**Оглавление**

Введение 3

Информация и преступление 4

Общая характеристика преступлений в сфере компьютерной информации. 6

Основные понятия 8

Уголовно правовая характеристика преступлений в сфере компьютерной информации. 10

Неправомерный доступ к компьютерной информации (ст. 272 УК). 10

Создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК). 13

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК) 16

Способы совершения компьютерных преступлений 18

Изъятие средств компьютерной техники 18

Перехват информации 18

Непосредственный перехват 18

Электронный перехват 19

Аудиоперехват 19

Видеоперехват 19

Предупреждение компьютерных преступлений 26

ЗАКЛЮЧЕНИЕ 27

Литература 28

# Введение

Развитие и все более широкое распространение новых орудий труда - информационных и телекоммуникационных технологий, обеспечивающих более эффективное пользование информационными ресурсами, определило необходимость правовой оценки ситуации и разработки организационно - правовых механизмов пресечения общественно опасного поведения (или «криминальной деятельности») в данной области.

Формирование отечественного законодательного регулирования в области информационных правоотношений прошло сложный путь. Признание обществом, а вслед за ним и законодателем факта существования информационного ресурса как реального объекта, имеющего материальное выражение, признание информации в качестве объекта гражданских прав, установление возможности признания права собственности физических и юридических лиц, государства на информацию, информационные системы, технологии и средства их обеспечения повлекло необходимость государственного реагирования в области уголовно-правовых запретов.

Анализ норм действующего УК РФ показывает, что развитие законодательного регулирования информационных правоотношений нашло в нем свое отражение, но для правильного понимания и оценки ряда предусмотренных УК РФ действий в качестве общественно опасных, необходимо привлечение норм всего законодательства, регламентирующих эти действия как незаконные, неправомерные.

Без ясного понимания норм, регулирующих информационные правоотношения, правоохранительные органы не имеют возможности правильно определить круг вопросов, подлежащих доказыванию, а затем и точно квалифицировать выявленные случаи преступлений. Без такого понимания невозможно и создание соответствующих методик расследования преступлений, совершенных в информационной сфере в целом. Между тем, подобные методики расследования криминальной деятельности являются крайне необходимыми в практике, поскольку нередко данная разновидность деятельности является составной частью иных преступлений.

Как следует из Особенной части УК РФ, информационные правоотношения в целом получили в нем широкую уголовно-правовую защиту. Из этого следует, *что информационные отношения стали новым объектом, а информация* - *новым предметом преступного посягательства.* Противоправные действия, связанные с использованием «компьютерных» и (или) «телекоммуникационных» инструментов - лишь специализированная часть преступной деятельности в сфере информации, направленной на нарушение прав и гарантий личности, юридических лиц и государства.

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.

# Информация и преступление

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.

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

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.

Можно выделить следующие характерные особенности компьютерных преступлений:

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.**

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:

# Общая характеристика преступлений в сфере компьютерной информации.

Особую тревогу 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”.

Глава о преступлениях в области компьютерной информации и включенные в нее нормы являются новыми и не имели аналогов в предшествовавшем отечественном уголовном законодательстве. Практика применения российскими правоохранительными органами непосредственно данных составов весьма ограничена в связи с тем, что нередко рассматриваемые противоправные действия являются составными элементами других более тяжких преступлений, а также в связи с трудностями определения и выявления признаков преступной деятельности данного вида.

|  |  |  |
| --- | --- | --- |
| Регулируемые законодательством действия, совершаемые с информацией (сообщениями) | | |
|  | |  |  | |
|  | |  | Создание и обработка информации | |
|  | |  |
|  | |  | Сбор и поиск информации (в т.ч. доступ к ней) | |
|  | |  |
|  | |  | Накопление и хранение информации | |
|  | |  |
|  | |  | Защита информации | |
|  | |  |
|  | |  | Распространение и предоставление информации | |
|  | |  |
|  | |  | Непредставление информации | |
|  | |  |
|  | |  | Копирование информации | |
|  | |  |
|  | |  | Уничтожение информации | |
|  | |  |
|  | |  | Изменение (модификация) информации | |
|  | |  |
|  | |  | Хищение, изъятие и утрата информации | |
|  | |  |
|  | |  | Блокирование информации | |
|  | |  |

***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);

***Родовым объектом*** преступлений в сфере компьютерной информации является общественная безопасность и порядок в отношениях, связанных с информационными процессами - процессами сбора, обработки, накопления, хранения, поиска и распространения информации, с использованием ЭВМ, их систем и сетей. Существенно то, что ***предметом***данных преступлений является компьютерная информация, а не информационное оборудование, обеспечивающее информационные процессы. Правонарушения, совершенные в ходе данных процессов, не связанные с использованием указанного оборудования, квалифицируются с помощью иных статей УК РФ, предусматривающих ответственность за соответствующие конкретные действия.

