Новосибирский государственный технический университет

Юридический факультет

Кафедра уголовно-правовых дисциплин

**КУРСОВАЯ РАБОТА**

по уголовному праву

**«Преступления в сфере компьютерной информации»**

 Выполнил студент 4 курса

 Макрищева Оксана Юрьевна

 группа ЮФЗ-51в

 Проверил:

 Поляков Сергей Альбертович

**Новосибирск – 2008**

**Содержание**

Введение…………………..…………………………………………………….…3

1. **Правовое регулирование отношений в сфере компьютерной информации**………………………………….……….…………………..5 1.1. Общая характеристика преступлений в компьютерной сфере по современному Российскому уголовному законодательству……………5

###  1.2. Криминалистическая характеристика компьютерных

###  преступлений…..…………………………………………………………..10

 1.3. Общие признаки преступлений в сфере компьютерной

 информации………………………………………………………………..13

1. **Уголовно-правовая характеристика преступлений**

**гл. 28 УК РФ**……………………………………………………………..16

 2.1. ст. 272 Неправомерный доступ к компьютерной информации……16

 2.2. ст. 273 Создание, использование и распространение вредоносных программ……………………………………………………………………21

 2.3. ст.274 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети……………………………………………………………….…………25

1. **Предупреждение компьютерных преступлений** …………..…….29

 Заключение……………………………………………………………………….37

 Список использованных источников и литературы……………………………39

**Введение**

Информационная Эра привела к драматическим изменениям в способе выполнения своих обязанностей для большого числа профессий. Теперь нетехнический специалист среднего уровня может выполнять работу, которую раньше делал высококвалифицированный программист. Служащий имеет в своем распоряжении столько точной и оперативной информации, сколько никогда не имел.

Но использование компьютеров и автоматизированных технологий приводит к появлению ряда проблем для руководства организацией. Компьютеры, часто объединенные в сети, могут предоставлять доступ к колоссальному количеству самых разнообразных данных. Поэтому люди беспокоятся о безопасности информации и наличии рисков, связанных с автоматизацией и предоставлением гораздо большего доступа к конфиденциальным, персональным или другим критическим данным. Все увеличивается число компьютерных преступлений, что может привести, в конечном счете, к подрыву экономики. И поэтому должно быть ясно, что информация - это ресурс, который надо защищать. Ответственность за защиту информации лежит на низшем звене руководства. Но также кто-то должен осуществлять общее руководство этой деятельностью, поэтому в организации должно иметься лицо в верхнем звене руководства, отвечающее за поддержание работоспособности информационных систем.

Еще совсем недавно все, что связано с ЭВМ (компьютерами), было непривычным для широких слоев населения России. Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Другая причина - реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием ЭВМ. Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности. Страны, уже прошедшие период компьютерного переоснащения, накопили свой криминальный опыт. Не исключено, что в Российской Федерации компьютерная преступность имеет высокую степень латентности в связи с общей криминогенной обстановкой и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных познаний.

Ситуация, сложившаяся в обществе, потребовала принятия норм уголовного права, которые предусматривали бы ответственность за совершение преступлений в сфере компьютерной информации.

1. **Правовое регулирование отношений в сфере компьютерной информации**

# Общая характеристика преступлений в компьютерной сфере по современному Российскому уголовному законодательству

Новое 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 именно компьютерной информации (т.е. информации на машинном носителе, в электронно-вычислительной машине, системе ЭВМ или их сети) 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.[[1]](#footnote-1)

Составы компьютерных преступлений приведены в 28 главе УК РФ, которая называется "Преступления в сфере компьютерной информации" и содержит три статьи: "Неправомерный доступ к компьютерной информации" (ст. 272), "Создание, использование и распространение вредоносных программ для ЭВМ" (ст. 273) и "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети" (ст. 274). Совершенно оправданно то, что преступления данного вида помещены в раздел IX "Преступления против общественной безопасности и общественного порядка", т.к. последствия неправомерного использования информации могут быть самыми разнообразными: это не только нарушение неприкосновенности интеллектуальной собственности, но и разглашение сведений о частной жизни граждан, имущественный ущерб в виде прямых убытков и неполученных доходов, потеря репутации фирмы, различные виды нарушений нормальной деятельности предприятия, отрасли и т.д.

Необходимо конкретизировать ряд понятиий и определений, используемых в данной главе УК РФ. Необходимый уровень проработки и разъяснения данных понятий дан известным специалистом в этой области Карелиной М.М.[[2]](#footnote-2)

**Информация -** важно различать информацию как термин обыденной жизни и как правовую категорию. Информация, как таковая, представляет собой категорию идеального, она неосязаема, непотребляема не амортизируется и не может быть объектом правоотношений безотносительно к ее носителю, содержанию, идентифицирующим признакам. В праве под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащихся в информационных системах. Весьма тесно связано с понятием информации и понятие информационных ресурсов, под которыми понимаются отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.

**Компьютерная информация -** введение законодателем в Уголовный кодекс термина компьютерная информация является новшеством. Ранее в Российском законодательстве, регулирующем информационные правоотношения, определения информации как компьютерной не существовало. Вероятней всего, определение компьютерная применительно к информации возникло для отграничения данного объекта посягательства от информационных преступлений, предусмотренных другими разделами Уголовного кодекса РФ. 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 ее использования**.**[[3]](#footnote-3)

**Конфиденциальная информация - понятие** конфиденциальной информации было введено в отечественную правовую практику с принятием Таможенного кодекса Российской Федерации. В ст. 16 приводится точное и емкое определение: конфиденциальная информация — это информация, не являющаяся общедоступной и могущая нанести ущерб правам и законным интересам предоставившего ее лица. В законе Об информации: информатизации и защите информации ст. 2 предлагается другая формулировка: документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.[[4]](#footnote-4)

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как:

* содержащая государственную тайну[[5]](#footnote-5)
* передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений, касающаяся тайны усыновления[[6]](#footnote-6)
* содержащая служебную тайну, коммерческую тайну, банковскую тайну, личную тайну, семейную тайну, информация, являющаяся объектом авторских и смежных прав[[7]](#footnote-7)
* информация, непосредственно затрагивающая права и свободы гражданина или персональные данные и др.

