). Но, как показывает статистика, преемственность в семьях инженеров очень высока (по ряду регионов она достигает 60%, то есть 6 детей из 10 в семьях инженеров идут по стопам родителей). Это можно объяснить семейным духом, высоким уровнем технического образования в российских ВУЗах, и, возможно, чем-то ещё, но я предпочитаю несколько иное объяснение –

а) чисто человеческая лень и надежда на «предков» со стороны подрастающего поколения (пойду в матВУЗ – папа с мамой в учёбе подсобят…)

б) родительская надежда на то, что титанический труд инженеров наконец-то оценят, пусть и не в них самих, а в детях (она же – надежда на справедливость – историческую, социальную, экономическую – если такая бывает …). При этом, наследственность в этих семьях, не смотря на известную фразу «на детях гениев природа отдыхает», я бы даже сказал усиленная. Не вдаваясь в биологические детали, скажу лишь, что в отличие от детей музыкантов, дети инженеров в 6 (против 3) случаях из 10 добиваются в жизни больших успехов, чем родители, сохраняя профессиональную принадлежность. О чём это говорит? О том, что дети в семьях инженеров имеют сильную предрасположенность к различным техническим увлечениям. И в наибольшей степени это относится к «лицам мужского пола». Так уж повелось, в силу строения мозга этих самых «лиц». А что сейчас самое передовое, самое интересное в мире техники? Правильно, автомобили и компьютеры. В соотношении где-то 40 на 60. К тому же «сила притяжения» технологии очень велика и к «армии молодых технарей» присоединяются и просто заинтересовавшиеся в компьютерах, родившиеся не в семьях инженеров люди. В результате, в силу стратификации уже внутри слоя людей, приобщившихся к компьютерным технологиям, мы получаем около 20% «ботаников», т.е. «законченных» технарей, действительно помешанных на компьютерах и электронике, и ничего, кроме этого, не воспринимающих, 40% - «средний класс» и 20% - «белые воротнички», снимающие сливки со всего компьютерного и электронного бизнеса. Остальные потихоньку «рассеиваются».

И «всплывают» личности стереотипические (те самые «ботаники») и личности неординарные, в стереотип не вписывающиеся («белые воротнички»). С первыми всё вроде бы понятно – их воспитала социальная среда, в некоторой степени стремление к технике в них заложено генетически. А вот вторая группа – воспитанники среды экономико-политической. Они вовремя осознали свои возможности в конкретный момент времени и в потенциале, определили «рыночную» цену своих знаний, сделали из увлечения карьеру. Их знания в большинстве случаев обширнее и систематизированнее, а следственно и ценнее, чем у самых «загруженных ботаников». Они – настоящая сила как в бизнесе, легальном бизнесе, так и в преступном мире.

Несанкционированный доступ к информации, хранящейся в компьюте­ре.

Понятие компьютерной информации определено в статье 272 Уголовного кодекса. 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.[[1]](#footnote-1) Чаще всего 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 преступников – хакеры[[2]](#footnote-2). Люди, увлеченные компьютерной техникой до такой степени, что это выходит за рамки приличий. По непроверенным данным в мире существуют целые 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 незаконного подключения к удаленным компьютерам. По этому поводу пишутся целые трактаты, их можно найти в неограниченном количестве в Интернете – глобальной всемирной компьютерной сети. Несанкционированный доступ к файлам законного пользователя осу­ществляется также нахождением слабых мест в защите системы. Однажды обнаружив их, нарушитель может неспеша 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 "бре­шей". Авторы больших сложных программ могут не заметить некоторых сла­бостей 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 у нас в стране стали создаваться высшие учебные заведения для обучения специалистов в области информационной безопасности. Несанкционированный 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 "несакнционированного 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, потому что именно эта страна является местом массового зарождения компьютерных технологий. Про Россию говорить пока рано, потому что она, на мой взгляд, только вступает на тернистый путь весобщей "окумпьютерризации", да и возможность совершить преступление в этой области у нас в стране несколько меньше, или порой они вообще не имеют смысла. Интересен случай использования "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 "троянского коня".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 "троянского коня", необходимо искать не его самого, а команды, его формирующие. Развивая эту идею, можно представить себе команды, которые создают команды и т. д.(сколь угодно большое число раз), которые создают "троянского коня".

**Хищение компьютерной информации.**

Россия в этом вопросе, как говорится, "впереди планеты всей", попытки повернуть на правовой путь распространения программного обеспечения практически ни к чему не приводят. Хотя в последнее время видны ощутимые сдвиги: в частности в Москве работниками милиции и налоговыми инспекторами был проведен ряд рейдов по торговым точкам, где было конфисковано большое количество пиратских копий лазерных дисков, взято под арест с последующим возбуждением уголовного дела около ста человек[[3]](#footnote-3). Если "обычные" хищения подпадают под действие существующего уго­ловного закона, то проблема хищения информации значительно более слож­на. Присвоение машинной информации, в том числе программного обеспече­ния, путем несанкционированного копирования не квалифицируется как хи­щение, поскольку хищение сопряжено с изьятием ценностей из фондов орга­низации. Не очень далека от истины шутка, что у нас 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 актив? Или нечто другое, о чем законодатель еще никогда прежде не знал? На мой взгляд, компьютерная программа отличается главным образом тем, что поддается свободному копированию, не теряя ни грамма своих свойств при этом. Виртуальные пространства позволяют размещать огромную, на первый взгляд, 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 очень высокий уровень охраны прав авторов, полностью 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, рассматриваемые в данном реферате, из-за специфичности свойств объекта авторских прав в нашем законодательстве рассмотрены отдельно. Для разговора об авторском праве в данной области, необходимо для начала определить используемые понятия. 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. 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[[4]](#footnote-4)

Каждый пользователь имеет право использовать только тот программный продукт, который он получил на основании договора либо приобрел путем покупки, взял в аренду или в прокат и т.д. На сегодня в нашей стране существует достаточно крепкая законодательная база для реальной охраны и регулирования вопросов в сфере авторства. Но к сожалению эти законы не подкреплены реальными действиями со стороны государства. Наше государство просто закрывает глаза на тот беспредел, по причине которого от нашей страны отворачиваются многие перспективные иностранные партнёры. Большую роль в регулировании вопросов охраны, на мой взгляд, стоит отвести органам ОВД, особенно в связи с тем, что с января 1996 года, в уголовном законе появится новый состав преступления[[5]](#footnote-5). Во многих странах мира, в органах полиции и прокуратуры существуют специальные отделы которые занимаются только вопросами охраны интеллектуальной собственности. 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 доступ к записям программ 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[[6]](#footnote-6). 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 называемый "гриф ограниченного пользования". Из толкования закона также можно судить, что частные фирмы, включая и коммерческие банки, вправе самостоятельно устанавливать ограниченные грифы в целях сохранения коммерческой, банковской, и иных тайн.