***Непосредственным объектом*** данных преступных деяний является безопасность информационных систем, базирующихся на использовании ЭВМ, системе ЭВМ или их сети.

***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.

## Основные понятия

*Информация (документ) -* это зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

*Компьютерная информация -* идентифицируемый, имеющий собственника элемент информационной системы - сведения, знания или набор команд (программа), хранящийся в ЭВМ или управляющий ею.

*ЭВМ (электронно-вычислительная машина)* есть комплекс электронных устройств, позволяющий осуществлять предписанные программой и (или) пользователем информационные процессы, в том числе последовательности действий по обработке информации и управлению устройствами, над документированной и иной (символьной, образной) информацией и выполнять ее ввод - вывод, уничтожение, копирование, модификацию, передачу информации в сети ЭВМ и другие действия.

*Система ЭВМ* - комплексы, в которых хотя бы одна ЭВМ является элементом системы, либо несколько ЭВМ составляют систему.

*Сети ЭВМ* - компьютеры, объединенные между собой сетями электросвязи.

*Машинные носители* компьютерной информации - устройства памяти ЭВМ, периферийные устройства ЭВМ, компьютерные устройства связи, сетевые устройства и сети электросвязи.

Общими для описания объективной стороны информационных преступлений являются и понятия уничтожение, блокирование, модификация, копирование информации и нарушение работы ЭВМ.

*Уничтожение информации* - наиболее опасное явление, поскольку при этом собственнику информации или информационной системы наносится максимальный реальный вред. Наиболее опасным разрушающим информационные системы фактором чаще всего являются действия людей: уничтожение информации осуществляется умышленными и неосторожными действиями лиц, имеющих возможность воздействия на эту информацию. Существование возможности восстановления уничтоженной неправомерным воздействием информации не является исключающим ответственность фактором.

*Блокирование -* результат воздействия на ЭВМ и ее элементы, повлекшие временную или постоянную невозможность осуществлять какие-либо операции над компьютерной информацией.

*Под модификацией информации* следует понимать внесение в нее любых изменений, обусловливающих ее отличие от той, которую включил в систему и владеет собственник информационного ресурса. Вопрос о легальности произведенной модификации информации следует решать с учетом положений законодательства об авторском праве. Законодательством санкционированы следующие виды легальной модификации программ, баз данных (а следовательно, информации) лицами, правомерно владеющими этой информацией:

* модификация в виде исправления явных ошибок;
* модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя;
* модификация в виде частичной декомпиляции программы для достижения способности к взаимодействию с другими программами.

*Копирование* - изготовление копии объекта. Копирование информации без явно выраженного согласия собственника информационного ресурса независимо от способа копирования подпадает под действие уголовного закона. Важным вопросом является проблема мысленного запечатления полученной информации в процессе ознакомления с нею в памяти человека, без которого, кстати, невозможно ее разглашение.

*Нарушение работы ЭВМ* - любая нестандартная (нештатная) ситуация с ЭВМ или ее устройствами, находящаяся в причинной связи с неправомерными действиями и повлекшая уничтожение, блокирование, модификацию или копирование информации.

# Уголовно правовая характеристика преступлений в сфере компьютерной информации.

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

Уголовная ответственность за неправомерный доступ к компьютерной информации установлена ст. 272 УК РФ. *Непосредственным объектом* данного преступного деяния являются общественные отношения, обеспечивающие безопасность информационных систем от внешних воздействий сточки зрения конфиденциальности содержащейся в них компьютерной информации. Конфиденциальность понимается как предотвращение возможности использования информации лицами, которые не имеют к ней отношения. *Предметом преступления* является компьютерная информация, охраняемая законом, находящаяся либо на машинном носителе, либо в ЭВМ, либо в системе ЭВМ или в сети ЭВМ.

