**Курсовая работа по уголовному праву**

**На тему**

**ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**

**2009**

# СОДЕРЖАНИЕ

Введение 3

1. Понятие компьютерной информации, развитие информационных отношений, последствия информатизации общества 8

2. Понятие и общая характеристика преступлений в сфере компьютерной информации 19

3. Характеристика конкретных видов преступлений в сфере компьютерной информации 25

3.1 Неправомерный доступ к компьютерной информации (статья 272) 28

3.2 Создание, использование и распространение вредоносных программ для эвм (статья 273) 31

3.3 Нарушение правил эксплуатации эвм, системы эвм или их сети (статья 274) 33

4. Способы защиты компьютерной информации от преступных посягательств 36

Заключение 43

Библиография 45

# введение

***Актуальность темы курсовой работы*** не вызывает сомнений.

Поступательно развивающийся научно-технический прогресс ставит важность компьютерных информационных технологий на первый план. Порой законодатель не успевает за все увеличивающимися темпами технократического и информационного развития общества. Изменения, происходящие в экономической жизни России – формирование и развитие частно - собственнических отношений, создание финансово-кредитной системы, предприятий различных форм собственности и т.п. - оказывают существенное влияние на вопросы правовой защиты информации, включая информацию компьютерную.[[1]](#footnote-1)

Обеспечение правовой защиты компьютерной информации выступает на первый план деятельности любой фирмы, учреждения, госслужбы и т.п. Следует подчеркнуть, что отдельные сферы государственной деятельности (банковские и финансовые институты, промышленные национальные информационные сети, системы государственного управления, оборонные и специальные структуры) требуют специальных мер правовой защиты и безопасности данных и предъявляют повышенные требования к надежности функционирования компьютерных информационных систем в соответствии с характером и важностью решаемых ими задач. Каждое противоправное посягательство в сфере компьютерной информации это не только сбой работы компьютерной сети и “моральный” ущерб для работников предприятия и сетевых администраторов. По мере развития технологий платежей электронных, “безбумажного” документооборота и других, серьезный сбой локальных сетей может парализовать работу целых корпораций и банков, что может привести к значительному материальному ущербу и колоссальным убыткам. Не случайно защита данных в компьютерных сетях, борьба с компьютерной преступностью становится одной из актуальных проблем российского уголовного законодательства.

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

Не вызывает сомнения, что компьютерные преступления во всем мире имеют устойчивую тенденцию к росту. Ключевым положением борьбы с кибертерроризмом является интеграция правовых систем различных стран. Возможно, поэтому отмечается снижение роли национального законодательства. На первый план выходят инструменты межгосударственного (международного) регулирования[[2]](#footnote-2).

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

К техническим мерам можно отнести защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения и т.п.

К организационным мерам относится охрана вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя и т.п.

К правовым мерам следует отнести разработку правовых норм, устанавливающих уголовную ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

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

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

- конфиденциальность (законность) информации;

- доступность информации для всех авторизованных зарегистрированных пользователей;

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

Таким образом, проблема компьютерной преступности составляет важную часть российского уголовного права. Разработка и совершенствование эффективной правовой основы, которая обеспечила бы нормальное функционирование механизма защиты компьютерной информации, представляет собой задачу на будущее. Но уже сегодня можно говорить о необходимости разработки нескольких правовых проблем в качестве составных частей правового механизма защиты компьютерной информации:

- установление контроля над несанкционированным, противоправным доступом к компьютерным информационным данным системы.

- ответственность за выполнение надлежащих технологических операций, связанных с защитой компьютерной информации.

***Целью*** исследования является изучение сущности, видов, субъектов, объектов компьютерных преступлений.

Для достижения указанной цели поставлены ***следующие задачи*:**

- рассмотреть возникновение и развитие информационных отношений, остановившись подробно на понятии, функциях информационных отношений, их значимости и последствиях информатизации общества;

- дать характеристику компьютерных преступлений;

- изучить конкретные виды компьютерных преступлений;

- описать основные способы защиты компьютерной информации от преступных посягательств.

В качестве ***предмета исследования*** выступили компьютерные преступления.

***Методологической основой работы*** служит диалектический метод познания и анализ рассматриваемых явлений.

Характер рассматриваемых в курсовой работе вопросов обусловил использование комплекса ***основных методов***:

* материалистические;
* исторические;
* метод сравнительного анализа;
* формально-юридический метод;
* эмпирические;
* источниковедческие.

Выбор ***структуры курсовой работы*** обусловлен последовательностью решения поставленных задач и логикой изучения темы.

* В первой главе рассматриваются возникновение и развитие информационных отношений, понятия, функции информационных отношений, их значимость и последствия информатизации общества.
* Во второй главе дается характеристика компьютерных преступлений.
* В третьей главе изучаются конкретные виды компьютерных преступлений.
* В четвертой главе описываются основные способы защиты компьютерной информации от преступных посягательств

При написании курсовой работы были изучены учебные материалы, монографии, публикации на страницах периодической печати.

# 1. Понятие компьютерной информации, Развитие информационных отношений, последствия информатизации общества

В связи с бурным процессом развития научно-технической революции сформировался новый вид общественных отношений - информационные. Данные общественные отношения образовались в связи с появлением информационных ресурсов, имеющих свои отличительные особенности:

1) они непотребляемы и подвержены не физическому, а моральному износу;

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

3) процесс их создания и использования осуществляется с помощью компьютерной техники.

Как следует из Особенной части УК РФ[[3]](#footnote-3), информационные правоотношения в целом получили в нём широкую уголовно-правовую защиту. Из этого следует, что информационные отношения стали новым объектом, а информация - новым предметом преступного посягательства. Неизбежным следствием появления новых общественных отношений стали правонарушения в сфере компьютерной информации, в том числе и в форме преступлений, которые представляют реальную угрозу для нормального развития и течения общественной жизни.