**Разработка и распространение компьютерных вирусов.**

Практически все пользователи компьютеров сталкивались с вирусами, и, как говориться, испытали все те прелести, что они несут. Позволю себе небольшое отступление и скажу, что в процессе разработки данной курсовой работы, на компьютер каким-то образом так сказать "просочился" один из вирусов, который специально был создан для уничтожения текстовой информации и загубил всю мою работу. А если представить все это в масштабах большого предприятия? В Уголовном кодексе существуют специальная статья под номером 273 речь, где речь идет о разработке и распространении компьютерных вирусов путем создания программ для ЭВМ или внесения изменений в существующие программы. Опасность компьютерного вируса состоит в том, что он может привести, как следует из текста статьи, к полной дезорганизации системы компьютерной информации и при этом, по мнению специалистов в данной области, может бездействовать достаточно длительное время, затем неожиданно активизироваться и привести к катастрофе[[7]](#footnote-7). Вирус может оказаться причиной катастрофы в таких областях использования компьютерной информации, как оборона, космонавтика, государственная собственность, борьба с преступностью. Именно высокой степенью общественной опасности, на мой взгляд, объясняется то, что уголовный закон преследует достаточно строго за сам факт создания вирусных компьютерных программ для ЭВМ или внесения изменений в уже существующие программы, не оговаривая наступления каких-либо последствий. Преступление считается оконченным, когда программа создана или изменения внесены. 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. Законодатель наконец осознал серьезность создавшейся ситуации, предусмотрев квалифицирующие признаки: такое преступление может иметь и тяжкие последствия – гибель людей, причинение тяжкого вреда здоровью, дезорганизация производства на предприятии или в отрасли промышленности, осложнение дипломатических отношений, вплоть до возникновения вооруженного конфликта. Приходит на память 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. 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. 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 тот записал зараженную версию программы. После этого он возвра­щает программе управление. Пользователъ 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 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" 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 копирование прог­рамм, что является обычной практикой у пользователей персональных ЭВМ. Так скопированными оказываются и зараженные программы. Специалисты предостерегают от копирования 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 . Эпидемия охватила бо­лее б тысяч компьютеров и 70 компьютерных систем. Пострадавшими оказа­лись, в частности, компьютерные центры НАСА, Диверморской лаборатории ядерных исследований, Гарвардского, Питсбургского, Мэрилендского, Вис­консинского, Калифорнийского, Стзнфордского 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 1984 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. В печати часто проводится 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. Замечу, что пожелание ограничить использование непроверенного программного обеспе­чения скорее всего так и останется практически невыполнимым. Это свя­зано с тем, что фирменные программы на "стерильных" носителях стоят немалых денег в конвертируемой валюте. Поэтому избежать их неконтроли­руемого копирования почти 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 гарантией, что никто не рискнет копировать такую дискету.

##### Уничтожение компьютерной информации

Под термином уничтожения информации понимается стирание ее в 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 програмного обеспечения или получить данную информацию от других пользователей, не освобождает виновного от 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.

**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 причем 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 удается сдать заказчику заведомо неисправную продук­цию. К подделке информации можно отнести также подтасовку 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 вторую категорию преступлений, в которых компь­ютер является "средством" достижения цели. В тех случаях, когда компьютерная аппаратура является предметом преступления против собственности, соответственно ее хищение, уничтожение или повреждение подлежит квалафикации по статьям 158-168 Уголовного кодекса. 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 действия не рассматриваются в качестве самостоятельных преступлений, а подлежат квалификации по иным статьям в соответствии с объектом посягательства[[8]](#footnote-8). Вся проблема стоит на мой взгляд в том, что компьютер по сути своей универсален, и позволяет выполнять практически любую работу очень широкого круга назначения[[9]](#footnote-9). 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"[[10]](#footnote-10). 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 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 компьютера.

## Способы совершения компьютерных преступлений

Способ совершения преступления слагается из комплекса специфических действий правонарушителя по подготовке, совершению и маскировке преступления. Обычно преступники, совершая эти действия, оставляют определенные следы, которые в последствие позволяют восстановить картину происшедшего, получить представление о своеобразии преступного поведения правонарушителя, о его личностных данных.

Отечественная криминалистическая наука стала всерьез заниматься вопросом характеристики способов совершения компьютерных преступлений лишь в начале 90-х годов. В этом плане мы отстаем от зарубежных исследователей почти на 20 лет. По-моему, нашим исследователям нужно использовать опыт зарубежных коллег.

В настоящее время можно выделить свыше 20 основных способов совершения компьютерных преступлений и около 40 их разновидностей. И их число постоянно растет. Я выделю 5 основных групп способов совершения компьютерных преступлений. Классифицирующий признак – метод использования преступником тех или иных действий, направленных на получение доступа к средствам компьютерной техники с различными намерениями.

### Изъятие средств компьютерной техники

Сюда относятся традиционные способы совершения «некомпьютерных» преступлений, в которых преступник, попросту говоря, изымает чужое имущество. Чужое имущество – средства компьютерной техники. К этой группе преступлений можно отнести, например, незаконное изъятие физических носителей, на которых находится ценная информация. Такие способы совершения компьютерных преступлений достаточно полно изучены отечественной криминалистической наукой, поэтому можно не заострять внимание на этой группе.

### Перехват информации

Способы основаны на действиях преступника, направленных на получение данных путем определенного перехвата. Виды перехватов:

### Непосредственный перехват

Подключение непосредственно к оборудованию компьютера, системы или сети. Например, к линии принтера или телефонной линии.

Подключение осуществляется с помощью использования бытовых средств и оборудования: телефона, отрезка провода и т.д. перехваченная информация записывается на физический носитель и переводится в человекообразную форму средствами компьютерной техники.

### Электронный перехват

Это дистанционный перехват. Он не требует непосредственного подключения к оборудованию компьютера. Способ основан на установлении приемника, который принимает электромагнитные волны. А если настроить этот приемник на определенную частоту, то можно принимать, например, волны, которые излучает экран монитора. Не вдаваясь в основы физики, скажу, что это принцип электронно-лучевой трубки (кинескоп монитора). Благодаря этому способу можно принимать сигналы с больших расстояний.

### Аудиоперехват

Это самый опасный способ перехвата информации. Он заключается в установке специального прослушивающего устройства (« жучок »). Эти устройства очень трудно обнаружить, потому что они искусно маскируются под обычные вещи. Аудиоперехват также может проводиться с помощью дорогостоящих лазерных установок, которые могут принимать звуковые вибрации, например, с оконного стекла. Этим способом пользуются, в основном, профессиональные преступники.

### Видеоперехват

Этот способ заключается в использовании преступником видеооптической техники для перехвата информации. Способ имеет две разновидности. Первая – физическая, заключается в применении преступником различных бытовых видеооптических приборов (подзорные трубы, бинокли, приборы ночного видения). Полученная информация может фиксироваться на физический носитель. Во втором случае преступник использует специальные электронные устройства, которые предполагают наличие различных каналов связи. Эти устройства состоят из передатчика и приемника. Можно понять, что передатчик находится в нужном помещении и передает получаемые сигналы на приемник, который находится в руках преступника. Этот способ видеоперехвата называется электронным. Он предполагает также использование преступником цифровых видеокамер, видеомагнитофонов с длительной записью и т.д.

**«Уборка мусора»**

Этот способ совершения компьютерных преступлений заключается в неправомерном использовании преступником отходов технологического процесса. Он осуществляется в двух формах: физической и электронной. В первом случае преступник осматривает содержимое мусорных корзин, емкостей для технологических отходов; собирает оставленные или выброшенные физические носители информации. Что касается электронного варианта, то он требует просмотра содержимого памяти компьютера для получения необходимой информации. Дело в том, что последние записанные данные не всегда полностью стираются из памяти компьютера. Существуют специальные программы, которые могут частично или полностью восстанавливать данные на компьютере. Преступник, используя такую программу, может получить необходимую информацию (уничтоженную с точки зрения пользователя). Нужно отметить, что такое происходит из-за халатности пользователя, который выполнил не все действия для полного уничтожения данных.