*Объективная сторона* данного преступления характеризуется деянием, последствием и причинной связи между ними. Деяние выражается в неправомерном доступе к компьютерной информации. *Доступом к ЭВМ* является санкционированное и упорядоченное собственником информационной системы взаимодействие лица с устройствами ЭВМ и (или) ознакомление лица сданными, содержащимися на машинных носителях или в ЭВМ. Регламентация порядка доступа к компьютерной информации устанавливается ее собственником в его внутренних нормативных актах, которые доводятся до сведения пользователей информации. Такая регламентация может содержаться также в договорах или соглашениях с пользователями информационных ресурсов. Нарушение установленного собственником информации порядка образует неправомерность доступа к компьютерной информации. Существенно, что современные информационные системы, как правило, обладают инструментами разграничения доступа для различного круга пользователей. Это создает предпосылки для оценки действий как неправомерного доступа и для случаев, когда пользователи, имеющие доступ к строго определенной части информационной системы, вторгаются в иные ее элементы, не имея для этого прямо выраженного согласия собственника системы.

Особо следует отметить компьютерную информацию, собственником которой является государство или его субъекты и образования. К государственной конфиденциальной информации относятся в частности служебная тайна, государственная тайна, данные предварительного следствия (ст. 310 УК РФ), сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст. 311 УК РФ), сведения о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа (ст. 320 УК РФ). Подобная информация охраняется государством непосредственно в силу соответствующего закона.

Следует различать преступную деятельность по захвату ЭВМ и машинных носителей с целью завладения ими как имуществом, имеющим самостоятельную материальную ценность, в не связи с тем, какая информация на них находится, и деятельность, совершаемую с целью доступа к компьютерной информации, связанную с изъятием указанных предметов как носителей этой информации. В первом случае такую деятельность при известных условиях необходимо отнести к преступлениям в сфере экономики. Преступная деятельность, направленная на противоправное причинение ущерба компьютерной информации является неправомерным доступом независимо от способа доступа. Поэтому утверждения о том, что «не образует объективной стороны... уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитными волнами, механическими ударами...» представляются не верными.

Поскольку собственник или владелец информационных ресурсов, обязан обеспечить режим защиты информации, в том числе и путем установления правил эксплуатации ЭВМ, препятствующих несанкционированному ознакомлению посторонних лиц с принадлежащими ему информационными ресурсами и их защиту от неправомерных действий, создается возможность оценки любого неправомерного доступа к компьютерной информации со стороны лица, имеющего доступ к ЭВМ, системе ЭВМ или к их сети (далее для краткости - «доступ к ЭВМ») как совершения совокупности преступлений (ст. 272 и 274 УК РФ), так как осуществляя неправомерный доступ, такое лицо нарушает правила использования конкретной компьютерной информации. Фактически лица, совершая указанные выше деяния, всегда (правомерно или неправомерно) получают возможность оперировать ресурсами чужого компьютера, нарушая правила их эксплуатации, установленные собственником или владельцем информационного ресурса. Имеются признаки совокупности преступлений и в случае незаконного использования объектов авторского права лицами, осуществлявшими копирование информации в виде программ для ЭВМ, при проникновении в ЭВМ с целью совершения хищения денежных средств, выявления идентифицирующей информации о физических (например, ПИН-коды кредитных карточек) и юридических (например, коды модемного управления расчетным счетом) лицах для последующего завладения их имуществом, шпионажа, диверсии и др. в таких случаях применяются правило, предусмотренное ч. 3 ст. 17 УК РФ.

С субъективной стороны преступление всегда совершается ***умышленно****.* В соответствии с действующим законодательством при создании информационных систем, основанных на применении компьютерной техники, их собственники обязаны предусмотреть такие меры безопасности, которые бы обеспечили лишь правомерный и упорядоченный доступ к информационным ресурсам. Преодоление этих мер защиты всегда связано с определенным профессионализмом лица, осуществляющего доступ к компьютерной информации. Применение профессиональных знаний для неправомерного доступа к компьютерной информации свидетельствует об осознании общественной опасности совершаемых действий и о прямом умысле на ознакомление с компьютерной информацией. Мотивы доступа к информации не имеют значения для квалификации содеянного по ст. 272 УК РФ, поскольку совокупность норм действующего законодательства объявляет любую информацию, имеющую собственника, конфиденциальной до момента, пока собственник информации прямо не объявит об обратном.