Информационные отношения возникают и развиваются в процессе сбора, обработки, накопления, поиска, получения, передачи и распространения информации. Объектами данных отношений могут выступать: информация, информационные процессы, информационные системы и ресурсы, информационная сфера (среда) и продукты; информационная безопасность, средства обеспечения автоматизированных информационных систем и их технологий; словари, тезаурусы и классификаторы; инструкции и методики, программы для ЭВМ; базы и банки данных; топологии интегральных микросхем и сами интегральные микросхемы; средства международного информационного обмена.[[4]](#footnote-4)

В настоящее время в соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[[5]](#footnote-5) под информацией понимаются сведения (сообщения, данные) независимо от формы их представления. Правовому регулированию подлежит преимущественно количественно ограниченная совокупность информации, а именно, документ или документированная информация. При этом документированная информация в качестве организационной формы выступает как зафиксированная на материальном носителе путём документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях её материальный носитель.

В правовом смысле документом может быть признан не каждый носитель, содержащий информацию, а лишь тот, который имеет реквизиты, позволяющие его идентифицировать по отношении к собственнику, владельцу и пользователю информации. При этом одним из пробелов действующего законодательства является то, что конкретные признаки, позволяющие идентифицировать тот или иной документ, законом не установлены. Представляется, что свойства реквизитов и порядок идентификации документа должны определяться в каждом случае отдельно в зависимости от физических свойств носителя информации.

Одним из особых видов информации, подпадающих под правовое регулирование и уже закреплённых в российском уголовном законодательстве в качестве предмета неправомерного доступа, является компьютерная или машинная информация. Информационное законодательство содержит определение информации, соответствующее современному уровню законодательного регулирования информационных отношений, однако существенным недостатком при этом выступает отсутствие общих законодательных критериев определения реквизитов документированной информации, в первую очередь, подпадающей под правовое регулирование, а также отсутствие легального толкования таких понятий, как «машинный носитель», «ЭВМ», «система ЭВМ», «сеть ЭВМ», порождающее неоднозначные трактовки данных понятий в научной литературе и правоприменительной практике.

Информация должна обладать определённой ценностью, а также наличием статуса ограниченного доступа. Несмотря на то, что собственнику информации предоставлено право самостоятельно устанавливать режим доступа к ней, в данном случае он ограничен законом и может получить уголовно-правовую защиту лишь в отношении той информации, отнесение которой к конфиденциальной прямо предусмотрено правовыми актами. В противном случае произошло бы неоправданное расширение предмета уголовно-правового регулирования защиты информации. Та информация, которая имеет определённую ценность для собственника, но законодательными актами не определена как конфиденциальная, может быть защищена собственником правовыми средствами в гражданско-правовом или ином порядке.

Несмотря на значимость информации, как объекта уголовно-правовой защиты, в современном российском уголовном законодательстве, а также в теории уголовного права не существует системного подхода к данной проблеме. В уголовном законодательстве самостоятельно обозначены лишь преступления в сфере компьютерной информации, хотя в современных условиях правомернее говорить о более широком понятии, а именно, о преступлениях в сфере информационно-коммуникационных (телекоммуникационных) отношений, включающих в себя все общественно опасные деяния, совершённые в информационно-коммуникационной сфере, а не только в сфере компьютерной информации. Введение в УК РФ главы 28 «Преступления в сфере компьютерной информации» не решает всех проблем обеспечения информационной безопасности уголовно-правовыми мерами, однако обозначает вектор развития уголовного законодательства в информационном обществе.[[6]](#footnote-6)

На наш взгляд необходимо конкретизировать ряд понятий и определений, используемых в данной главе УК РФ. Необходимый уровень проработки и разъяснения данных понятий дан известным специалистом в этой области Карелиной М.М.[[7]](#footnote-7)

Компьютерная информация - информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ.

В дополнение к определению, необходимо заметить, что под компьютерной информацией понимаются не только сами сведения (информация), а также форма их представления в машинном (компьютерном) виде, т.е. совокупность символов, зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, либо ином материальном носителе). При рассмотрении дел следует учитывать, что при определённых условиях и физические поля могут являться носителями информации.

Программа для ЭВМ (компьютера) - объективная форма представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определённого результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

База данных - это объективная форма представления и организации совокупности данных (например: статей, расчётов), систематизированных таким образом, чтобы эти данные могли быть найдены и обработаны с помощью ЭВМ.

Особенно удачным видится определение компьютерной информации, которое даётся д.ю.н., професором кафедры криминалистики МГУ им. М.В. Ломоносова В.В. Крыловым, предлагающим следующее криминалистическое определение компьютерной информации как специального объекта преступного посягательства. Компьютерная информация есть сведения, знания или набор команд (программа), предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях – идентифицируемый элемент информационной системы, имеющей собственника, установившего правила её использования[[8]](#footnote-8).

Но представляется правильным и следующее - при использовании компьютерной информации в качестве средства совершения другого преступления отношения по её охране страдают неизбежно, т.е. она сама становится предметом общественно опасного деяния.

Негативным последствием информатизации общества является появление так называемой компьютерной преступности. Сложность решения вопроса заключается в том, что диапазон противоправных действий, совершаемых с использованием средств компьютерной техники, чрезвычайно широк. К разряду компьютерных следует отнести те преступления, у которых объектом преступного посягательства является информация, обрабатываемая и хранящаяся в компьютерных системах, а орудием посягательства служит компьютер. По этому пути пошло и российское законодательство.[[9]](#footnote-9)

Понятие «компьютерные преступления» изначально возникло как определение традиционных преступлений (например, кражи и мошенничества), совершаемых с помощью компьютерной техники (только как критерий определения способа совершения преступления). Позднее, основываясь на исследованиях криминалистов, к компьютерным преступлениям стали относить также преступления, совершённые в отношении компьютерной информации, т.е. компьютерная информация была признана объектом преступлений. С одной стороны, появление угрозы неправомерного доступа к информации с помощью компьютерной техники, а также специфика данного способа совершения преступления, привели к осознанию социальной ценности информации с ограниченным доступом и необходимости её уголовно-правовой защиты. С другой стороны, ныне существующее признание предметом неправомерного доступа лишь компьютерной информации, позволяет говорить лишь о частичности или «однобокости» уголовно-правовой защиты информации с ограниченным доступом, поэтому уголовному праву на современном этапе необходимо перейти от «частных» случаев защиты информации от неправомерного доступа к более общему подходу и не ставить пределы данной защиты в зависимость от вида носителей информации.[[10]](#footnote-10)