В третью группу способов совершения компьютерных преступлений можно отнести действия преступника, направленные на получение несанкционированного доступа к средствам компьютерной техники. К ним относятся следующие:

**«За дураком».**

Правонарушителями в данном случае являются внутренние пользователи определенной системы. Используя этот способ, преступник получает несанкционированный доступ к средствам компьютерной техники путем прямого подключения к ним. Подключиться можно с помощью телефонной проводки. Преступление совершается в тот момент, когда сотрудник, который отвечает за работу средства компьютерной техники, ненадолго покидает свое рабочее место, оставляя технику в активном режиме. Как видно этот способ основан на низкой бдительности сотрудников организации.

**«Компьютерный абордаж».**

Когда преступник получает доступ к компьютеру, он не может сразу получить нужные ему данные, так как на полезную информацию обычно ставят пароль доступа. Используя данный способ, преступник производит подбор кода. Для этих целей используются специальные программы, которые с помощью высокого быстродействия компьютера перебирают все возможные варианты пароля. В том случае если преступник знает пароль доступа или кода нет, то доступ получается значительно быстрее. Рассматривая данный способ совершения компьютерных преступлений, необходимо сказать, что существует множество программ, которые взламывают пароль доступа. Но есть также и программы – «сторожи», которые отключают пользователя от системы в случае многократного некорректного доступа. Эти программы я рассмотрю позже. Благодаря им преступниками стал использоваться другой метод – метод «интеллектуального подбора». В этом случае программе – «взломщику» передаются некоторые данные о личности составителя пароля (имена, фамилии, интересы, номера телефонов и т.д.), добытые преступником с помощью других способов совершения компьютерных преступлений. Так как из такого рода данных обычно составляются пароли, эффективность этого метода достаточно высока. По оценкам специалистов с помощью метода «интеллектуального подбора» вскрывается 42% от общего числа паролей.

**Неспешный выбор.**

Данный способ характеризуется поиском преступником слабых мест в защите компьютерной системы. Когда такое место найдено, преступник копирует нужную информацию на физический носитель. Этот способ назван так, потому что поиск слабых мест производится долго и очень тщательно.

**«Брешь».**

В этом случае преступник ищет конкретно участки программы, имеющие ошибки. Такие «бреши» используются преступником многократно, пока не будут обнаружены. Дело в том, что программисты иногда допускают ошибки при разработке программных средств. Такие ошибки впоследствии может обнаружить только высококвалифицированный специалист. Иногда же программисты намеренно делают такие «бреши» с целью подготовки совершения преступления.

**«Люк».**

Когда преступник находит «брешь», он может ввести туда несколько команд. Эти команды срабатывают в определенное время или при определенных условиях, образуя тем самым «люк», который открывается по мере необходимости.

**«Маскарад».**

С помощью данного способа преступник входит в компьютерную систему, выдавая себя за законного пользователя. Самый простой путь к проникновению в такие системы – получить коды законных пользователей. Это можно получить путем подкупа, вымогательства и т.д., либо используя метод «компьютерный абордаж», рассмотренный выше.

**Мистификация.**

Пользователь, который подключается к чьей-нибудь системе, обычно уверен, что он общается с нужным ему абонентом. Этим пользуется преступник, который правильно отвечает на вопросы обманутого пользователя. Пока пользователь находится в заблуждении, преступник может получать необходимую информацию (коды доступа, отклик на пароль и т.д.).

**«Аварийная ситуация».**

Этот способ совершения компьютерных преступлений характерен тем, что преступник для получения несанкционированного доступа использует программы, которые находятся на самом компьютере. Обычно это программы, которые отвечают за «здоровье» компьютера. Они ликвидируют сбои и другие отклонения в компьютере. Этим программам необходим непосредственный доступ к наиболее важным данным. Благодаря им преступник может войти в систему вместе с ними.

**«Склад без стен».**

В этом случае преступник проникает в систему во время поломки компьютера. В это время нарушается система защиты.

К четвертой группе способов совершения компьютерных преступлений я отношу группу методов манипуляции данными и управляющими командами средств компьютерной техники.

**Подмена данных.**

Наиболее популярный способ совершения преступления, потому что достаточно простой. Действия преступника при этом направлены на изменеие или введение новых данных. Это осуществляется при вводе-выводе информации. Например, в банковские счета можно добавить суммы, которые туда не зачислялись, а потом получить эти деньги. Известны случаи, когда этот способ применялся сотрудниками автозаправочных станций, которые изменяли учетные данные путем частичного повреждения физических носителей информации. В результате этого практически невозможно было определить, сколько бензина было продано.

**«Троянский конь».**

Это тоже весьма популярный способ совершения преступления. Он заключается во введении преступником в чужое программное обеспечение специальных программ. Эти программы начинают выполнять новые действия, которые не были запланированы законным владельцем средства компьютерной техники. В соответствии со статьей 273 УК РФ под такой программой понимается «программа для ЭВМ, приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети». «Троянский конь» по сути чем-то напоминает «люк». Отличие в том, что «троянский конь» не требует непосредственного участия самого преступника, программа делает все сама. Обычно она используется преступниками для отчисления на заранее открытый счет определенной суммы с каждой операции. Далее я рассмотрю некоторые виды этой программы.

**«Троянская матрешка».**

Это вид «троянского коня». Предполагает собой самоуничтожение программы из чужого программного обеспечения после выполнения своей задачи.

**«Салями».**

Данный способ основан на быстродействии средств компьютерной техники. Дело в том, что при совершении коммерческих сделок конечные суммы округляются. Остаточные суммы настолько малы, что вообще не учитываются. Накопление денежных средств преступником происходит за счет отчисления сумм со многих операций.

**«Логическая бомба».**

Этот способ преступник использует, когда уверен, что наступят определенные обстоятельства. Способ представляет собой тайное внесение в чужое программное обеспечение специальных команд, которые срабатывают при определенных обстоятельствах. Разновидностью этого способа является «временная бомба». Как можно догадаться, данная программа включается по достижении какого-либо времени.

**Компьютерные вирусы.**

Это программы, которые самопроизвольно присоединяются к другим программам и при запуске последних выполняют различные нежелательные действия (порча файлов и каталогов, искажение и уничтожение информации и т.д.). Этот способ совершения компьютерных преступлений наиболее популярен. В настоящее время в мире существует очень много видов компьютерных вирусов (более 4000). Но всех их можно разбить на несколько групп:

**Загрузочные вирусы.** Заражение происходит при загрузке компьютера с носителя информации, содержащего вирус. Заразить сам носитель достаточно просто. На него вирус может попасть, если пользователь вставил его в приемное устройство зараженного включенного компьютера. При этом вирус автоматически внедряется во внутреннюю структуру носителя.

**Файловые вирусы.** Они поражают исполняемые файлы: EXE, COM, SYS, BAT. Эти вирусы заражают компьютер, если была запущена программа, которая уже содержит вирус. В этом случае происходит дальнейшее заражение других программ, по сути напоминающее вирусное заболевание. Сначала появление вируса практически невозможно зафиксировать, так как он заразил не все нужные программы. Далее происходят нарушения в работе компьютера, степень которых зависит от типа и вида вируса. Большинство вирусов не носят разрушительного характера, так как пишутся программистами-любителями. Этого не скажешь про другую часть вирусов, которая пишется профессиональными программистами, часто имеющими корыстные цели. Для изучения вирусов создана специальная наука – компьютерная вирусология. С точки зрения этой науки вирусы можно разделить на резидентные и нерезидентные, «вульгарные» и «раздробленные».