**Информационные ресурсы -** понятие информационных ресурсов, весьма тесно связано с понятием информации, под которыми понимаются отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, в частности, в банках данных ст. 2 Федерального закона Об информации, информатизации и защите информации

**Компьютерное право -** термин компьютерное право возник в промышленно развитых странах в середине нашего столетия в связи с широким использованием средств вычислительной техники и других, связанных с ними технических средств: в различных сферах общественной деятельности и частной жизни и формированием отношений, возникающих в процессе производства и применения новых информационных технологий. В самостоятельную отрасль права оно не выделилось ни в одной стране мира и состоит из нормативно-правовых актов разного уровня, относящихся к различным отраслям права: государственному, административному, гражданскому, уголовному и т.д.

**Неправомерный доступ к компьютерной информации -** в специальной литературе под неправомерным доступом к компьютерной информации понимается несанкционированное собственником информации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ. В. С. Комиссаров ( Д.ю.н., профессор) определяет под неправомерным доступом к компьютерной информации получение возможности виновным лицом на ознакомление с информацией или распоряжения ею по своему усмотрению, совершаемое без согласия собственника либо иного уполномоченного лица. Самостоятельной формой неправомерного доступа являются случаи введения в компьютерную систему, сеть или в определенный массив информации без согласия собственника этого массива или иного лица заведомо ложной информации, которая искажает смысл и направленность данного блока информации.

**Уничтожение информации -** это приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние.

**Блокирование информации -** это создание недоступности, невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства, или выключения реакции какого-либо устройства ЭВМ при сохранении самой информации.

**Модификация информации -** изменение первоначальной информации без согласия ее собственника или иного законного лица.

**Копирование информации -** это снятие копии с оригинальной информации с сохранением ее не поврежденности и возможности использования по назначению.

**Нарушение работы ЭВМ, системы ЭВМ или их сети -** нештатные ситуации, связанные со сбоями в работе оборудования, выдачей неверной информации, отказе в выдаче информации, выходом из строя отключением ЭВМ, элементов системы ЭВМ или их сети и т.д. Однако во всех этих случаях обязательным условием является сохранение физической целости ЭВМ, системы ЭВМ или их сети. Если наряду с названными последствиями нарушается и целостность компьютерной системы, как физической вещи, то содеянное требует дополнительной квалификации по статьям о преступлениях против собственности.

**Машинные носители -** мобильные устройства накопления информации, обеспечивающие взаимодействие ЭВМ с окружающей средой накопители на гибких и жестких, а также записываемых магнитооптических дисках, стримеры и т.д..

**Система ЭВМ -** это совокупность взаимосвязанных ЭВМ и их обеспечения, предназначенная для повышения эффективности их работы.

**Сеть ЭВМ** - совокупность распределенных на какой-либо территории и взаимосвязанных для коллективного пользования ими ЭВМ.

**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:

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

### Криминалистическая характеристика компьютерных преступлений

Криминалистическая характеристика компьютерных преступлений отличается от уже известных преступных посягательств определенной спецификой. В первую очередь в нее должны входить криминалистически значимые сведения о личности правонарушителя, мотивации и целеполагании его преступного поведения, типичных способах, предметах и местах посягательств, а также о потерпевшей стороне. Данные о личности преступника в настоящее время базируется на двух специфических группах информации. Первая из которых включает в себя данные о личности неизвестного преступника как по оставленным им следам, так и по другим источникам с целью установления и приемов его розыска и задержания. Такая информация дает представление об общих свойствах какой-то группы лиц, среди которых может находиться преступник. Вторая же группа включает в себя информацию, полученную с помощью изучения личности задержанного подозреваемого или обвиняемого с целью оценки личности субъекта. Такое разделение на группы данных помогает впоследствии выделить типовые модели категорий преступников, каким-то образом провести типизацию преступников.

«Компьютерных» преступников можно разделить на определенные обособленные группы:

* Лица, в которых сочетаются профессионализм в программировании с элементами фанатизма и изобретательности. По мнению некоторых авторов, эти субъекты воспринимают средства компьютерной техники как определенный вызов своим знаниям и умениям. Здесь присутствует некий спортивный азарт. Именно это чаще всего и становится причиной преступлений. Происходит перерождение любителя-программиста в профессионального преступника.
* Лица, страдающие новым видом психических заболеваний - информационными болезнями или компьютерными фобиями. Эти заболевания вызываются систематическим нарушением информационного режима: информационным голодом, информационными перегрузками и т.д. Изучением данного вопроса занимается новая отрасль медицины – информационная медицина. Обычно преступление совершается без наличия преступного умысла. И преступлением чаще всего является повреждение или уничтожение средств компьютерной техники. По моему мнению, при наличии подобных фактов необходимо заключение судебно-психиатрической экспертизы на предмет вменяемости преступника в момент совершения преступления. Так как во время совершения преступления происходит в какой-то степени потеря контроля над своими действиями.
* Профессиональные «компьютерные» преступники. Здесь присутствуют явно корыстные цели. Преступники данной группы чаще всего входят в состав каких-нибудь преступных образований. Это высококлассные специалисты, которые представляют явную угрозу для общества.