Частью 2 ст. 272 УК РФ предусмотрено три квалифицирующих признака, состоящих в совершении рассматриваемого преступления: совершение группой лиц по предварительному сговору или организованной группой, совершение лицом с использованием своего служебного положения и совершение лицом, имеющим доступ к ЭВМ. Для использования служебного положения характерно, что лицо, осуществившее неправомерный доступ к ЭВМ, по своей служебной компетенции или трудовому договору (контракту) имеющее определенные полномочия, превысило свои права или нарушило свои обязанности или использовало их вопреки интересам работодателя. Лицо, имеющее доступ к ЭВМ, может иметь таковой в силу указанных выше соглашений или договоров в качестве пользователя информационной системы. Умышленное нарушение достигнутых с собственником договоренностей о порядке пользования информацией и нарушение согласованных правил доступа к информационному ресурсу является квалифицирующим обстоятельством и соответствует идее законодателя об усилении защиты прав субъектов в сфере информационных процессов «...в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба».

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

Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ установлена ст. 273 УК РФ. Непосредственным ***объектом*** данных преступных деяний являются общественные отношения, обеспечивающие безопасность информационных систем с точки зрения целостности содержащейся в них компьютерной информации от внешних воздействий. Говоря о целостности, подразумевают защиту данных от разрушения и изменения. ***Предметом*** этого преступления являются альтернативно программа для ЭВМ или машинный носитель с вредоносной программой. Хотя в ст. 273 УК РФ термины «программы» и «машинные носители» употребляются во множественном числе, для уголовной ответственности по этой статье УК достаточно наличия предмета в виде только одной программы или только одного машинного носителя вредоносной программы.

Программы для ЭВМ являются разновидностью компьютерной информации. Под *«программой для ЭВМ»* законодательством понимается объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определенного результата. Программы фактически существует в двух видах - в виде **«исходного текста»**, т.е. описанного с помощью языков программирования алгоритма обработки данных или управления ими, и в виде **«объектного кода»** - исходного текста, компилированного в набор машиночитаемых символов. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения. Программа, специально разработанная или модифицированная для несанкционированного собственником информационной системы уничтожения, блокирования, модификации либо копирования информации, нарушения обычной работы ЭВМ, является **вредоносной**.

Ранее для обозначения этого явления в литературе часто использовалось понятие «компьютерный вирус» или «информационные инфекции». Так же именовалось данное явление в проекте ныне действующего Уголовного кодекса. Использовав определение «вредоносные» программы, законодатель позволил практике расширить существовавшие представления о программах подобного рода. Ранее в специальной литературе, посвященной «компьютерной вирусологии» считалось, что в тех случаях, когда в результате действия «вирусов» происходят существенные разрушения файловой системы, уничтожение информации и т.п. - «вирус» является опасным, если же в результате его действия на экране, например, появляются стихи, брань и т.п., «вирус» считается безопасным. Учитывая определение законодателя, ВП могут быть разделены на три больших класса на базе представлений о цели создания программы и последствиях ее действия.

***Первый класс ВП,*** обладая свойствами самостоятельного размножения в системах и сетях ЭВМ, не всегда приводит к существенным последствиям для информационных ресурсов, хотя в некоторых случаях и модифицирует информацию, а иногда и блокирует ЭВМ, их сети и системы. Разработчики этого класса ВП не рассматривают свою деятельность как общественно-опасную, хотя объективно она является таковой.

***Второй класс ВП*** - «опасные вирусы», разрушающие информационные системы и приносящие существенный вред.

***Третий класс ВП*** предназначен для организации неправомерного доступа к чужим информационным ресурсам. Известные случаи противоправного проникновения в ЭВМ показывают, что злоумышленники обычно вынуждены, прежде всего, изменять различными способами, в том числе и путем внедрения ВП, программные средства (или порядок их работы), обеспечивающие взаимодействие устройств ЭВМ между собой и с пользователем. Такие ВП обеспечивают вход в систему или привилегированный режим работы с ней.