**резидентные и нерезидентные**

Во-первых, нужно дать определение резидентной программе. Резидентной называется программа, которая по окончании работы оставляет свой код в оперативной памяти компьютера. Оперативная память – это память, предназначенная для исполняемых в данный момент программ и оперативно необходимых для этого данных. Резидентная программа работает параллельно другим программам. И если вирус попадает в оперативную память компьютера, то он фактически заражает все программы, с которыми функционирует параллельно. Резидентный вирус, оставляя свой код в оперативной памяти, возобновляется при каждом включении компьютера. Менее опасными являются нерезидентные вирусы. Они оставляют в оперативной памяти небольшие программы, которые не имеют алгоритма распространения вируса. Такой вирус погибает при выключении компьютера.

**«вульгарные» и «раздробленные» вирусы**

Такое деление произведено по алгоритму строения и обнаружения того или иного вируса. «Вульгарные» вирусы написаны одним блоком и легко обнаруживаются специалистами с помощью специальных антивирусных программ, которые я рассмотрю чуть позже. Что касается «раздробленного» вируса, то нужно сказать, что такая программа разделена на части. Эти части никак не связаны друг с другом, но они «собираются» при определенных условиях во вполне здоровый вирус. При выполнении своей задачи такой вирус распадается или самоуничтожается.

Далее я рассмотрю наиболее популярные вирусные модификации:

**Вирусы-«черви».** Эти вирусы не изменяют программные файлы. Они проникают в память компьютера из компьютерной сети, и вычисляют адреса других компьютеров. Затем в обнаруженные компьютеры рассылаются копии вируса.

**«Паразитические».** Сюда входят вирусы, которые обязательно изменяют программные файлы.

**«Студенческие».** Обычно это вирусы, которые написаны любителями. Такие вирусы содержат много ошибок, и легко обнаруживаются специальными программами.

**Вирусы-«невидимки».**

Это достаточно совершенные вирусы. Их трудно обнаружить антивирусной программой и невозможно увидеть при обычном просмотре файлов, так как при открытии зараженного файла они немедленно удаляются из него, а при закрытии опять заражают.

**Вирусы-«призраки».** Это тоже трудно обнаруживаемые вирусы. Дело в том, что они, заражая программы, постоянно меняют свой код (содержание). Так что во всех следующих зараженных программах нельзя заметить какого-то совпадения. Поэтому эти вирусы трудно обнаружить с помощью антивирусных программ, основанных на этом принципе.

Две последние группы вирусов представляют наибольшую опасность. Эта проблема заставляет вирусологов отходить от стандартных антивирусных программ и находить другие методы борьбы с вирусами.

**«Асинхронная атака».**

Для понимания этого способа совершения компьютерных преступлений нужно дать понятие операционной системе. Операционная система – комплекс программных средств, обеспечивающих управление информационными процессами при функционировании компьютерной системы. Главная задача операционной системы – обеспечение максимальной производительности компьютера. Функции: управление, коммуникация, планирование и т.д. Понятно, что такой комплекс программ имеет очень большую структуру, состав, размеры. Разработкой операционных систем занимаются профессиональные группы программистов иногда в течение нескольких лет. Поэтому операционные системы невозможно проверить на полную работоспособность. Искусный преступник может внести коррективы в нужную операционную систему и заставить работать ее в своих корыстных целях. Такие изменения заметить достаточно сложно. Внесенные команды будут выполняться одновременно с командами пользователя.

**Моделирование.**

Данный способ совершения компьютерных преступлений представляет собой моделирование поведения устройства или системы с помощью программного обеспечения. Например: «двойная» бухгалтерия. Здесь одновременно существуют две бухгалтерские программы, одна из которых функционирует в законном режиме, а другая - в незаконном. С помощью незаконной программы проводят теневые сделки.

**Копирование.**

Этот способ совершения преступления представляет собой незаконное копирование информации преступником программных средств компьютерной техники. Преступник незаконно копирует информацию на свой физический носитель, а затем использует ее в своих корыстных целях. Этот способ распространен из-за своей простоты. Например: два лица заключают договор на разработку программного средства. Заказчик при этом платит определенную сумму за работу. Исполнитель же просто копирует нужную программу из какого-нибудь источника, выдавая ее за свою, и предоставляет ее заказчику.

**Преодоление программных средств защиты.**

Это скорей вспомогательный способ совершения преступления. Он представляет собой умышленное преодоление системы защиты. Существует несколько разновидностей этого способа:

**Создание копии ключевой дискеты.**

Для запускания некоторых систем необходима ключевая дискета. На этой дискете записаны необходимые системные файлы. Преступник может незаконно создать копию такой дискеты с помощью известной программы DISKCOPY. Позже это поможет преступнику попасть в нужную систему.

**Модификация кода системы защиты.**

Код системы защиты выполняет в компьютере следующие функции:

###### Проверка ключевой дискеты

* Проверка санкционированности запуска защищенного информационного ресурса

Модифицируя этот код, преступник просто обходит эти функции. То есть происходит обход системы защиты. Данный способ может быть реализован только высококлассным специалистом, имеющим опыт в этом деле. Время обхода системы защиты может исчисляться неделями.

Использование механизма установки (снятия) программных средств защиты информации.

Некоторые программные средства защиты устанавливаются на физический носитель и закрепляются на нем вместе с другими данными. Так что невозможно произвести копирование с такого носителя. В данном случае преступник производит некий алгоритм действий и снимает защищенные программы с носителя. Этот процесс требует немалых знаний и опыта от правонарушителя.

**Снятие системы защиты из памяти ЭВМ.**

Система защиты периодически загружает защищаемое программное средство в оперативную память для передачи управления этой программой коду защиты. Когда код еще не взял управление на себя, в оперативной памяти находится совершенно незащищенная программа. Преступнику остается сохранить ее в каком-нибудь файле.

В заключение данной главы хотелось бы сказать, что способов совершения компьютерных преступлений становится все больше и больше. Это происходит по мере совершенствования средств компьютерной техники. Хочется надеяться, что эта проблема будет глубже изучена отечественной криминалистикой, так как по проведенному исследованию о существовании тех или иных способов совершения компьютерных преступлений знают всего около 10% респондентов.

## Предупреждение компьютерных преступлений

Почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры. В данном случае профилактические меры следует понимать как деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению. В нашей стране разработкой методов и средств предупреждения компьютерных преступлений занимается криминалистическая наука. Это наука о закономерностях движения уголовно-релевантной информации при совершении и расследовании преступлений и основанных на них методах раскрытия, расследования и предупреждения преступлений. Как видно из определения, предупреждение преступлений является важной составной частью методологии криминалистики.

В настоящее время можно выделить три основных группы мер предупреждения компьютерных преступлений. Выделяя их, я сразу же буду раскрывать их смысл.

Правовые

В эту группу мер предупреждения компьютерных преступлений прежде всего относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере. Если обратиться к истории, то мы увидим, что первый нормативно- правовой акт такого типа был принят американскими штатами Флорида и Аризона в 1978 году. Этот закон назывался «Computer crime act of 1978». Затем почти во всех штатах Америки были приняты аналогичные законодательства. Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных преступлений. Что же касается нашей страны, то первым шагом в этом направлении можно считать Федеральный Закон «О правовой охране программ для ЭВМ и баз данных» от 23 сентября 1992 года. Аналогичные законы в зарубежных странах были приняты на 5-10 лет раньше. 20 и 25 января 1995 года Федеральным Собранием были приняты 2 закона соответственно: «О связи» и «Об информации, информатизации и защите информации». Эти правовые акты явились прогрессивным шагом в развитии данного направления, они:

* Дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны
* Устанавливают и закрепляют права и обязанности собственника на эти объекты
* Определяют правовой режим функционирования средств информационных технологий
* Определяют категории доступа определенных субъектов к конкретным видам информации
* Устанавливают категории секретности данных и информации
* Дают определение и границы правового применения термина «конфиденциальная информация»
* Аналогичные законы действуют в западных странах уже более 20 лет.
* Решающим законодательным аккордом в этой области можно считать принятие в июне 1996 года Уголовного кодекса РФ, устанавливающего уголовную ответственность за компьютерные преступления. Информация в нем – объект уголовно-правовой охраны.
* Организационно-технические меры предупреждения компьютерных преступлений.
* Я рассмотрю данные меры, применяемые в западных странах.