Последних можно разделить еще на 2 группы по категориям доступа к средствам компьютерной техники:

* *Внутренние* пользователи (лица, которые имеют непосредственный доступ к необходимой информации)
* *Внешние* пользователи (субъекты, которые обращаются к информационной системе или посреднику за получением необходимой им информации)

По мнению специалистов, подавляющее число преступлений совершается именно внутренними пользователями (обычно это рабочие и служащие фирм и компаний). Внешние пользователи – это лица, которые хорошо осведомлены о деятельности потерпевшей стороны. Круг внешних пользователей настолько широк, что не поддается никакой систематизации и классификации (ими может быть практически любой человек).

Теперь можно рассмотреть мотивы и цели совершения преступлений. По этому вопросу в настоящее время можно выделить 5 наиболее распространенных мотивов совершения преступлений, которые я расположил в рейтинговом порядке:

* Корыстные соображения – 66% (преступления совершаются лицами третьей группы, которую я выделил раньше)
* Политические цели – 17% (шпионаж и т.д. Совершаются только преступниками третьей группы)
* Исследовательский интерес – 7% (совершаются лицами первой группы)
* Озорство и хулиганские побуждения – 5% («хакеры», преступники первой группы)
* Месть – 5% (преступники первой и второй групп)

«Хакеры» – это пользователи компьютерных систем, которые занимаются поиском незаконного доступа к средствам компьютерной техники. В народе это прозвище вызывает ассоциацию с «компьютерными хулиганами».

Также в настоящее время можно выделить некоторые преступные цели, для достижения которых преступники использовали средства компьютерной техники: подделка счетов, фальсификация платежных документов, хищение наличных или безналичных денежных средств, отмывание денег, незаконное получение кредитов и т.п. При этом большинство преступлений связано с хищением денег, а немного меньше – с повреждением или разрушением средств компьютерной техники.

Что же касается потерпевшей стороны, то в большинстве случаев ей становятся юридические лица (учреждения, организации и предприятия всех форм собственности). Это можно объяснить тем, что в России компьютеризация коснулась пока только сферы хозяйственной жизни. Для большинства граждан средства компьютерной техники остаются пока недоступными из-за довольно высокой (по российским меркам) цены. Но, я думаю, процесс компьютеризации скоро заполнит и общественную жизнь страны, как, например, в США.

### Общие признаки преступлений в сфере компьютерной информации

 **Общим объектом** компьютерных преступлений будет выступать совокупность всех общественных отношений, охраняемых уголовным законом; **родовым** - общественная безопасность и общественный порядок; **видовым** - совокупность общественных отношений по правомерному и безопасному использованию информации; **непосредственный объект** трактуется, исходя из названий и диспозиций конкретных статей. Необходимо различать, является ли компьютерная информация только лишь **предметом** преступлений такого вида или же она может выступать и их **средством**, когда электронно-вычислительная техника используется с целью совершения другого противоправного посягательства на иной объект. Последняя точка зрения высказывалась ранее некоторыми авторами[[8]](#footnote-8).

Принятие ее означало бы излишнее расширение рамок понятия "компьютерное преступление" и затруднить работу не только законодателя, но прежде всего правоприменителя.

 Разработчики УК РФ пошли по первому пути, четко сформулировав составы главы 28 таким образом, что Компьютерная Информация в каждом случае является только предметом совершения компьютерного преступления.

 Но представляется правильным и следующее - при использовании компьютерной информации в качестве средства совершения другого преступления отношения по ее охране страдают неизбежно, т.е. она сама становится предметом общественно опасного деяния. Невозможно противоправно воспользоваться компьютерной информацией для совершения иного преступления, не нарушив при этом ее защиты, т.е. не совершив одного из действий, перечисленных в ст. 20 Федерального закона "Об информации, информатизации и защите информации": утечки, утраты, искажения, подделки, уничтожения, модификации, копирования, блокирования и других форм незаконного вмешательства в информационные ресурсы и системы.

Практически все анализируемые преступления относятся к преступлениям средней тяжести, т.е. их максимальная наказуемость в виде лишения свободы не превышает 5 лет. Исключением является лишь создание использование и распространение вредоносных программ для ЭВМ, повлекшее по неосторожности тяжкое последствие, которое наказывается лишением свободы на срок от 3 до 7 лет и поэтому относится к тяжким преступлениям. При характеристике объективной стороны рассматриваемых составов, отмечается, что большинство из них конструктивно сформулированы как материальные, поэтому предполагают не только совершение общественно опасного деяния, но и наступление общественно опасных последствий, а также установление причинной связи между этими двумя признаками. Однако в силу ч. 2 ст. 9 временем совершения каждого из этих преступлений будет признаваться время окончания именно деяния независимо от времени наступления последствий. Сами же общественно опасные деяния чаще всего выступают здесь в форме действий и лишь иногда — как бездействие. В одном случае такой признак объективной стороны состава преступления, как способ его совершения, сформулирован в качестве обязательного признака основного и квалифицированного составов. В остальных он, а также время, место, обстановка, орудия, средства совершения преступления могут быть учтены судом в качестве смягчающих или отягчающих обстоятельств.

Из всех признаков субъективной стороны значение будет иметь только один — вина. При этом, исходя из ч. 2 ст. 24, для всех преступлений данного вида необходимо наличие вины в форме умысла, и лишь два квалифицированных состава предусматривают две ее формы, умысел по отношению к деянию и неосторожность в отношении наступивших общественно опасных последствий. Факультативные признаки субъективной стороны так же, как и в вопросе о стороне объективной, не будут иметь значения для квалификации преступления. Так, мотивами совершения таких деяний чаще всего бывают корысть либо хулиганские побуждения, но могут быть и соображения интереса, чувство мести, не исключено совершение их с целью скрыть другое преступление и т.д. Естественно, что особую трудность вызовет проблема отграничения неосторожного и невиновного причинения вреда, что связано с повышенной сложностью и скрытностью процессов, происходящих в сетях и системах ЭВМ.