***Объективная сторона*** данного преступления выражается в создании, использовании и распространении ВП для ЭВМ, наступившими в результате этих деяний последствиями и причинной связи между ними. ***Действия по созданию*** ВП включают: постановку задачи, определение среды существования и цели ВП; выбор средств и языков реализации ВП; написание непосредственно текста ВП; ее отладка; запуск и непосредственное действие ВП. Внесение изменений вредоносного характера в уже существующую программу, превращающую ее во вредоносную, как правило, связано с модификацией программ, что может быть при некоторых условиях расценено как неправомерный доступ к компьютерной информации (ст. 272 УК РФ).

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.

***Использование*** ВП подразумевает применение разработанных иным лицом ВП при эксплуатации ЭВМ и обработке информации. Следует обратить особое внимание на признак санкционированности наступления опасных последствий при действии ВП. Очевидно, что собственник информационного ресурса вправе в необходимых случаях (например, исследовательские работы по созданию антивирусных средств и т.п.) использовать вредоносные программы.

***Под распространением программ*** в соответствии с законом понимается 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. Распространением вредоносных программ является не только передача самих программ в виде набора объектных кодов, но и опубликование или индивидуальная рассылка исходных текстов подобных программных продуктов. Указанные действия должны находиться **в причинной связи с наступившими последствиями** - уничтожением, блокированием, модификацией либо копированием информации, нарушением работы ЭВМ, системы ЭВМ или их сети.

***Субъективная сторона*** данного состава преступления характеризуется двумя формами вины: умыслом в отношении преступления, ответственность за которое установлена ч.1 ст. 273 УК РФ, и неосторожностью по отношению к тяжким последствиям, предусмотренным ч. 2 этой статьи. Для субъективной стороны данного состава преступления существен признак **заведомости**. При создании программы для ЭВМ или внесении изменений в существующую программу, сопровождаемых несанкционированным уничтожением, блокированием, модификацией или копированием информации, нарушением работы ЭВМ, системы ЭВМ или их сети умысел может быть прямым или косвенным, а при распространении вредоносных программ или машинных носителей с такими программами - только прямым. Заведомость означает, что лицо должно достоверно знать, что создаваемая программа будет вредоносной или таковой она окажется после внесения в нее изменений, либо лицо должно также достоверно знать, что распространяемая программа вредоносна или вредоносен машинный носитель с такой программой. При этом достаточно, чтобы это лицо знало не обо всех вредоносных свойствах ВП, а лишь о некоторых из них.

Частью 2 статьи 273 УК РФ предусмотрен один квалифицирующий признак-причинение по неосторожности тяжких последствий. Под тяжкими последствиями понимается причинение существенного материального ущерба собственнику или собственникам информационных систем, пострадавших от действия ВП, а также их пользователям, возникший, в том числе, в связи с восстановлением работоспособности информационных систем после действия ВП, утрата важной информации или серьезное нарушение прав собственников на ее использование, выход из строя крупных систем управления, основанных на работе ЭВМ и др. Известно, что в результате распространения ВП возникают значительные, и вместе с тем не всегда точно определяемые потери.

**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)

*Непосредственным объектом данного* преступного деяния являются общественные отношения, обеспечивающие внутреннюю безопасность информационных систем, базирующихся на использовании ЭВМ, системы ЭВМ или их сети с точки зрения целостности и конфиденциальности содержащейся в них компьютерной информации. Иными словами, интерес владельца компьютерной системы или сети относительно правильной эксплуатации системы или сети.

Существует два вида *правил эксплуатации ЭВМ,* которыми должны руководствоваться в своей деятельности лица, работающие с ЭВМ. Первый вид правил - *инструкции по работе с ЭВМ и машинными носителями информации*, разработанные изготовителем ЭВМ и периферийных технических устройств, поставляемых вместе с данным экземпляром ЭВМ. Эти правила обязательны к соблюдению пользователем ЭВМ под угрозой, как минимум, потери прав на гарантийный ремонт и обслуживание. Второй вид правил - *правила, установленные собственником или владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения, определяющие порядок пользования ЭВМ, системы ЭВМ и сети ЭВМ, а также иными носителями информации.*

***Объективная сторона*** данного деяния заключается в действиях или бездействии лица, которое в соответствии с правилами, установленными собственником информационной системы, обязано было осуществлять операции с компьютерной информацией в определенном порядке, но не соблюдало эти правила, и это послужило причиной уничтожения, блокирования или модификации информации, понятия которых давались ранее.