Рассмотрю отдельные положительные, на мой взгляд, организационно-технические меры предупреждения компьютерных преступлений, применяемые в развитых зарубежных странах

В настоящее время руководство профилактикой компьютерных преступлений в этих странах осуществляется по следующим направлениям

1) соответствие управленческих процедур требованиям компьютерной безопасности;

2) разработка вопросов технической защиты компьютерных залов и компьютерного оборудования;

3) разработка стандартов обработки данных и стандартов компьютерной безопасности;

4) осуществление кадровой политики с целью обеспечения компьютерной безопасности;

Например, национальным бюро стандартов США были разработаны базовые требования безопасности, предъявляемые к компьютерным сетям. В их числе:

— пригодность — гарантия того, что сеть пригодна для обеспечения санкционированного доступа;

— контролируемая доступность — гарантия, что сеть обеспечит доступ только санкционированному пользователю для решения санкционированных задач;

— неприкосновенность — защита данных от несанкционированного их изменения и уничтожения;

— конфиденциальность — защита данных от несанкционированного раскрытия;

— безопасность передачи данных — гарантия того, что идентификация пользователей, качество передаваемых данных, время и продолжительность передачи данных обеспечены.

На основе данных требований были созданы соответствующие механизмы технического контроля, отвечающие следующим критериям:

1) целостность — базовая надежность, гарантирующая, что механизм работает как должно;

2) возможность проверки — способность записывать информацию, которая может иметь значение в раскрытии и расследовании попыток посягательства на средства компьютерной техники и других событий, относящихся к вопросам безопасности системы.

В результате практической реализации этих мер стало возможно:

- контролировать физический доступ к средствам компьютерной техники (СКТ);

. контролировать электромагнитное излучение аппаратных СКТ;

— наблюдать за возможной угрозой СКТ и фиксировать каждую такую попытку (методом мониторинга).

Как видно из вышеприведенного, цели и основные положения защиты информации в зарубежных странах по ряду базовых позиций совпадают с российскими и предполагают:

а) предотвращение утечки, хищения, утраты, искажения и подделки информации;

б) предотвращение угроз безопасности личности, общества и государства;

п) предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;

г) обеспечение правового режима функционирования документированной информации как объекта собственности;

д) сохранение государственной тайны и конфиденциальности документированной информации;

е) обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

По методам применения тех или иных организационно-технических мер предупреждения компьютерных преступлений специалистами отдельно выделяются три их основные группы

1) организационные;

2) технические;

3) комплексные (сочетающие в себе отдельные методы двух первых групп).

Организационные меры защиты СКТ включают в себя совокупность организационных мероприятий по подбору проверке и инструктажу персонала, участвующего на всех стадиях ин формационного процесса; разработке плана восстановления информационных объектов после выхода их из строя; организации программно-технического обслуживания СКТ; возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; осуществлению режима секретности при функционировании компьютерных систем; обеспечению режима физической охраны объектов; материально-техническому обеспечению и т. д. и т. п. Организационные мероприятия, по мнению многих специалистов, занимающихся вопросами безопасности компьютерных систем, являются важным и одним из эффективных средств защиты информации, одновременно являясь фундаментом, на котором строится в дальнейшем вся система защиты.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями способствующими совершению компьютерных преступлений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;

6) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в т. ч. находящейся в форме машинной информации;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

В функциональные обязанности указанных лиц прежде всего должны входить следующие позиции осуществления организационных мер обеспечения безопасности СКТ:

1) обеспечение поддержки со стороны руководства конкретной организации требований защиты СКТ;

2) разработка комплексного плана защиты информации;

3) определение приоритетных направлений защиты информации в соответствии со спецификой деятельности организации;

4) составление общей сметы расходов финансирования охранных мероприятий в соответствии с разработанным планом и утверждение ее в качестве приложения к плану руководством организации;

5) определение ответственности сотрудников организации за безопасность информации в пределах установленной им компетенции путем заключения соответствующих договоров между сотрудником и администрацией;

6) разработка, внедрение и контроль за исполнением раз личного рода инструкций, правил и приказов, регламентирующих формы допуска, уровни секретности информации, конкретных лиц, допущенных к работе с секретными (конфиденциальными) данными и т. п.;

7) разработка эффективных мер борьбы с нарушителями защиты СКТ.

При этом, как показывает практика, наиболее надежным средством повышения эффективности мер безопасности СКТ является обучение и ознакомление работающего персонала с применяемыми в конкретной организации организационно-техническими мерами защиты.

Технические меры представляют собой применение различных устройств специального назначения:

Источники бесперебойного питания.

Устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находится компьютерная техника.

Устройства комплексной защиты телефонии.

Устройства пожарной защиты.

Средства защиты портов компьютера.

Также для защиты программного обеспечения нужно ввести параметры доступа в компьютер. Доступ может быть определен как:

— общий (безусловно предоставляемый каждому пользователю);

— отказ (безусловный отказ, например разрешение на удаление порции информации);

— зависимый от события (управляемый событием), предусматривает блокировку обращения пользователя, например в определенные интервалы времени или при обращении к компьютерной системе с определенного терминала;

— зависимый от содержания данных (в этом случае решение о доступе основывается на текущем значении данных, например некоторому пользователю запрещено читать те или иные данные);

— зависимый от состояния (динамического состояния компьютерной системы), осуществляется в зависимости от текущего состояния компьютерной системы, управляющих программ и системы защиты, например может быть запрещен доступ к файлу, если носитель машинной информации не находится в состоянии «только чтение» либо пока не будет открыт логический диск, содержащий этот файл;

— частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз — таким образом предотвращается возможность динамического управления событиями);

— по имени или другим признакам пользователя (например, пользователю должно быть более 18 лет);

— зависимый от полномочий (предусматривает обращение пользователя к данным в зависимости от режима: только чтение, только выполнение и т.д.)

зависимый от предыстории обращения

по разрешению (по паролю)

Что же касается антивирусных программ, то ученые сходятся в том, что в настоящее время существует достаточное их количество, чтобы обезвредить практически любой вирус. Из российских разработок можно выделить: AVP Касперского, AIDSTEST, Adinf, Sheriff, Doctor Web,. Про последнюю программу можно сказать, что она уничтожает даже самокодирующиеся вирусы, которые я выделил в третьей главе. Антивирусные программы обеспечивают защиту компьютера от вирусов на 97%. Три же процента это подтверждение того, что не бывает абсолютно надежных систем. Вообще если соблюдать простые правила (создавать архивы нужных программ, не устанавливать на компьютер носители информации сомнительного происхождения, периодически проверять компьютер на предмет появления вирусов и т.д.) можно избежать лишних проблем.

В заключение данной главы я бы хотел отметить, что от разработок в области компьютерной безопасности зависит очень многое. В конечном итоге это должно привести к образованию индустрии средств безопасности компьютерных систем и технологий.

**Международный и отечественный опыт борьбы и предупреждения компьютерных преступлений и вновь возникающие проблемы.**

Исходя из изложенного можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 272-274 УК.

Кроме этого, нас ждет появление таких специфических форм компьютерных правонарушений, к которым не применимы составы преступлений, предусмотренные вышеуказанными статьями.