Субъект нескольких составов является специальным. В остальных случаях им может стать, в принципе, любой человек, особенно если учесть всевозрастающую компьютерную грамотность населения. Ответственность за преступления против компьютерной безопасности наступает с 16 лет ст. 20 УК.

Диспозиции статей 28-й главы описательные, зачастую — бланкетные или отсылочные. Так: для применения ряда их необходимо обратиться к ст. 35 УК, к нормативно-правовому акту об охране компьютерной информации, правилам эксплуатации ЭВМ и т.п.

Санкции — альтернативные, за исключением двух квалифицированных составов, где они — в силу тяжести последствий преступления — «урезаны» до относительно-определенных.

1. **Уголовно-правовая характеристика преступлений гл. 28 УК РФ**

### ст. 272 «Неправомерный доступ к компьютерной информации»

 Статья 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации (информации на машинном носителе, к которому относятся гибкие магнитные диски, магнитно – оптичиские диски, перфокарты, магнитные ленты либо непосредственно в ЭВМ, системе ЭВМ или их сети ), если это повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы вычислительных систем.

 Данная статья защищает право лиц на неприкосновенность информации в системе. Владельцем информационной вычислительной системы (и информации в ней) может быть любое лицо, правомерно пользующееся услугами по обработке информации как собственник вычислительной системы (ЭВМ, сети ЭВМ) или как лицо, приобретшее право использования системы (информации). Данная статья защищает компьютерную информацию любых предприятий, учреждений, организаций и частных лиц. Диспозиция соответствующей нормы заключается в неправомерном доступе к охраняемой законом компьютерной информации.

 Неправомерным является доступ, противоречащий действующим правовым нормам, актам управления, приказам, распоряжениям и иным актам, регулирующим отношения по доступу лиц (группы лиц) к информации.[[9]](#footnote-9) Кроме того, неправомерным будет доступ, если лицо незаконно использовало технические средства для проникновения в ЭВМ и (или) ее сеть, например введение чужого пароля либо снятие необходимого пароля, модификация программы и пр. Под неправомерным доступом к охраняемой законом компьютерной информации следует понимать также самовольное получение информации без разрешения ее собственника или владельца. [[10]](#footnote-10)

 Эта статья, состоящая из 2-х частей, содержит достаточно много признаков, обязательных для объекта, объективной и субъективной сторон состава преступления.

 Мотивы и цели данного преступления могут быть любыми. Это и корыстный мотив, месть, зависть, цель получить какую-либо информацию, желание причинить вред, желание проверить свои профессиональные способности или самоутвердится.[[11]](#footnote-11)

**Предмет преступления** - компьютерная информация. Диспозиция статьи, указывая на это, требует четкого понимания рассмотренных ранее дефиниций - ЭВМ (компьютер), Сеть, Система Компьютеров, Носитель информации и т.д.

Как уже отмечалось, **состав преступления** сформулирован как материальный, причем деяние определено в форме действия и предполагается обязательное наступление одного из следующих последствий:

* уничтожения информации
* блокирования информации
* модификации информации
* копирования информации
* нарушения работы ЭВМ, системы ЭВМ или их сети, что может выразиться в нарушении работы как отдельных программ, баз данных, выдаче искаженной информации, так и нештатном функционировании аппаратных средств и периферийных устройств, либо нарушении нормального функционирования сети. [[12]](#footnote-12)

 Важным является установление причинной связи между несанкционированным доступом и наступлением последствий. При функционировании сложных компьютерных систем возможны уничтожение, блокирование и нарушение работы ЭВМ в результате технических неисправностей или ошибок в программных средствах. В этом случае лицо совершившего неправомерный доступ к компьютерной информации не подлежит ответственности из-за отсутствия причинной связи между действиями и наступившими последствиями.

 Данное преступление считается оконченным в момент наступления предусмотренных в данной статье последствий, те. все действия выполненные до формальной подачи последней команды (как например), будут образовывать состав неоконченного преступления.

**Объект** - общественные отношения, связанные с безопасностью использования компьютерной информации.[[13]](#footnote-13)

**Объективную сторону** данного преступления составляет неправомерный доступ к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем:

* использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты;
* незаконного использования действующих паролей или кодов для проникновения в компьютер, либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя;
* хищения носителей информации, при условии, что были приняты меры их охраны если это деяние повлекло уничтожение или блокирование информации.

 Преступное деяние, ответственность за которое предусмотрено ст. 272 должно состоять в неправомерном доступе к охраняемой законом компьютерной информации, который всегда носит характер совершения определенных действий и может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств позволяющих преодолеть установленные системы защиты; незаконного применения действующих паролей или маскировка под видом законного пользователя для проникновения в компьютер, хищения носителей информации, при условии, что были приняты меры их охраны, если это деяние повлекло уничтожение или блокирование информации.

 Под охраняемой законом информацией понимается информация, для которой законодательно установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая тайна, персональные данные и т.д.[[14]](#footnote-14)

Причем в отношении этой информации системы должны приниматься специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

 Неправомерный доступ к компьютерной информации должен осуществляться умышленно. Совершая это преступление, лицо должно сознавать, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление либо относится к ним безразлично.