Понятие существенного вреда является оценочным и установление объема причиненного собственнику информационной системы вреда в результате воздействия вредоносных программ или нарушения правил эксплуатации ЭВМ будет осуществляться судом с учетом совокупности полученных данных. Следует правильно различать последствия воздействия на компьютерную информацию, причинившие вред информационным ресурсам, и вред, причиненный преступными действиями в целом. Так, например, при изменении данных в информационной системе (в частности, данных учета движения товарно-материальных ценностей) с целью совершения их хищения вред, наносимый информационной системе, определяется затратами собственника системы на восстановление правильного учета. Вред, нанесенный непосредственно хищением, является самостоятельным видом вреда, причиненного криминальной деятельностью.

При правильной оценке данной разновидности преступной деятельности как направленной на причинение ущерба компьютерной информации, не могут быть квалифицированы как нарушение правил эксплуатации ЭВМ действия, связанные с использованием средств и элементов информационного оборудования при совершении с ними или с их помощью действий, не относящихся к обработке информации.

Как уже указывалось, доступом к ЭВМ является санкционированное и упорядоченное собственником информационной системы взаимодействие лица с устройствами ЭВМ и (или) ознакомление лица сданными, содержащимися на машинных носителях или в ЭВМ. Совершение указанных действий лицом, имеющим доступ к ЭВМ, рассматривается законодателем как отягчающее наказание обстоятельство, поскольку ст. 63 УК РФ совершение преступления с использованием доверия, оказанного виновному в силу его служебного положения или договора, признается таковым.

***Субъективная сторона*** рассматриваемого состава преступления характеризуется виной в форме умысла, прямого или косвенного. Виновный осознает, что, во-первых, нарушает правила эксплуатации ЭВМ, системы ЭВМ или их сети и, во-вторых, такое нарушение является общественно опасным; предвидит возможность или неизбежность альтернативно уничтожения, блокирования или модификации охраняемой законом информации ЭВМ и во всех случаях причинения существенного вреда и желает наступления этих последствий либо сознательно их допускает или относится к ним 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.

# 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. 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.

# 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.

Правовые меры предупреждения компьютерных преступлений.

В эту группу мер предупреждения компьютерных преступлений прежде всего относят нормы законодательства, устанавливающие уголовную ответственность за противоправные деяния в компьютерной сфере. Первым шагом в этом направлении можно считать Федеральный Закон «О правовой охране программ для ЭВМ и баз данных» от 23 сентября 1992 года. 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»

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.

# 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 является весьма проблематичным

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. 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.

# Литература

1. Уголовный кодекс Российской Федерации от 24.05.96. – СПб.: Альфа, 1996;

2. Федеральный закон "Об информации, информатизации и защите информации" от 3. 20 февраля 1995 года №24-ФЗ;

4. Закон Российской Федерации "Об авторском и смежных правах" от 9 июля 1993 года №5351-1;

5. Закон Российской Федерации "О правовой охране программ для электронных вычислительных машин и баз данных" от 23 сентября 1992 года №3523-1;

6. Наумов А.В. Комментарий к Уголовному кодексу. – М.: Юристъ, 1997;

7. Комментарий Федерального Закона «Об информации, информатизации и защите информации». М.: Институт государства и права РАН, 1996.

8. Копылов В.А. Информационное право. – М.: Юристъ, 1997;

9. Уголовное право. Особенная часть. П/р Казаченко И.Я., Незнамовой З.А., Новоселова Г.П. – М.: Норма – Инфра, 1998;

10. Hackzone – территория взлома, №2, 1999 (электронная версия).

11. Крылов В.В. Информационные преступления – новый криминалистический объект // Российская юстиция. 1997. № 4.

1. Ю.Ляпунов, В.Максимов, “Ответственность за компьютерные преступления”, “Законность” №1, 1997г.
2. ”Криминалистические проблемы оценки преступлений в сфере компьютерной информации.”, “Уголовное право” № 4, 1997г..