Ряд авторов предлагает ввести ещё одно понимание компьютерных преступлений, не содержащиеся в уголовно-правовом законодательстве России. Под компьютерными преступлениями понимаются преступления, в которых компьютеры и другие средства компьютерной техники используются преступниками как средство совершения корыстного преступления, их умысел направлен на завладение чужим имуществом путём внесения изменений в программы и базы данных. Одной из главных проблем проявившегося в последние годы так называемого компьютерного права является определение компьютерных преступлений. Наиболее распространённое определение, понимающее под компьютерным преступлением - преступление, совершённое с использованием компьютерной техники или направленное против безопасности компьютерной информации, не отвечает потребностям науки и практики сегодняшнего дня и нуждается в уточнении. Можно выделить три подхода. Первый заключается в отнесении к преступлениям несанкционированного доступа в защищенные компьютерные системы, заражения вирусами, противоправного использования компьютерных систем и информации. Он характерен для таких стран, как Норвегия, Сингапур, Словакия, Филиппины, Южная Корея. Второй подход заключается в признании компьютерными преступлениями лишь тех деяний, которые связаны с причинением ущерба имуществу и электронной обработке информации (Дания, Швеция, Швейцария, Япония). Третий подход характерен для стран с высоким уровнем компьютеризации, значительной компьютерной преступностью (США, Великобритания, Франция, Германия, Нидерланды) и развитой правовой базой. Он состоит в криминализации деяний, связанных не только с имущественным ущербом, но и с нарушением прав личности, с угрозой национальной безопасности и т.д. Данный подход в основном принят и в России, поскольку существует достаточно развитая нормативная база по информационной безопасности.

На основе проведённого анализа существующих в научной литературе в настоящее время классификаций компьютерных преступлений, а также УК РФ и УК зарубежных стран, предлагается следующая классификация компьютерных преступлений. Согласно данной классификации компьютерные преступления первоначально подразделяются на две большие группы:

1) собственно компьютерные преступления и

2) преступления смежные с компьютерными преступлениями. Внутри первой группы выделяем:

- компьютерный саботаж;

- компьютерное мошенничество;

- несанкционированный доступ к компьютерной информации;

- неправомерное завладение компьютерной информацией;

- модификация компьютерной информации;

- изготовление и сбыт специальных средств для получения несанкционированного доступа к компьютерной системе или сети;

- создание, использование и распространение вредоносных программ для ЭВМ;

- нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети.

До настоящего времени наукой не выработано чёткого единого определения компьютерного преступления. Это объясняется целым рядом причин: 1) сравнительно небольшой срок законодательной регламентации данного вида общественных отношений и уголовно-правовой оценки компьютерных преступлений; 2) при попытках сформировать искомое понятие учёные-юристы используют различные подходы к данной проблеме (в зависимости от отраслей науки); 3) относительно слабо развитое международное сотрудничество и недостаточный международный обмен опытом по решению данной проблемы.[[11]](#footnote-11)

Из-за своей специфической природы и повышенной социальной опасности компьютерные преступления практически с момента своего появления анализировались криминологами, криминалистами и специалистами в области компьютеров с различных точек зрения, однако до сих пор не выработано единого взгляда на данный вид преступлений. Условно точки зрения специалистов в данной области можно разделить на три группы:

1. Компьютерные преступления представляют собой самостоятельный вид преступной деятельности, который представляет собой самостоятельные составы преступлений.

2. Компьютерных преступлений как самостоятельного вида не существует, их следует рассматривать лишь как квалифицирующий признак обычных, «традиционных» преступлений. При этом компьютер при совершении преступления выступает в качестве объекта преступления, орудия преступления, средства, на котором подготавливается преступление или среды, в которой оно совершается.

3. Предлагается также весьма расширительное толкование понятия компьютерных преступлений, в соответствии с которым к ним относятся любые посягательства на связи и отношения людей, опосредующих применение и использование компьютерной техники. Третий подход, на наш взгляд, является излишне расширительным, по существу, безграничным. Первый же - совершенно очевиден, общедоступен и, именно из-за этого, широко применяется в мировой практике.

Информационные ресурсы в современном обществе объективно обладают значительной ценностью, действующее уголовное законодательство не содержит комплексного подхода к проблеме обеспечения информационной безопасности уголовно-правовыми мерами.

Сегодня, уголовное законодательство ограничивается лишь фрагментарными мерами защиты охраняемой законом информации в зависимости от её содержания или типа носителя. На современном этапе развития процесса информатизации в России возникла необходимость разработки в уголовном законодательстве системы преступлений в сфере информационных отношений, составной частью которых должны выступить уже закрепленные в УК РФ преступления в сфере компьютерной информации, которые определили направления развития уголовной науки. Разработка категории преступлений в сфере информационных отношений применительно к неправомерному доступу также обусловлена особенностями системы современного российского информационного законодательства. Данная система основана на единственном критерии классификации информации как объекта правового регулирования: разделении информации по содержанию на общедоступную и с режимом ограниченного доступа.

Признавая теоретическую значимость подобного рода исследовании, отметим, что они пока ещё не привели к формированию целостного научного представления о социально-юридической природе составов незаконного использования компьютерной информации, не содержат ответов на сложные вопросы квалификации данного вида преступного посягательства, практически не затрагивают проблем эффективности действия норм, содержащихся в статьях 272, 273 и 274 УК РФ.