**С** **субъективной стороны** преступление характеризуется наличием прямого умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и желание их наступления) или косвенного умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и сознательное допущение их наступления либо безразличное отношение к наступлению последствий).[[15]](#footnote-15) Неправомерный доступ к компьютерной информации - умышленное деяние, поскольку в диспозиции ст.272 УК не указано обратное. Человек, пытающийся получить доступ к информации, должен сознавать, что свободный доступ к информации ограничен, он не имеет прав на доступ к этой информации. Об умысле будут свидетельствовать меры защиты информации от доступа посторонних (коды, пароли и т.п.), которые приходится преодолеть, чтобы получить доступ к информации, вывод на экран дисплея компьютера предупреждающих сообщений, устные уведомления о запрете доступа к информации и т.д.[[16]](#footnote-16)

**Субъектами** данного **преступления** в основном могут являться лица, имеющие опыт работы с компьютерной техникой, и поэтому в силу профессиональных знаний они обязаны предвидеть возможные последствия уничтожения, блокирования, модификации информации либо нарушения работы ЭВМ, системы ЭВМ и их сети.По общему правилу субъектами преступления , предусмотренного ст. 272, может быть лицо, достигшее 16-летнего возраста, однако часть вторая ст.272 предусматривает наличие специального субъекта, совершившего данное преступление. Это совершение деяния:

* группой лиц по предварительному сговору,
* организованной группой,
* лицом с использованием своего служебного положения,
* лицом, имеющим доступ к ЭВМ, их системе или сети.

Например, инженер по ремонту компьютерной техники имеет доступ к ЭВМ в силу своих служебных обязанностей, но вносить какие либо изменения в информацию находящуюся в памяти ЭВМ не имеет права.

 Согласно части 1 статьи санкция основного состава альтернативно предусматривает три вида наказаний: штраф, исправительные работы и лишение свободы. Первый, в свою очередь, может быть двух видов: кратный минимальному размеру оплаты труда (от 200 до 500) и кратный размеру зарплаты или иного дохода осужденного (период от 2 до 5 месяцев). Исправительные работы могут быть назначены в размере от 6 месяцев до 1 года, а лишение свободы - от 6 месяцев до 2 лет.

 Санкция же согласно части 2 статьи ужесточена: в нее введен новый вид наказания (арест на срок от 3 до 6 мес.), размеры остальных увеличены: штраф от 500 до 800 минимальных размеров оплаты труда или зарплаты за период от 5 до 8 месяцев; исправительные работы от 1 года до 2 лет; лишение свободы до 5 лет. При этом надо помнить, что Федеральным законом "О введении в действие Уголовного кодекса Российской Федерации" от 13 июня 1996 г. наказание в виде ареста вводится в действие постепенно, в течение ближайших 5 лет. Все виды наказаний - как ч. 1, так и ч. 2 - основные и не исключают возможность присоединения какого-либо из дополнительных видов, перечисленных в п. п. 2 и 3 ст. 45, кроме штрафа и конфискации имущества.

### ст. 273 «Создание, использование и распространение вредоносных программ»

 Статья 273 предусматривает ответственность за создание и распространение различного рода компьютерных “вирусов” и других программ, которые могут нарушить целостность информации, нарушить нормальную штатную работу компьютера, сети ЭВМ. Статья защищает права владельца компьютерной системы на неприкосновенность и целостность находящейся в ней информации. Необходимо отметить, что эта статья явилась преемницей ст.269 Проекта УК РФ “Создание, использование и распространение вирусных программ”. Смена дефиниций была сделана законодателем осознано, т.к. в случае принятия только вирусов в качестве средства совершения данного преступления произошло бы неправданное смещение в понимании такого средства. Во-первых, компьютерный вирус может быть и безвредным для информации, требующей гарантированной целостности. Во-вторых, существует большое количество типов программ, приводящим к крайне нежелательным последствиям, но они не попадают под традиционное понимание “Компьютерного вируса”.

 Под **вредоносными программами** в смысле ст. 273 УК РФ понимаются программы специально созданные для нарушения нормального функционирования компьютерных программ. Под нормальным функционированием понимается выполнение операций для которых эти программы предназначены, определенные в документации на программу. Наиболее распространенными видами вредоносных программ являются "компьютерные вирусы" и "логические бомбы".

"**Компьютерные вирусы**" - это программы, которые умеют воспроизводить себя в нескольких экземплярах, модифицировать (изменять) программу к которой они присоединились и тем самым нарушать ее нормальное функционирование.

"**Логическая бомба**" - это умышленное изменение кода программы, частично или полностью выводящее из строя программу либо систему ЭВМ при определенных заранее условиях, например наступления определенного времени. Принципиальное отличие "логических бомб" от “компьютерных вирусов” состоит в том, что они изначально являются частью программы и не переходят в другие программы, а компьютерные вирусы являются динамичными программами и могут распространяться даже по компьютерным сетям. Преступление, предусмотренное ст. 273, наиболее опасное из содержащихся в главе 28, что отражено в санкции за него.

 Непосредственным **объектом** данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания.

**Состав** части 1 формальный и предусматривает совершение одного из действий:

* создание программ (очевидно, вернее - "программы") для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части;
* внесение в существующие программы изменений, обладающих аналогичными свойствами;
* использование двух названных видов программ;
* их распространение;
* использование машинных носителей с такими программами;
* распространение таких носителей.

 Хотя данный состав является формальным и не требует наступления каких-либо последствий, уголовная ответственность возникает уже в результате создания программы, независимо от того использовалась эта программа или нет. [[17]](#footnote-17) Однако следует учитывать, что в ряде случаев использование подобных программ не будет являться уголовно наказуемым. Это прежде всего относится к деятельности организаций, осуществляющих разработку антивирусных программ и имеющих лицензию на деятельность по защите информации, выданную Государственной технической комиссией при Президенте.

 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 или внесения изменений в программу.

 Последними, кроме названного компьютерного вируса, могут быть хорошо известные программистам "логическая бомба", "люк", "асинхронная атака" и другие.

 Под использованием либо распространением вредоносных программ или машинных носителей к ним понимается соответственно введение этих программ в ЭВМ, систему ЭВМ или их сеть, а также продажа, обмен, дарение или безвозмездная передача другим лицам.[[18]](#footnote-18)

С **субъективной стороны** состав данного преступления характеризуется виной в форме прямого умысла: когда виновный осознавал общественную опасность своих действий, предвидел возможность либо даже неизбежность наступления опасных последствий, но тем не менее желал эти действия совершить, т.е. создание вредоносных программ заведомо для создателя программы должно привести к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ.