Интересным для рассмотрения представляется следующий случай.[[11]](#footnote-11)

В наличии труднодоказуемого и практически ненаказуемого "компьютерного хулиганства" недавно убедилось российское информационное агентство "Интерфакс".

8 июля оно распространило сенсационное сообщение со ссылкой на пресс-службу правительства Армении о том, что во время переговоров на границе Армении и Турции один из охранников турецкой делегации открыл огонь по главе правительства Армении Гранту Багратяну и министру обороны Армении Вазгену Саркисяну. Во время перестрелки они якобы получили ранения, а ответным огнем со стороны армянской охраны был убит покушавшийся и ранен губернатор турецкой провинции Карс.

Сообщение оказалось "дезой". Чуть было не вспыхнул международный скандал. По счастью, спецслужбы быстро выяснили, что имело место, как они классифицировали, "компьютерное хулиганство". "Утку" запустил в информационную компьютерную сеть сотрудник газеты "Республика Армения" некий господин Арташес Хачатрян. Его постигло страшное наказание. "Хулигана" уволили с работы.

Но все же сделана первая попытка реализации уголовно-правовой политики России в новой для нее области - сфере компьютерных правоотношений. Насколько она окажется успешной, как сможет снять накопившиеся здесь противоречия, защитить права заинтересованных лиц - будет зависеть от многих факторов политического, экономического, научно-технического, организационного характера.

Немаловажное значение будет играть понимание правоведами транснационального характера компьютерной преступности и, как следствие, установление международных контактов с правоохранительными структурами. Такими же значимыми факторами будут и контакты с частными охранными структурами и структурами информационной безопасности в кредитно-денежной сфере.

Сегодняшние реалии заставляют двигаться в этих направлениях.

По данным правоохранительных органов криминальное поле кредитно-банковской системы активно заполняется преступлениями, связанными с использованием электронных средств доступа к информации (компьютерные, телекоммуникационные системы, кредитные карточки и др.). Для правоохранительных органов эта проблема наиболее остро встает в связи с переходом абсолютного числа банковских и финансовых структур на расчеты с использованием компьютерных сетей, которыми оснащены более 2270 коммерческих банков.

Например, только по данным ГУЭП МВД России, в 1995-1996 гг. выявлено более 250 преступлений с использованием электронных средств доступа, ущерб от которых составил около 200 млрд. руб.[[12]](#footnote-12)

По данным Федеральной службы реагирования на ЧП в компьютерном пространстве (U.S. Federal Computer Incident Response Capability, FedCIRC), только в прошлом году было зарегистрировано более 2500 случаев, квалифицируемых как ЧП в компьютерной системе или сети, вызванное отказом механизма защиты или умышленной попыткой либо угрозой нарушения этого механизма. Согласно подсчетам отдела ФБР по борьбе с компьютерными преступлениями (Вашингтон, округ Колумбия), хотя бы просто обнаружить удается менее 15% всех преступлений этого рода и лишь 10% из них предаются огласке. Понятно, что без тщательно отработанных методик расследования, помогающих людям обрести чувство защищенности, под сомнением оказывается - ни больше ни меньше - стабильность сегодняшних военных и коммерческих предприятий, не говоря уже об электронной торговле на базе Internet. [[13]](#footnote-13)

В текущем году расположенный в Сан-Франциско Институт компьютерной безопасности (Computer Security Institute, CSI) совместно с ФБР провел исследование, выявившее некоторые закономерности в области компьютерных преступлений . В основу был положен опрос, направленный на определение “размеров бедствия”, а попутно - на повышение уровня осведомленности о компьютерных преступлениях в рядах их настоящих и потенциальных жертв.

Опрос CSI/FBI, охвативший 563 организации, от самых мелких до крупнейших, подтвердил известное предположение, что компьютерные преступления представляют реальную угрозу, усугубляемую тем, что она носит скрытый характер. 60% респондентов смогли оценить свои потери от этих преступлений : суммарная цифра превышает 100 млн дол.

Результаты статистического анализа убытков и типов преступлений не могут считаться достаточно корректными, поскольку, во-первых, не все группы жертв смогли предоставить достоверные сведения о своих финансовых потерях, а во-вторых, чисто денежными потерями ущерб в данном случае далеко не ограничивается. Тем не менее цифры получились любопытные. Три четверти респондентов, понесших финансовые убытки, пострадали от таких преступлений, как мошенничество (26 респондентов, 24 890 тыс. дол.), утечка секретной информации (22 респондента, 21 050 тыс. дол.) и мошенничество с использованием телекоммуникационных систем.

Остальные убытки стали результатом внедрения вирусов, диверсий против данных или сетей, несанкционированного доступа “своих” и “чужаков”, а также новой разновидности кражи - переносных компьютеров.

Долгое время считалось, что причины большинства проблем, связанных с защитой компьютеров, нужно искать внутри фирм. Однако лишь 43% опрошенных сообщили о нападениях “изнутри” (от одного до пяти случаев в каждой фирме), тогда как о таком же количестве покушений извне поведали 47% респондентов.

Подобная картина требует кардинальных решений на международном уровне.

И первые попытки уже сделаны.[[14]](#footnote-14)

"Мы отстаем от преступников на один шаг, а должны быть на шаг впереди" - так сформулировал главную задачу стран - членов "восьмерки" в борьбе с киберпреступностью министр внутренних дел Великобритании Джек Стро.

Британского коллегу поддержала министр юстиции США Джанет Рино, заявившая: "Мы больше не можем бороться с преступлениями XXI века с помощью инструментов XIX века. Точно так же, как компьютеры помогают преступнику, они могут помочь правоохранительным ведомствам". Стро и Рино выступили 10 декабря на пресс-конференции по итогам состоявшейся в Вашингтоне встречи руководителей правоохранительных органов Великобритании, Германии, Италии, Канады, России, США, Франции и Японии.

На этой встрече был принят план совместных действий по борьбе с киберпреступностью, который предусматривает резкую активизацию сотрудничества правоохранительных органов стран "восьмерки". В частности, в соответствии с этим планом будет установлена круглосуточная связь для "своевременного, эффективного реагирования" на транснациональные преступления в сфере высоких технологий. Планом оговариваются также выделение "в достаточном количестве подготовленного и оснащенного специальным оборудованием персонала", "разработка средств быстрого выслеживания идущих по компьютерным сетям атак" с целью оперативного установления компьютерного взломщика.

Если высылка преступника в силу его национальной принадлежности невозможна, страны "восьмерки" обязуются применить к нему те же судебные меры и выделить такие же ресурсы, какие бросила бы на это потерпевшая страна. По словам руководителей правоохранительных органов стран "восьмерки", это обязательство имеет крайне важное значение, так как слишком часто преступник покидает страну, в которой совершил преступление, и возвращается к себе на родину, надеясь укрыться от правосудия.

Министры договорились также предпринять шаги, которые должны помешать киберпреступникам изменять или уничтожать "электронные улики" преступления в компьютерных сетях. Решено доработать действующие национальные законодательства таким образом, чтобы в них содержалось четкое определение компьютерного преступления.

Страны "восьмерки" намерены активнее сотрудничать с компаниями -- изготовителями ЭВМ в разработке новых технических решений, облегчающих задачу предотвращения или обнаружения этого вида преступлений и наказания за них.

Предполагается использование таких технологий, как видеосвязь, позволяющая получать показания у свидетелей, где бы те ни находились.

По словам министра юстиции США Рино, выступившей в роли хозяйки встречи, эти шаги "знаменуют огромный прогресс в наших усилиях по борьбе со всеми видами преступлений, совершаемых с помощью компьютера".