Представители правоохранительных органов испытывают затруднения при квалификации преступлений в сфере компьютерной информации. Это объясняется рядом причин:

1) это недостаточная проработка действующего законодательства, а также следственной и судебной практики привлечения к уголовной ответственности за компьютерные преступления;

2) трудности доказывания и судебных исследований, связанных с использованием нетрадиционных носителей информации, недостаточная изученность и практика этого объекта права;

3) криминалистические проблемы, состоящие и том, что технико-криминалистические, тактические и методические приёмы, методы и средства раскрытия и расследования подобного рода преступлений в полной мере не отработаны как на теоретическом, так и на практическом уровнях;

4) сложности организационного характера, состоящие в том, что при относительном насыщении аппаратными и техническими средствами правоохранительные органы до сих пор не имеют развитой системы локальных сетей, достаточного количества квалифицированных специалистов по использованию таких средств для целей расследования.[[12]](#footnote-12)

Российское уголовное законодательство включает в себя ряд неизвестных ранее составов преступлений, среди которых есть нормы, направленные на защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности[[13]](#footnote-13).

Таким образом, необходимость установления уголовно-правовой защиты компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации.

# 2. Понятие и общая характеристика преступлений в сфере компьютерной информации

Динамичные условия современного развития общества нередко наталкиваются на проблемы, которые являются зеркальным отражением его стремления к созданию более совершенных эффективных моделей существования. Одной из таких проблем являются злоупотребления при использовании средств ЭВМ, информационных технологий.

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что несанкционированные вмешательства в деятельность автоматизированных систем управления и контроля различных объектов способны вызвать тяжкие и необратимые последствия, связанные не только с имущественным ущербом, но и с физическим вредом людям.

В современной литературе широко описываются разные случаи проникновения хакеров не только в финансовые струю; но и в суперсекретные базы данных военных ведомств и ядер объектов. Введение в Уголовный кодекс ст. 272-274 свидетельствует о стремлении законодателя не только обеспечить уголовно-правовое регулирование новой сферы общественных отношений, но и путем угрозы уголовным наказанием максимально снизить негативные издержки неправомерного или недобросовестного обращения с ЭВМ и компьютерной информацией.

Представляется, что использовать термин «компьютерные преступления» в отношении деяний, предусмотренных гл. 28 УК, не совсем корректно.

Термин «компьютерные преступления» означает совершение деяний, в которых компьютер выступает в качестве предмета посягательства, а также когда он является техническим средством совершения преступления. Как предмет посягательства компьютер является предметом преступлений против собственности, и его хищение, уничтожение или повреждение квалифицируются по ст. 158-168 УК.

Информационная структура (программа, информация), которая содержится в компьютере, не может являться предметом преступлений против собственности, так как машинная информация не отвечает одному из основных критериев предмета этих преступлений - она не обладает физическим признаком (не объективирована в конкретно осязаемой форме). Поэтому ее нельзя похитить, повредить или уничтожить как другое имущество. Единственно, она может выступать в качестве объекта авторского права, и в этом случае ответственность наступает по ст. 146 УК (нарушение авторских и смежных прав).

Компьютер как техническое средство совершения преступления рассматривается в одном ряду с такими средствами, как оружие, автомобиль либо любое иное техническое приспособление.[[14]](#footnote-14)

В этом смысле его использование имеет прикладное значение, например, для облегчения хищения, сокрытия налогов и т.д. Такие действия в настоящее время по УК РФ не рассматриваются в качестве самостоятельных преступлений, а являются способом совершения иных преступлений, квалифицируемых по другим статьям УК РФ.

Особенность деяний, предусмотренных гл. 28 УК, заключается в том, что предметом этих посягательств являются информация, содержащаяся в компьютере, и компьютер как носитель информации. Ущерб в этих случаях причиняется отношениям, обеспечивающим безопасное производство, хранение, использование или распространение информации и информационных ресурсов либо их защиту. Причинение такого ущерба осуществляется с помощью компьютера как средства (инструмента) совершения преступления. Поэтому более точным является наименование преступлений, предусмотренных в гл. 28 УК, в соответствии с ее названием «Преступления в сфере компьютерной информации».[[15]](#footnote-15)

Видовым объектом данных преступлений выступают отношения по безопасному производству, хранению, использованию или распространению информации и информационных ресурсов либо их защиты.

Предмет соответствующих преступлений компьютерная информация. В праве под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащиеся в информационных системах. Однако при этом необходимо одно уточнение. УК говорит не о любой, а именно о компьютерной информации, и поэтому речь идет только о той информации, которая неотделима от ЭВМ. ЭВМ представляет собой совокупность аппаратно-технических средств и средств программирования, позволяющую производить операции над символьной и образной информацией. Система ЭВМ это упорядоченная совокупность взаимосвязанных и взаимодействующих как единое целое ЭВМ, обеспечивающих выполнение определенной функции. Сеть ЭВМ представляет собой совокупность двух или более соединенных каналом связи и имеющих программное обеспечение, позволяющее осуществлять эту связь. Она может быть локальной (в пределах одного учреждения), региональной или международной (например, Internet). Компьютерная информация может находиться или на машинном носителе (магнитном диске, являющемся либо составной частью ЭВМ, либо принадлежностью её периферийного устройства, магнитной ленте, перфокарте, дискете (компактные переносные магнитные диски), магнитно-оптическом диске (CD-ROMe) или непосредственно в ЭВМ (в постоянном и оперативном запоминающих устройствах), либо в системе ЭВМ или их сети.

Как предмет преступления информация может быть двух видов. В ст. 272 и 274 УК речь идет об охраняемой законом компьютерной информации. В ст. 273 УК предметом является общедоступная информация.[[16]](#footnote-16)

Охраняемая законом информация это информация ограниченного доступа, специальный правовой статус которой устанавливается законами или иными нормативными актами. Степень и уровень защиты информации такого рода устанавливаются ни основании федеральных законов уполномоченными органами в отношении персональных данных либо собственником информационных ресурсов или уполномоченным лицом в отношении конфиденциальной документированной информации. Перечень сведений конфиденциального характера утвержден Указом Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г[[17]](#footnote-17). В этот перечень входят:

- сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих к распространению в средствах массовой информации в установленных федеральными законами случаях;

- сведения, составляющие тайну следствия и судопроизводства, служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);

- сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);

- сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);

- сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Вместе с тем это не означает абсолютную закрытость перечисленных данных. В некоторых случаях законодательством устанавливаются исключения. Так, перечень сведений, которые не могут и признаваться коммерческой тайной, установлен постановлением «жительства РСФСР «О перечне сведений, которые не могут составлять коммерческую тайну» от 5 декабря 1991 г. № 35. Второй вид информации это информация общего пользования, предназначенная для пользования неограниченным кругом лиц. Для преступления, предусмотренного ст. 273 УК, предметом является информация как первого, так и второго вида. По характеристике объективной стороны неправомерный доступ к компьютерной информации (ст. 272 УК), а также создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК) совершаются только путем активных действий, время как нарушение правил эксплуатации ЭВМ, системы или их сети (ст. 274 УК) как путем активных действий, и бездействием. При этом преступления, предусмотренные ст. 272 и 274 УК, предполагают не только совершение общественно опасного деяния, но и наступление общественно опасны следствий, а также установление причинной связи между деянием и последствием. Отсутствие реальных последствий в таких случаях обусловливает квалификацию содеянного как покушение и преступление. Однако покушение на преступления, предусмотренные ч. 2 ст. 273 и 274 УК, невозможно. Способ, место, время и обстановка как дополнительные признаки на квалификацию не влияют, но могут учитываться при назначении наказания.

Характер субъективного отношения к содеянному в ст. 272 УК по большей части законодателем не определяется. Однако не означает, что преступления в сфере компьютерной информации могут совершаться и с неосторожной, и с умышленной формами вины. За исключением ч. 2 ст. 273 и 274 УК, где прямо оговаривается неосторожное отношение к наступившим тяжким ни следствиям, в остальных случаях эти преступления совершаю и только умышленно. Мотивы и цели, которыми руководствуются виновные лица, могут быть различными и для квалификации преступления не имеют. Это могут быть хулиганские или корыстные побуждения, месть и т.п.

Специальные признаки субъекта описываются законодательством лишь в ч. 2 ст. 272 УК и ч. 1 ст. 274 УК. В остальных случаях это может быть любое вменяемое лицо, достигшее 16-лет возраста.

Таким образом, преступления в сфере компьютерной информации можно определить как умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производственное хранение, использование или распространение информации и информационных ресурсов либо их защиту.[[18]](#footnote-18)

# 3. Характеристика конкретных видов преступлений в сфере компьютерной информации

В условиях стремительной информатизации, захватившей практически все стороны жизни нашего общества, роста количества ЭВМ. карманных персональных компьютеров (КПК), мобильных телефонов, смартфонов и др. устройств, используемых в России, недостаточного уровня защищенности информации от противоправных посягательств, не исключено, что в скором времени проблема уголовно-правового регулирования информационной безопасности станет в один ряд с такими глобальными проблемами современности, как экологический кризис, организованная преступность, коррупция, отсталость развивающихся стран и др. Таким образом, защита информации нуждается в ещё более эффективной правовой (в том числе и уголовно-правовой) охране.

Признавая теоретическую значимость подобного рода исследований, отметим, что они пока ещё не привели к формированию целостного научного представления о социально-юридической природе составов незаконного посягательства и не затрагивают проблем эффективности действия норм, содержащихся в статьях 272, 273 и 274 УК РФ.

Важнейшей проблемой уголовно-правовых мер обеспечения информационной безопасности является проблема защиты информации от неправомерного доступа. Наличие данной проблемы заключается в том, что защите от неправомерного доступа подлежит наиболее ценная охраняемая законом информация, а также в том, что неправомерный доступ к охраняемой законом информации влечёт, как правило, значительные общественно опасные последствия, в частности, нарушение её конфиденциальности, целостности и доступности. Вместе с тем, современные уголовно-правовые меры защиты информации от неправомерного доступа основаны на приоритетности защиты информации, находящейся на определённых носителях (компьютерной информации), что, в силу несоответствия данного подхода положениям информационного законодательства, влечёт отсутствие чёткой системы уголовно-правовой защиты информации от неправомерного доступа.[[19]](#footnote-19)

Вышеуказанные обстоятельства выступают причиной необходимости разработки системы противодействия преступлениям в сфере компьютерной информации, одной из составляющих которой должен выступить неправомерный доступ к охраняемой законом информации. При этом степень уголовно-правовой защиты информации должна определяться её содержанием, а не свойствами носителя.

Уголовно-правовая защита компьютерной информации привлекала внимание многих исследователей, в частности, таких как: Ю.М. Батурин, Н.Н. Безруков, СВ. Бородин, Т.А. Бушуева, В.В. Вехов, А.Г. Волеводз, и др. Однако большинство данных исследований носят преимущественно криминалистическую или криминологическую направленность. Уголовно-правовые исследования, как правило, заключаются в рассмотрении основных элементов состава преступления, предусмотренного статьями 272-274 Уголовного кодекса Российской Федерации. Изложенное позволяет говорить о том, что в настоящий момент проблема комплексного уголовно-правового подхода к защите компьютерной информации, независимо от типа носителя, требует детального изучения и возможно внесение соответствующих изменений в действующее законодательство.

Российское уголовное законодательство включает в себя ряд неизвестных ранее составов преступлений, среди которых есть нормы, направленные на защиту компьютерной информации. Такие нормы появились в российском законодательстве впервые. К уголовно-наказуемым отнесены:

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

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

3) нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети (ст. 274 УК РФ).

**Видовым объектом** преступлений в сфере компьютерной информации являютсяинформационные отношения, т. е. отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Из этого определения следует, что и информационные отношения стали новым объектом преступления. Конкретно эти преступления направлены против той части установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации. Необходимость установления уголовной ответственности за причинение вреда в связи с использованием именно компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации по сравнению, скажем, с информацией, зафиксированной на бумаге и хранящейся в сейфе.