 Использование или распространение вредоносных программ тоже может осуществляться умышленно.

 При установлении прямого умысла в действиях виновного преступление подлежит квалификации в зависимости от цели, которую перед собой ставил последний, или когда наступили последствия - то в зависимости от наступивших последствий. В этом случае действия, предусмотренные статьей окажутся лишь способом достижения поставленной цели и совершенное деяние подлежит квалификации по классической совокупности совершенных преступлений.

 Необходимо также учитывать, что преступление может быть также совершено как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям.

**Субъект** преступления - общий, т.е. субьектом данного преступления может быть любой гражданин, достигший 16 лет.

**Санкция** части 1 предусматривает один основной вид наказания (лишение свободы на срок до 3 лет) и один дополнительный (штраф в размере 200-500 минимальных размеров оплаты труда или зарплаты либо иного дохода лица за период 2-5 мес.).

Частью 2 ст. 273 криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия.

 При этом "тяжкие последствия" - оценочная категория, которая подлежит квалификации судом. Согласно п.8 постановления Пленума Верховного Суда Российской Федерации от 29 апреля 1996 г. N 1 суд, признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (тяжкие или особо тяжкие последствия, крупный или значительный ущерб, существенный вред, ответственное должностное положение подсудимого и др.), не должен ограничиваться ссылкой на соответствующий признак, а обязан привести в описательной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака.[[19]](#footnote-19)

**Санкция** второй части данной статьи - относительно-определенная: лишение свободы на срок от 3 до 7 лет. Таким образом, именно это преступление из всей главы относится к категории тяжких.

## ст. 274. «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»

 Компьютерные системы в настоящее время все больше влияют на нашу жизнь и выход из строя ЭВМ, систем ЭВМ или их сети может привести к катастрофическим последствиям, поэтому законодатель посчитал необходимым установить уголовную ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети. И именно статья 274 УК РФ устанавливает такую ответственность, акцентируя что это деяние должно причинить существенный вред. Целью действия ст. 274 должно быть предупреждение невыполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Данная уголовная норма, естественно, не содержит конкретных технических требований и отсылает к ведомственным инструкциям и правилам, определяющим порядок работы, которые должны устанавливаться специально управомоченным лицом и доводиться до пользователей. Применение данной статьи невозможно для систем публичного доступа, например, глобальной компьютерной сети Internet; ее действие распространяется только на компьютеры и локальные сети организаций.[[20]](#footnote-20)

 В этой статье также считается, что под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим ее правовой защиты, например - государственная, служебная и коммерческая, банковская тайны, персональные данные и т.д. [[21]](#footnote-21)

Данная статья требует чтобы между фактом нарушения и наступившим существенным вредом была установлена причинная связь и полностью доказано, что наступившие последствия являются результатом именно нарушения правил эксплуатации.

 Непосредственный **объект** преступления, предусмотренного этой статьей, - отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, т.е. конкретно аппаратно-технического комплекса.

Под таковыми правилами понимаются,

* во-первых, Общероссийские санитарные нормы и правила для работников вычислительных центров,
* во-вторых, техническая документация на приобретаемые компьютеры,
* в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Нарушение этих правил (несоблюдение, ненадлежащее соблюдение либо прямое нарушение) может быть осуществлено путем как активного действия, так и бездействия.

 Состав части 1 статьи сформулирован как материальный. При этом общественно опасные последствия заключаются в одновременном наличии двух факторов:

* уничтожения, блокирования или модификации охраняемой законом информации ЭВМ;
* вызванного этим существенного вреда.

Необходимо учитывать, что поскольку речь идет о правилах эксплуатации именно ЭВМ, т.е. программно-аппаратной структуры, то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации, а не организационную или правовую.

 Представляется правильным отнесение к таковым следующих: блокировку системы защиты от несанкционированного доступа, нарушение правил электро- и противопожарной безопасности, использование ЭВМ в условиях, не отвечающих тем, которые установлены документацией по ее применению (по температурному режиму, влажности, величине магнитных полей и т.п.), отключение сигнализации, длительное оставление без присмотра и многие другие. Однако все эти действия должны рассматриваться не самостоятельно, а только лишь в связи с угрозой безопасности хранимой в ЭВМ и охраняемой законом информации.

 Правонарушение может быть определено как преступление только при наступлении существенного вреда.

 Определение существенного вреда, предусмотренного в данной статье будет устанавливаться судебной практикой в каждом конкретном случае исходя их обстоятельств дела, однако очевидно, существенный вред должен быть менее значительным, чем тяжкие последствия.

 Слабость правоприменительной практики не дает четкого понимания природы последнего, но все же целесообразно считать допустимым следующее:[[22]](#footnote-22)

Под существенным вредом следует понимать, прежде всего, вред, наносимый информации в ее значимой, существенной части. Это, например, уничтожение, блокирование, модификация ценной информации (относящейся к объектам особой важности, либо срочной, либо большого ее объема, либо трудно восстановимой или вообще не подлежащей восстановлению и т.д.); уничтожение системы защиты, повлекшее дальнейший ущерб информационным ресурсам; широкое распространение искаженных сведений и т.п.

**Вина** выражается в форме прямого или косвенного умысла. Факультативные признаки субъективной (как и объективной) стороны состава преступления могут быть учтены судом в качестве смягчающих или отягчающих ответственность обстоятельств.

**Объективная сторона** данного преступления состоит в нарушении правил эксплуатации ЭВМ и повлекших уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ при условии, что в результате этих действий был причинен существенный вред. [[23]](#footnote-23)

Как уже отмечалось, между фактом нарушения и наступившим существенным вредом должна быть установлена причинная связь и полностью доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными в ст. 272, 273 УК РФ.