Тема компьютерной преступности сейчас приобрела важное значение и для России, заявил глава российской делегации на встрече "восьмерки" генеральный прокурор РФ Юрий Скуратов. "Начиная с 1991 г. у нас фиксируются случаи несанкционированного проникновения в компьютерные сети, а также более опасные преступления , связанные с хищениями или попытками хищений финансовых средств путем проникновения в системы Центробанка, Внешторгбанка и других финансовых учреждений, -- сказал он. -- Поэтому российская сторона была заинтересована в проведении этой дискуссии. Мы исходили также из того обстоятельства, что лучше быть готовым к тому, чтобы дать ответ на предстоящие вызовы, чем в очередной раз говорить о своей неподготовленности".

Участники встречи приняли коммюнике, в котором подчеркивается, что "характер современных коммуникаций не позволяет ни одной стране в одиночку бороться с проблемой преступности в сфере высоких технологии" и требует выработки общего подхода.

Надо отметить, что российские правоохранительные органы (МВД, ФСБ, ФАПСИ, Прокуратура...) в достаточной степени осознали угрозу которую таит в себе информатизация общества и государства. В меру возможностей, отпущенных скудным финансированием ведомства пытаются делать упреждающие шаги.[[15]](#footnote-15)

Один из самых крупных проектов "компьютеризации" России знаменитые компании SIEMENS NIXDORE и ORACLE осуществляют совместно с Министерством внутренних дел.

Когда работа будет закончена, отечественные сыщики будут обладать одной из самых современных и самых мощных информационных сетей в мире.

Создавать компьютерную сеть МВД у нас начали еще в 1991году, понимая, что с бумажными картотеками много преступников не наловишь.

Контракт подписали с немецкой фирмой Siemens Nixdorf, известной своей основательностью и качеством. Программное обеспечение для управления базами данных, в которых МВД хранит миллионы записей, приобретено у не менее знаменитой американской фирмы Oracle. Правда, до прикладной базы, которая бы помогала разбираться в массивах милицейской информации, иностранцев допустили только на расстояние "вытянутой руки": основные программы разработаны в Новосибирске специальным Центром разработки МВД. Создание милицейской компьютерной сети, которая в конце концов должна раскинуться от Калининграда до Южно-Сахалинска, - сегодня один из немногих глобальных российских информационных проектов, который выполняется четко и в положенные сроки.

Остается пожелать, чтобы подобная сеть сама не стала объектом посягательств преступников.

В завершение хочется с грустью заметить, что страховые компании всерьез предлагают страховать риски безопасности информации[[16]](#footnote-16).

Так страховая компания "Интеррос-Согласие" приступила к страхованию банковских рисков.

"Интеррос-Согласие" будет страховать банки от хищения или потери денежных и других ценностей при перевозке, от финансовых потерь в результате мошенничества персонала банка, подделок и подлогов ценных бумаг, электронных и компьютерных преступлений.

Эти риски "Интеррос-Согласие" намерена перестраховывать на лондонском страховом рынке, российские компании привлекаться к перестрахованию не будут.

В основе нового страхового продукта лежат используемые в мировой практике условия страхования банковских рисков Bankers Blanket Bond (B.B.B.).

При подготовке этого продукта специалисты "Интеррос-Согласия" провели ряд консультаций с британской страховой брокерской фирмы Johnson&Higgins, которая является одним из лидеров в мировом банковском страховании.

**Доказательство в судебных делах по компьютерным преступлениям**

Судебное расследование компьютерных преступлений обычно бывает более сложным, нежели других видов преступлений. Оно требует специальной технической подготовки и в большей степени зависит от показаний свидетелей-экспертов. Обвинение в процессе по делу о компьютерном преступлении должно строиться так, чтобы судья и присяжные, мало знающие о компьютерах и их работе, смогли разобраться в очень сложных технических документах. Свидетели должны убедительно объяснить, почему последствия «неосязаемой» потери данных, являющихся чьей-либо собственностью, или нарушение работы компьютера столь же серьезны, как и ущерб при хищении материальных ценностей (а часто и более серьезны).

Судебные дела по компьютерным преступлениям относительно новы для следователей и обвинителей. Лишь немногие судьи и присяжные имеют представление о компьютерных технологиях, поэтому отношение к компьютерным преступлениям с их стороны может значительно различаться. Одни считают такие преступления серьезными, другие, видя, что преступление не привело к хищению компьютеров или нанесению ущерба зданиям, могут недооценивать его последствия. В некоторых случаях слабое знание специфики проблемы судьей и присяжными может быть даже опасным, так как неверная интерпретация представленного доказательства иногда приводит к ошибочному заключению.

В качестве примера можно привести судебное разбирательство по известному делу Роберта Т. Мориса о внедрении программы-червя в сеть Internet в 1988 году. Эта программа не нанесла прямого материального ущерба, так как не были похищены или повреждены данные. Однако компьютерные центры потеряли миллионы за то время, которое ушло на выявление этой программы и когда не могла выполняться никакая другая работа, а также время, ушедшее на проверку и восстановление работоспособности систем. Во время судебного процесса обвиняемый подтвердил внедрение программы-червя, но заявил, что это было сделано без злого умысла, в результате чего он был осужден условно. И таких случаев, когда условное осуждение выбиралось в качестве наказания за компьютерные преступления, принесшие многомиллионный ущерб, немало.

Какие же основания позволяют утверждать, что факт совершения компьютерного преступления имел место? Что является его доказательством, уликой? В случае убийства ответ прост. Это отпечаток пальца на столе на месте преступления, след пули, записка, выпавшая из кармана убийцы, когда он убегал из комнаты. В случае мошенничества ответ более сложен. Например, если преступник вошел в компьютерную систему по чужому паролю и перевел деньги с одного счета на другой, будет ли контрольный журнал компьютера уликой преступления? Будет ли уликой распечатка этого контрольного журнала, сделанная на следующий день после совершения преступления? Или распечатки, сделанные в последующие дни? Или достаточно лишь копии этих распечаток? Типичный ответ юриста заключается в том, что все это может считаться доказательством при определенных обстоятельствах.

В судебных разбирательствах по компьютерным преступлениям часто возникает вопрос о том, какие файлы и другие компьютерные документы могут быть использованы в качестве доказательств правонарушения.

На сегодняшний день в разных законах (а тем более в законах разных стран) имеются существенные различия даже в определении того, что такое компьютеры и как они работают. Но все же рост компьютерных преступлений и судебных прецедентов по ним позволяет судам проявлять все большую осведомленность относительно того, какие доказательства и как должны представляться в ходе судебных разбирательств по компьютерным преступлениям, а правоохранительным органам разрабатывать процедуры проверки компьютерных доказательств во время расследования преступления и правила обращения с ними для представления в суд. Поскольку новый Уголовный кодекс России, где впервые появилась глава «Преступления в сфере компьютерной информации», вступил в силу только в январе 1997 года, в нашей стране пока не накоплен опыт судебных дел по компьютерным преступлениям и не разработаны документы, регламентирующие представление компьютерных доказательств.

ЗАКЛЮЧЕНИЕ

Преступления в сфере компьютерной информации, особенно это касается взлома удаленных компьютеров, практически являются идеальной возможностью для преступников совершать свои деяния без наказания. Практическая возможность доказательства этих преступлений сводится к цифре очень приближенной к нулю. Конечно особо громкие дела известны всему миру, но в связи с компьютерной и законодательной безграмотностью нашего населения дела, связанные с хищением информации, взломов компьютеров и тому подобное, почти не когда не заводятся, а если такое случается то редко и сложно доказуемые.