Таким образом, необходимость установления уголовно-правовой защиты компьютерной информации вызвана возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации. Уголовный кодекс РФ в главе 28 впервые в отечественном законодательстве предусмотрел ответственность за совершение преступлений в сфере компьютерной информации. Появление в уголовном законе данной главы - несомненный шаг вперёд не только в борьбе с компьютерной преступностью, но и вообще в сфере борьбы с преступностью в области высоких технологий.[[20]](#footnote-20)

## 

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

**Объектом** преступления являются отношения в сфере охраны компьютерной информации.

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

**Информация** (сведения различного характера) содержится в базе данных, которая является объективной формой представления и организации совокупности данных, систематизированных таким образом, чтобы они могли быть найдены и обработаны с помощью ЭВМ. Гибкие диски (дискеты), жесткие диски и компакт-диски позволяют переносить документы и программы с одного компьютера на другой, хранить информацию, не используемую постоянно на компьютере, делать архивные копии информации, содержащейся на жестком диске. [[21]](#footnote-21)

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

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

Обязательный элемент объективной стороны данного **состава - последствия.** [[22]](#footnote-22)

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

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

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

**Копирование информации -** создание копий файлов и системных областей дисков.

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

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

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

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

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

Совершение преступления **группой** лиц по предварительному сговору будет иметь место, когда неправомерный доступ осуществили два лица, заранее договорившиеся о совместном его совершении.[[23]](#footnote-23)

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

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

## 

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

**Объектом** преступления являются отношения в сфере обеспечения компьютерной безопасности.

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

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

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

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

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

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

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

**С субъективной стороны** преступление может быть совершенно как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям. При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил виновный, а когда наступили последствия, к достижению которых он стремился, - и зависимости от наступивших последствий. Лицо сознает, что создает программу, зараженную "вирусом", либо внедряет "вирус" в чужую программу или распространяет и использует его, и желает совершить эти действия. В этом случае действия, предусмотренные ст. 273 УК, оказываются лишь способом достижения поставленной цели. Совершенное деяние подлежит квалификации по совокупности совершенных преступлений.

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

## 

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

**Объектом** преступления являются отношения в сфере обеспечения безопасности. **Объективную сторону** преступления образует нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это причинило существенный вред.

К такого вида нарушениям можно отнести несоблюдение общих средств защиты информации, а также нарушение режима эксплуатации ЭВМ. Выделяют два основных средства защиты: копирование информации и ограничение доступа к информации. Нарушение режима эксплуатации ЭВМ образуют, например, несанкционированные изменение, уничтожение или передача информации. Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети состоит в несоблюдении правил режима их работы, предусмотренных инструкциями, исходящими из технических характеристик, правил внутреннего распорядка, а также правил обращения с компьютерной информацией, установленных собственником или владельцем информации либо законом или иным нормативным актом. Под охраняемой законом информацией следует понимать информацию, изъятую из публичного оборота на основании закона, других нормативных актов, а также правил внутреннего распорядка, основанных на упомянутых нормативных документах. По общему правилу такая информация имеет гриф ограниченного пользования. Представляется, что частные фирмы, включая коммерческие банки, вправе устанавливать ограничительные грифы в целях сохранения коммерческой или банковской тайны. [[24]](#footnote-24)

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

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

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

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

Квалифицирующим признаком ч. 2 ст. 274 УК является наступление **тяжких последствий,** а **субъективная сторона** характеризуется **неосторожной** формой вины по отношению к этим последствиям.[[25]](#footnote-25)

# 4. СПОСОБЫ ЗАЩИТЫ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ОТ ПРЕСТУПНЫХ ПОСЯГАТЕЛЬСТВ

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

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

1. Сбои оборудования:

- сбои кабельной системы;

- перебои электропитания;

- сбои дисковых систем;

- сбои систем архивации данных;

- сбои работы серверов, рабочих станций, сетевых карт и т.д.

2. Потери информации из-за некорректной работы оборудования:

- потеря или изменение данных при ошибках оборудования;

- потери при заражении системы компьютерными вирусами;

3. Потери, связанные с несанкционированным доступом:

- несанкционированное копирование, уничтожение или

подделка информации;

- ознакомление с конфиденциальной информацией,

составляющей тайну, посторонних лиц;

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

5. Ошибки обслуживающего персонала и пользователей:

- случайное уничтожение или изменение данных;

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

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

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

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

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

- административные меры защиты, включающие контроль доступа в помещения, разработку стратегии безопасности фирмы, планов действий в чрезвычайных ситуациях и т.д.[[26]](#footnote-26)

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

Проблема защиты информации от противоправного несанкционированного доступа особо обострилась с широким распространением локальных и, особенно, глобальных компьютерных сетей. Необходимо также отметить, что зачастую ущерб наносится не из-за “злого умысла”, а из-за элементарных ошибок пользователей, которые случайно портят или удаляют жизненно важные данные. В связи с этим, помимо контроля доступа, необходимым элементом защиты информации в компьютерных сетях является разграничение полномочий пользователей.[[27]](#footnote-27)

В компьютерных сетях при организации контроля доступа и разграничения полномочий пользователей чаще всего используются встроенные средства сетевых операционных систем. Так, крупнейший производитель сетевых ОС - корпорация Novell - в своем последнем продукте NetWare 4.1 предусмотрел помимо стандартных средств ограничения доступа, таких, как система паролей и разграничения полномочий, ряд новых возможностей, обеспечивающих первый класс защиты данных. Новая версия NetWare предусматривает, в частности, возможность кодирования данных по принципу “открытого ключа” (алгоритм RSA) с формированием электронной подписи для передаваемых по сети пакетов. В то же время в такой системе организации защиты все равно остается слабое место: уровень доступа и возможность входа в систему определяются специальным известным законным пользователем паролем.

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

- База данных, содержащая информацию по всем сетевым ресурсам,

пользователям, паролям, шифровальным ключам и т.д.

- Авторизационный сервер, обрабатывающий все запросы пользователей на предмет получения того или иного вида сетевых услуг.

Авторизационный сервер, получая запрос от пользователя, обращается к базе данных и определяет, имеет ли пользователь право на совершение данной операции. Примечательно, что пароли пользователей по сети не передаются, что также повышает степень защиты информации.

- Ticket-granting server (сервер выдачи разрешений) получает от авторизационного сервера “пропуск”, содержащий имя пользователя и его сетевой адрес, время запроса и ряд других параметров, а также уникальный сессионный ключ. Пакет, содержащий “пропуск”, передается также в зашифрованном по алгоритму DES виде. После получения и расшифровки “пропуска” сервер выдачи разрешений проверяет запрос и сравнивает ключи и затем дает “добро” на использование сетевой аппаратуры или программ.