**Субъективную сторону** части 1 данной статьи характеризует наличие умысла направленного на нарушение правил эксплуатации ЭВМ. В случае наступления тяжких последствий ответственность по части 2 ст. 274 наступает только в случае неосторожных действий.

 Умышленное нарушение правил эксплуатации ЭВМ, систем ЭВМ и их сети влечет уголовную ответственность в соответствии с наступившими последствиями и нарушение правил эксплуатации в данном случае становится способом совершения преступления. Например, действия технического специалиста больницы поставившего полученную по сетям программу без предварительной проверки (что говорит о преступной неосторожности) на наличие в ней компьютерного вируса, повлекшее нарушение работы ЭВМ (сети ЭВМ) и отказ работы систем жизнеобеспечения реанимационного отделения, повлекшее смерть больного должны квалифицироваться по части 2 ст. 274.

 Представляется, что подобные действия совершенные умышленно должны квалифицироваться как покушение на убийство.

**Субъект** данного преступления - специальный, это лицо в силу должностных обязанностей имеющее доступ к ЭВМ, системе ЭВМ и их сети и обязанное соблюдать установленные для них правила эксплуатации.

**Санкция** части 1 ст. 274 состоит из трех альтернативных видов наказания: лишение права занимать определенную должность или заниматься определенной деятельностью на срок до 5 лет, обязательные работы от 180 до 240 часов и ограничение свободы до 2 лет.

 Часть 2 - состав с двумя формами вины, предусматривающий в качестве квалифицирующего признака наступление по неосторожности тяжких последствий. Содержание последних, очевидно, аналогично таковому для ч. 2 ст. 273. Санкция нормы существенно отличается от предыдущей: только лишение свободы до 4 лет.

## Предупреждение компьютерных преступлений

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

В настоящее время можно выделить три основных группы мер предупреждения компьютерных преступлений

* **Правовые**

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

* Дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны
* Устанавливают и закрепляют права и обязанности собственника на эти объекты
* Определяют правовой режим функционирования средств информационных технологий
* Определяют категории доступа определенных субъектов к конкретным видам информации
* Устанавливают категории секретности данных и информации
* Дают определение и границы правового применения термина «конфиденциальная информация»

Аналогичные законы действуют в западных странах уже более 20 лет.

Решающим законодательным аккордом в этой области можно считать принятие в июне 1996 года Уголовного кодекса РФ, устанавливающего уголовную ответственность за компьютерные преступления. Информация в нем – объект уголовно-правовой охраны.

* **Организационно-технические меры предупреждения компьютерных преступлений**

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

* соответствие управленческих процедур требованиям компьютерной безопасности;
* разработка вопросов технической защиты компьютерных залов и компьютерного оборудования;
* разработка стандартов обработки данных и стандартов компьютерной безопасности;
* осуществление кадровой политики с целью обеспечения компьютерной безопасности;

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

* пригодность — гарантия того, что сеть пригодна для обеспечения санкционированного доступа;
* контролируемая доступность — гарантия, что сеть обеспечит доступ только санкционированному пользователю для решения санкционированных задач;
* неприкосновенность — защита данных от несанкционированного их изменения и уничтожения;
* конфиденциальность — защита данных от несанкционированного раскрытия;
* безопасность передачи данных — гарантия того, что идентификация пользователей, качество передаваемых данных, время и продолжительность передачи данных обеспечены.

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

* целостность — базовая надежность, гарантирующая, что механизм работает как должно;
* возможность проверки — способность записывать информацию, которая может иметь значение в раскрытии и расследовании попыток посягательства на средства компьютерной техники и других событий, относящихся к вопросам безопасности системы.

В результате практической реализации этих мер стало возможно:

* контролировать физический доступ к средствам компьютерной техники (СКТ);
* . контролировать электромагнитное излучение аппаратных СКТ;
* наблюдать за возможной угрозой СКТ и фиксировать каждую такую попытку (методом мониторинга).

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

* предотвращение утечки, хищения, утраты, искажения и подделки информации;
* предотвращение угроз безопасности личности, общества и государства;
* предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и системы;
* обеспечение правового режима функционирования документированной информации как объекта собственности;
* сохранение государственной тайны и конфиденциальности документированной информации;
* обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

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

1) организационные;

2) технические;

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

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

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

* неконтролируемый доступ сотрудников к пульту управления (клавиатуре) компьютера, используемого как автономно, так и в качестве рабочей станции автоматизированной сети для дистанционной передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;
* бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать указанную в п. 1 ЭВМ в качестве орудия совершения преступления;
* низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;
* несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;
* отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации и ее безопасности в части защиты средств компьютерной техники от несанкционированного доступа;
* отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности, в т. ч. находящейся в форме машинной информации;
* отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

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

* обеспечение поддержки со стороны руководства конкретной организации требований защиты СКТ;
* разработка комплексного плана защиты информации;
* определение приоритетных направлений защиты информации в соответствии со спецификой деятельности организации;
* составление общей сметы расходов финансирования охранных мероприятий в соответствии с разработанным планом и угверждение ее в качестве приложения к плану руководством организации;
* определение ответственности сотрудников организации за безопасность информации в пределах установленной им компетенции путем заключения соответствующих договоров между сотрудником и администрацией;
* разработка, внедрение и контроль за исполнением раз личного рода инструкций, правил и приказов, регламентирующих формы допуска, уровни секретности информации, конкретных лиц, допущенных к работе с секретными (конфиденциальными) данными и т. п.;
* разработка эффективных мер борьбы с нарушителями защиты СКТ.

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

Технические меры представляют собой применение различных устройств специального назначения:

* Источники бесперебойного питания.
* Устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находится компьютерная техника.
* Устройства комплексной защиты телефонии.
* Устройства пожарной защиты.
* Средства защиты портов компьютера.