Впервые мир узнал о компьютерных преступлениях в начале 70-х годов, когда в Америке было выявлено довольно большое количество таких деяний. Как известно – наиболее опасные преступления – это те, которые носят экономический характер. Например – это неправомерное обогащение путем злоупотребления с автоматизированными информационными системами, экономический шпионаж, кража программ и так называемого "компьютерного времени", традиционные экономические преступления, совершаемые с помощью компьютера. Изначально, как показывает история, органы уголовной юстиции боролись с ней при помощи традиционных правовых норм о преступлениях против собственности: краже, присвоении, мошенничестве, злоупотреблении доверием и тому подобное. Однако вскоре практика показала, что такой подход не отвечает всем требованиям сложившейся ситуации, поскольку многие преступления в сфере компьютерной деятельности не охватываются традиционными составами преступлений. Во многих преступлениях отсутствовал материальный признак, так как предмет отсутствует как материальная вещь, существующая в реальном физическом мире. "Обман компьютера" – вещь несколько эфемерная, потому что это всего-лишь механизм и обмануть его в принципе невозможно. С таким же успехом можно обманывать дверной замок. Уничтожение имущества тоже не подходит под данные преступления – нет уничтожения как такового. Хотя подобные действия, описанные мной выше и могут принести значительный имущественный ущерб – без физического повреждения компьютера такой состав попросту не имеет смысла. Преступления в сфере компьютерной информации имеют, на мой взгляд, как бы двоякий смысл, и поэтому требуют специальных статей в Уголовном кодексе. Принятый в недавнем прошлом кодекс содержит целую главу, включающую в себя три статьи, что, на мой взгляд, несколько мало. Даже исходя из дословного толкования, позволю себе сказать, что они уже несколько устарели по смысловому значению, и требуют обновлений.

Разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. И российские криминологи и криминалисты внесут в это свой вклад. Ели только российские политики не дадут им умереть с голоду …

Список использованной литературы

1. ***Законодательные акты и комментарии***
   1. Уголовный кодекс Российской Федерации от 24.05.96. – СПб.: Альфа, 1996;
   2. Федеральный закон "Об информации, информатизации и защите информации" от 20 февраля 1995 года №24-ФЗ;
   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;
   5. Наумов А.В. Комментарий к Уголовному кодексу. – М.: Юристъ, 1997;
   6. Скуратов Ю.И., Лебедев В.М. Комментарий к Уголовному кодексу. – М., 1996;
   7. Комментарий Федерального Закона «Об информации, информатизации и защите информации». М.: Институт государства и права РАН, 1996.
2. ***Учебники и монографии***
   1. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность. - М., 1991;
   2. Беляев В.С. Безопасность в распределительных системах. – М., 1995;
   3. Борзенков Г.Н., Комиссаров В.С. Уголовное право Российской Федерации. – М.: Олимп, 1997;
   4. Ведеев Д.В. Защита данных в компьютерных сетях. - М., 1995;
   5. Здравомыслов Б.В. Уголовное право России. Особенная часть. – М.: Юристъ, 1996;
   6. Копылов В.А. Информационное право. – М.: Юристъ, 1997;
   7. Уголовное право. Особенная часть. П/р Казаченко И.Я., Незнамовой З.А., Новоселова Г.П. – М.: Норма – Инфра, 1998;
   8. В.С. Горбатов, О.Ю. Полянская, “Доказывание в судебных делах по компьютерным преступлениям”, Москва, МИФИ, 97
   9. Крылов В.В. Информационные компьютерные преступления. М.: ИнфраМ-Норма, 1997.
3. ***Статьи в журналах и интернет***
   1. Hackzone – территория взлома, №2, 1999 (электронная версия).
   2. Крылов В.В. Информационные преступления – новый криминалистический объект // Российская юстиция. 1997. № 4.
   3. Баев О.Я., Мещеряков В.А. «Проблемы уголовно-правового регулирования в сфере компьютерной информации».// «Защита информации. Конфидент», № 5, 1998.
   4. Горбатов В.С., Полянская О.Ю. «Доказательство в судебных делах по компьютерным преступлениям». // «Защита информации. Конфидент», № 6, 1997.
   5. Никифоров И. «Компьютерные преступления». // «Защита информации. Конфидент», № 5, 1995.
   6. Завадский И.И. «Информационная война – что это такое?» // «Защита информации. Конфидент», № 5, 1996.
   7. Рачук Т.В. «Уголовные наказания за информационные преступления» // «Защита информации. Конфидент», № 4, 1997.
   8. Фоменков Г.В. «О безопасности в Internet» // «Защита информации. Конфидент», № 6, 1998.
   9. Гайкович В.Ю “Основы безопасности информационных технологий”, Москва, “Инфо-М”, 98
   10. Ю.Ляпунов, В.Максимов, “Ответственность за компьютерные преступления”, “Законность” №1, 1997г.
   11. D.J.Icove, Как бороться со взломщиками компьютеров, Сети и Телекоммуникации, №4, 1997г.

1. см. Бюллетень Верховного Суда СССР, 1982, №6, страница 22 [↑](#footnote-ref-1)
2. От английского hucker - взломщик [↑](#footnote-ref-2)
3. данные взяты из телевизионных передач и журнальных статей издательства "Компьютерра" [↑](#footnote-ref-3)
4. см. ст. №1 Закона "О правовой охране программ для электронных вычислительных машин и баз данных." [↑](#footnote-ref-4)
5. см. ст.146 УК РФ “Нарушение авторских и смежных прав.” [↑](#footnote-ref-5)
6. см. ст. 137, 138, 183 УК РФ [↑](#footnote-ref-6)
7. см. Батурин Ю.М. Компьютерная преступность и компьютерная безопасность., М., 1991 г. [↑](#footnote-ref-7)
8. см. Новое уголовное право России. Особенная часть, М., 1996 года, страница 241 – 274. [↑](#footnote-ref-8)
9. в частности стоит упомянуть про открытый психологами и физиологами эффект "двадцать пятого кадра", который якобы позволят осуществлять на человека внушающее воздействие на уровне подсознания. Ученые утверждают, что таким способом вполне можно убить человека. [↑](#footnote-ref-9)
10. Пример взят из книги Д.Ведеева Защита данных в компьютерных сетях М., 1995, № 3, стр. [↑](#footnote-ref-10)
11. Национальная Служба Новостей, по материалам газеты ТРУД, 18.07.97 “ЭВМ в черной маске”. [↑](#footnote-ref-11)
12. И.Викторов, М.Миронов. "ЗАКОННОСТЬ В КРЕДИТНО-БАНКОВСКОЙ СФЕРЕ", Законность №11, 1997г. [↑](#footnote-ref-12)
13. D.J.Iocoveю. Как бороться со взломщиками компьютеров, Сети и Телекоммуникации №5, 1998г.

    http://ftp.infoart.ru/it/press/cwm/30\_97/colla.htm [↑](#footnote-ref-13)
14. Министры "восьмерки" приняли план борьбы с киберпреступностью, ИТАР-ТАСС

    Компьютерная неделя N5 (129) от 10/2/1998 Москва

    http://old.pcweek.ru/98\_05/iso/ns20.htm [↑](#footnote-ref-14)
15. Михаил Самсонов, Дмитрий Будневский, МАФИЯ В СЕТЯХ, Милицейский компьютер за несколько секунд установит личность преступника

    http://www.milparade.ru/project/mafia.htm [↑](#footnote-ref-15)
16. RBCNET, компания “Интеррос-Согласие”, 04.09.97

    http:/www.rbcnet.ru/ecopress/040997/1009/insure\_68\_2 [↑](#footnote-ref-16)