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

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

- шифрование данных, передаваемых по линии при помощи генерируемых цифровых ключей;

- контроль доступа в зависимости от дня недели или времени суток (всего 14 ограничений).

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

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

Средства защиты информации нельзя проектировать, покупать или устанавливать до тех пор, пока не произведен соответствующий анализ. Анализ риска должен дать объективную оценку многих факторов (подверженность появлению нарушения работы, вероятность появления нарушения работы, ущерб от коммерческих потерь, снижение коэффициента готовности системы, общественные отношения, юридические проблемы) и предоставить информацию для определения подходящих типов и уровней безопасности. Коммерческие организации все в большей степени переносят критическую корпоративную информацию с больших вычислительных систем в среду открытых систем и встречаются с новыми и сложными проблемами при реализации и эксплуатации системы безопасности. Сегодня все больше организаций разворачивают мощные распределенные базы данных и приложения клиент/сервер для управления коммерческими данными. При увеличении распределения возрастает также и риск неавторизованного доступа к данным и их искажения.[[28]](#footnote-28)

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

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

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

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

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

# Заключение

В связи с бурным процессом развития научно-технической революции сформировался новый вид общественных отношений - информационные. Информационные отношения стали новым объектом, а информация - новым предметом преступного посягательства. Неизбежным следствием появления новых общественных отношений стали правонарушения в сфере компьютерной информации, в том числе и в форме преступлений, которые представляют реальную угрозу для нормального развития и течения общественной жизни.

Преступления в сфере компьютерной информации можно определить как умышленные общественно опасные деяния (действие или бездействие), причиняющие вред либо создающие угрозу причинения вреда общественным отношениям, регламентирующим безопасное производственное хранение, использование или распространение информации и информационных ресурсов либо их защиту.

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

**Видовым объектом** преступлений в сфере компьютерной информации являются информационные отношения, т. е. отношения, возникающие при формировании и использовании информационных ресурсов на основе создания, сбора, обработки, накопления, хранения, поиска, распространения и предоставления потребителю документированной информации; создании и использовании информационных технологий и средств их обеспечения; защите информации, прав субъектов, участвующих в информационных процессах и информатизации.

Вышеуказанные обстоятельства выступают причиной необходимости разработки системы противодействия преступлениям в сфере компьютерной информации, одной из составляющих которой должен выступить неправомерный доступ к охраняемой законом информации. При этом степень уголовно-правовой защиты информации должна определяться её содержанием, а не свойствами носителя.

Таким образом, можно сделать вывод, что существует необходимость совершенствования уголовно-правовой защиты компьютерной информации в связи с постоянно возрастающим значением и широким применением ЭВМ во многих сферах деятельности и наряду с этим повышенной уязвимостью компьютерной информации.

# Библиография

**Нормативные акты**

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (принят ГД ФС РФ 24.05.1996) (ред. от 09.11.2009) (с изм. и доп., вступающими в силу с 17.11.2009)// СЗ РФ.- 1996.- № 25.- Ст. 2954.
2. Указ Президента РФ от 06.03.1997 N 188 (ред. от 23.09.2005) "Об утверждении Перечня сведений конфиденциального характера" // СЗ РФ.- 1997.-№ 10.- Ст. 1127.
3. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (принят ГД ФС РФ 08.07.2006) // СЗ РФ.- 2006.- №31 (1 ч.)- Ст. 3448.

**Литература общего содержания**

Городов О.А. Информационное право: Учебник / О.А. Городов.- Москва: Проспект, 2008.

1. Иванов В.Д. Уголовное право: Общая часть: Учебник / В.Д. Иванов.- Ростов-на-Дону: Феникс, 2002.

Клепицкий, И.А. Уголовное право. Особенная часть: Учеб. пособие для вузов.- М.: ИНФРА-М, 2004.

Копылов В.А. Информационное право. - М.: Юристъ, 2002.

Крылов В.В. Современная криминалистика Правовая информатика и кибернетика - М.: Леке, 2007.

Лапина М.А. Информационное право: Учеб. пособие для вузов / Под ред. И.Ш. Килясханова.- М.: ЮНИТИ-Дана: Закон и право, 2004.

Мельниченко А.Б., С.Н. Радачинский. Уголовное право. Особенная часть.- Ростов-на-Дону, 2002.

Российское уголовное право. Особенная часть / Под ред. Л.В. Иногамовой-Хегай, B.C. Комиссарова, А.И. Рарога. - М.: ИНФРА-М, 2003.

Сверчков В.В. Уголовное право. Особенная часть: Конспект лекций. - М.: Юрайт-Издат, 2007.

**Периодические издания**

Айсанов Р. М. Общественно-опасные последствия неправомерного доступа к компьютерной информации в форме ее уничтожения: уголовно-правовой аспект // "Черные дыры" в Российском Законодательстве. - 2007 .- № 3 .- С. 471-472.

Белоус М. А. Понятие и общая характеристика преступлений в сфере компьютерной информации // "Черные дыры" в Российском Законодательстве. - 2008 .- № 1 .- С. 246-248.

Ведеев Д. Защита данных в компьютерных сетях // Открытые системы.- 2001.- № 3.- С. 12-18.

Галкин А.И. Компьютерная информация как объект правовой защиты // Следователь.- 2009.- №4.- С. 2-5.

Галкин А.И. Уголовная ответственность за преступления в сфере компьютерной информации // Следователь.- 2009.- №5.- С. 2-10.

Ермошин В. Г. Методы защиты конфиденциальной компьютерной информации организаций от внутренних угроз // Вопросы защиты информации. - 2009 .- № 3.- С. 53.

Магомедов М. Д. Некоторые проблемы преступности в сфере компьютерной информации // "Черные дыры" в Российском Законодательстве. - 2009 .- № 1 .- С. 150-151.

1. Саломатина С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом. // Закон и право.- 2009.- №1.- С. 47-48.