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

* общий (безусловно предоставляемый каждому пользователю);
* отказ (безусловный отказ, например разрешение на удаление порции информации);
* зависимый от события (управляемый событием), предусматривает блокировку обращения пользователя, например в определенные интервалы времени или при обращении к компьютерной системе с определенного терминала;
* зависимый от содержания данных (в этом случае решение о доступе основывается на текущем значении данных, например некоторому пользователю запрещено читать те или иные данные);
* зависимый от состояния (динамического состояния компьютерной системы), осуществляется в зависимости от текущего состояния компьютерной системы, управляющих программ и системы защиты, например может быть запрещен доступ к файлу, если носитель машинной информации не находится в состоянии «только чтение» либо пока не будет открыт логический диск, содержащий этот файл;
* частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз — таким образом предотвращается возможность динамического управления событиями);
* по имени или другим признакам пользователя (например, пользователю должно быть более 18 лет);
* зависимый от полномочий (предусматривает обращение пользователя к данным в зависимости от режима: только чтение, только выполнение и т.д.)
* зависимый от предыстории обращения
* по разрешению (по паролю)

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

**Заключение**

В ходе изучения действующего уголовного законодательства в области регулирования компьютерного права и специфики расследования преступлений в сфере компьютерной информации были сделаны определенные обобщения:

Преступления в области компьютерной информации являются частью информационных преступлений, объединенных единым инструментом обработки информации — компьютером. Практически все преступления относятся к преступлениям средней тяжести. Исключением является лишь преступления: квалифицируемые ч.2 ст.273, относящиеся к тяжким преступлениям. Для всех преступлений данного вида необходимо наличие вины в форме умысла. Субъектом преступления может стать любой человек старше 16 лет, особенно если учесть всевозрастающую компьютерную грамотность населения.

Известные на сегодня способы совершения компьютерных преступлений отличаются значительным, и постоянно расширяющимся разнообразием. Совершают преступления данной категории чаще всего люди со специальной подготовкой в области автоматизированной обработки информации, причем более половины из их числа в составе преступных групп. Основная опасность исходит от внутренних пользователей — ими совершается более 90 преступлений.

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.

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

Преступления в сфере компьютерной информации имеют, на мой взгляд, как бы двоякий смысл, и поэтому требуют специальных статей в Уголовном кодексе. Уголовный кодекс содержит целую главу, включающую в себя три статьи, что, на мой взгляд, несколько мало. Даже исходя из дословного толкования, позволю себе сказать, что они уже несколько устарели по смысловому значению, и требуют обновлений.

**Список использованных источников и литературы**

1. Конституция Российской Федерации: принята всенародным голосованием 12 декабря 1993г.
2. Гражданский кодекс РФ (Федеральный закон принят Государственной Думой 21.10.94г.)
3. Уголовный кодекс РФ (Федеральный закон принят Государственной Думой 24.05.96г.)
4. Наумов А.В. Комментарий к Уголовному кодексу. – М.: Юристъ, 1997;
5. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"
6. Закон "О государственной тайне" от 21 июля 1993 г. N 5485-1
7. Крылов В.В. Информационные компьютерные преступления. М.: ИнфраМ-Норма, 1997.
8. Карелина М.М. Преступления в сфере компьютерной информации, Москва,1998
9. Н. Селиванов. Проблемы борьбы с компьютерной преступностью. - Законность, 1993, No. 8, с. 37.
10. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10)
11. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1)
12. "Компьютеризация и уголовное право" (В.В. Голубев, "Законодательство", 1999 г., N 8)
1. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1) [↑](#footnote-ref-1)
2. Карелина М.М. Преступления в сфере компьютерной информации, М. 1998 http://www.relcom.ru/ComputerLaw/New\_code.htm [↑](#footnote-ref-2)
3. В.Крылов, “Российская юстиция” №4, 1997г. [↑](#footnote-ref-3)
4. Указ Президента РФ Об утверждении перечня сведений конфиденциального характера» от 06.03.97г. N188 [↑](#footnote-ref-4)
5. Закон РФ О государственной тайне ст.ст. 275, 276, 283, 284 УК РФ [↑](#footnote-ref-5)
6. ч. 2 ст. 23 Конституции РФ, УК РФ (ст.138, ст.155) [↑](#footnote-ref-6)
7. ГК РФ (ст. 139), УК РФ (ст.183, 137, 146, 140) [↑](#footnote-ref-7)
8. Н. Селиванов. Проблемы борьбы с компьютерной преступностью. - Законность, 1993, No. 8, с. 37. [↑](#footnote-ref-8)
9. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-9)
10. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-10)
11. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-11)
12. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1) [↑](#footnote-ref-12)
13. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-13)
14. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" [↑](#footnote-ref-14)
15. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-15)
16. "Ответственность за неправомерный доступ к компьютерной информации" (Кочои С., Савельев Д., "Российская юстиция", 1999, N 1) [↑](#footnote-ref-16)
17. "Компьютеризация и уголовное право" (В.В. Голубев, "Законодательство", 1999 г., N 8) [↑](#footnote-ref-17)
18. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-18)
19. "Преступления в сфере компьютерной информации" (Гульбин Ю., "Российская юстиция", 1997, N 10) [↑](#footnote-ref-19)
20. "Компьютеризация и уголовное право" (В.В. Голубев, "Законодательство", 1999 г., N 8) [↑](#footnote-ref-20)
21. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" [↑](#footnote-ref-21)
22. Карелина М.М. Преступления в сфере компьютерной информации,М 1998 [↑](#footnote-ref-22)
23. Постатейный Комментарий к Уголовному кодексу РФ 1996 г. (под ред. Наумова А.В.) [↑](#footnote-ref-23)