Сизов А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. - 2007 .- № 4 .- С. 27.

Сизов А.В. Причины и условия совершения преступлений в сфере компьютерной информации // Информационное право.- 2008 .- № 2 .- С. 38-41.

Талимончик В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Правоведение.- 2008.- №2.- С. 103-110.

1. Хилюта В. «Компьютерные хищения» // Законность.- 2009.- №1.- С. 36-38.

Ястребов Д. А. Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений // Российский следователь .- 2008.- №17 .- С. 25.

Ястребов Д.А. Причины роста компьютерной преступности // Человек и закон.- 2008.- №8.- С. 122-126.

**Интернет-ресурсы**

Васильев В.А. Проблемы развития законодательства в сфере борьбы с киберпреступностью: crime-research.ru

Карелина М.М. Преступления в сфере компьютерной информации // http://www.relcom.ru/ ComputerLaw /New\_code.htm

1. Хилюта В. «Компьютерные хищения» // Законность.- 2009.- №1.- С. 36-38. [↑](#footnote-ref-1)
2. Васильев В.А. Проблемы развития законодательства в сфере борьбы с киберпреступностью: crime-research.ru [↑](#footnote-ref-2)
3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (принят ГД ФС РФ 24.05.1996) (ред. от 09.11.2009) (с изм. и доп., вступающими в силу с 17.11.2009)// СЗ РФ.- 1996.- № 25.- Ст. 2954. [↑](#footnote-ref-3)
4. Галкин А.И. Компьютерная информация как объект правовой защиты // Следователь.- 2009.- №4.- С. 2-5. [↑](#footnote-ref-4)
5. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" (принят ГД ФС РФ 08.07.2006) // СЗ РФ.- 2006.- №31 (1 ч.)- Ст. 3448. [↑](#footnote-ref-5)
6. Лапина М.А. Информационное право: Учеб. пособие для вузов / Под ред. И.Ш. Килясханова.- М.: ЮНИТИ-Дана: Закон и право, 2004 .- С. 113-117. [↑](#footnote-ref-6)
7. Карелина М.М. Преступления в сфере компьютерной информации // http://www.relcom.ru/ ComputerLaw /New\_code.htm [↑](#footnote-ref-7)
8. Крылов В.В. Современная криминалистика Правовая информатика и кибернетика - М.: Леке, 2007. - С. 205-207. [↑](#footnote-ref-8)
9. Копылов В.А. Информационное право. - М.: Юристъ, 2002г.- С. 40-43. [↑](#footnote-ref-9)
10. Талимончик В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Правоведение.- 2008.- №2.- С. 103-110. [↑](#footnote-ref-10)
11. Городов О.А. Информационное право : Учебник / О.А. Городов.- Москва: Проспект, 2008.- С. 69-70. [↑](#footnote-ref-11)
12. Магомедов М. Д. Некоторые проблемы преступности в сфере компьютерной информации // "Черные дыры" в Российском Законодательстве. - 2009 .- № 1 .- С. 150-151. [↑](#footnote-ref-12)
13. Саломатина С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом. // Закон и право.- 2009.- №1.- С. 47-48. [↑](#footnote-ref-13)
14. Сверчков В.В. Уголовное право. Особенная часть: Конспект лекций. - М.: Юрайт-Издат, 2007. - С. 232-237. [↑](#footnote-ref-14)
15. Сизов А.В. Причины и условия совершения преступлений в сфере компьютерной информации // Информационное право.- 2008 .- № 2 .- С. 38-41. [↑](#footnote-ref-15)
16. Белоус М. А. Понятие и общая характеристика преступлений в сфере компьютерной информации // "Черные дыры" в Российском Законодательстве. - 2008 .- № 1 .- С. 246-248. [↑](#footnote-ref-16)
17. Указ Президента РФ от 06.03.1997 N 188 (ред. от 23.09.2005) "Об утверждении Перечня сведений конфиденциального характера" // СЗ РФ.- 1997.-№ 10.- Ст. 1127. [↑](#footnote-ref-17)
18. Российское уголовное право. Особенная часть / Под ред. Л.В. Иногамовой-Хегай, B.C. Комиссарова, А.И. Рарога. - М.: ИНФРА-М, 2003. - С. 568-572. [↑](#footnote-ref-18)
19. Клепицкий, И.А. Уголовное право. Особенная часть: Учеб. пособие для вузов.- М.: ИНФРА-М, 2004 .- С. 152-154. [↑](#footnote-ref-19)
20. Галкин А.И. Уголовная ответственность за преступления в сфере компьютерной информации // Следователь.- 2009.- №5.- С. 2-10. [↑](#footnote-ref-20)
21. Айсанов Р. М. Общественно-опасные последствия неправомерного доступа к компьютерной информации в форме ее уничтожения: уголовно-правовой аспект // "Черные дыры" в Российском Законодательстве. - 2007 .- № 3 .- С. 471-472. [↑](#footnote-ref-21)
22. Ястребов Д. А. Вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений // Российский следователь .- 2008.- №17 .- С. 25. [↑](#footnote-ref-22)
23. Ястребов Д.А. Причины роста компьютерной преступности // Человек и закон.- 2008.- №8.- С. 122-126. [↑](#footnote-ref-23)
24. Сизов А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. - 2007 .- № 4 .- С. 27. [↑](#footnote-ref-24)
25. Иванов, В.Д. Уголовное право: Общая часть: Учебник / В.Д. Иванов.- Ростов-на-Дону: Феникс, 2002.- С. 191-193. [↑](#footnote-ref-25)
26. Ведеев Д. Защита данных в компьютерных сетях // Открытые системы.- 2001.- № 3.- С. 12-18. [↑](#footnote-ref-26)
27. Ермошин В. Г. Методы защиты конфиденциальной компьютерной информации организаций от внутренних угроз // Вопросы защиты информации. - 2009 .- № 3.- С. 53. [↑](#footnote-ref-27)
28. Мельниченко А.Б., С.Н. Радачинский. Уголовное право. Особенная часть. Ростов-на-Дону, 2002г, С. 298-300. [↑](#footnote-ref-28)