**СОДЕРЖАНИЕ**

ВВЕДЕНИЕ …………………………………………..………………………..….3

 1. ПРАВОВОЙ АНАЛИЗ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ………………………….……..….….….6

 1.1. Общая характеристика преступлений в сфере компьютерной информации…………………..……………….………………………..............….6

1.2. Информация и информационная безопасность как предмет уголовно- правовой защиты……….......................................................................................10

 2.ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ………………………………….……………………………..16

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

 2.2. Создание, использование и распространение вредоносных программ

 для ЭВМ ………………. ...…………….……...…….…………………..21

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

ЗАКЛЮЧЕНИЕ ...……………………..……………………………………...29

ГЛОССАРИЙ …………………………………..………………………………..31

БИБЛИОГРАФИЧЕСКИЙ СПИСОК ………………..………………………...33

ПРИЛОЖЕНИЯ

**ВВЕДЕНИЕ**

Выбранная мною тема бесспорно актуальна. Об этом свидетельствуют изменения, происходящие в экономической жизни России – создание финансово-кредитной системы; предприятий различных форм собственности оказывают существенное влияние на вопросы защиты информации. Проблемы информационной безопасности постоянно усугубляются процессами проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и, прежде всего вычислительных систем. А так же обширный перечень возможных способов компьютерных преступлений.

Объектом посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением. Квалификация правонарушения зависит от того, является ли компьютер только объектом посягательства или он выступает в роли инструмента.

. Каждый сбой работы компьютерной сети это не только моральный ущерб для работников предприятий и сетевых администраторов. По мере развития технологий электронных платежей, «безбумажного» документооборота и других, серьёзный сбой локальных сетей может просто парализовать работу целых корпораций и банков, что приводит к ощутимым материальным потерям.

Способы преступлений в сфере компьютерной информации чрезвычайно многообразны. Это и несанкционированный доступ к информации, хранящейся в компьютере, и ввод в программное обеспечение «логических бомб», которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему, разработка и распространение компьютерных вирусов, и хищение компьютерной информации. Компьютерное преступление может произойти также из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.

В настоящее время все меры противодействия компьютерным преступлениям можно подразделить на: технические, организационные и правовые. К техническим мерам можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, принятие конструкционных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности и многое другое. К организационным мерам относятся охрана компьютерных систем, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, организацию обслуживания вычислительного центра посторонней организацией или лицами, незаинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство) , возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п.. К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. К правовым мерам относятся также вопросы общественного контроля над разработчиками компьютерных систем и принятие соответствующих международных.

До недавнего времени, а именно до 1 января 1997 года, даты вступления в действие нового Уголовного Кодекса Российской Федерации (УК РФ) , в России отсутствовала возможность эффективно бороться с компьютерными преступлениями. Несмотря на явную общественную опасность, данные посягательства не были противозаконными, т.е. они не упоминались уголовным законодательством. Хотя, еще до принятия нового УК в России была осознана необходимость правовой борьбы с компьютерной преступностью. Был принят ряд законов, которые внесли правовую определенность в явление компьютеризации нашего общества вообще и проблему компьютерной преступности в частности и вместе с другими правовыми актами сформировали пласт, именуемый «законодательством в сфере информатизации», охватывающий в настоящее время несколько сотен нормативно-правовых актов. Непосредственно законодательство России в области информатизации начало формироваться с 1991 года.

Целью данной работы является исследование составов преступлений уголовно-правового характера связанных с информационной безопасностью человека. Информационной безопасностью в компьютерных сетях и программах ЭВМ. Исходя из поставленной цели, необходимо выделить следующие задачи: рассмотреть составы преступлений в сфере компьютерной информации. Попытаться, возможно, полнее раскрыть содержание видов преступлений в сфере компьютерной информации.

Изучив большое количество учебной литературы, в данной работе я решила придерживаться научных, учебных трудов следующих авторов: А. Н. Игнатова и Ю. А. Красикова, Прохорова Л.А. и Прохоровой М.Л.

1. **ПРАВОВОЙ АНАЛИЗ ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**
	1. **Общая характеристика преступлений в сфере компьютерной информации**

Развитие современного общества, основанного на использовании огромного количества самой разнообразной информации, немыслимо без широкого внедрения во все сферы жизни общества электронно-вычислительной техники. Она служит не только для хранения и обработки соответствующей информации на уровне отдельных управленческих или хозяйственных единиц или использования как средства связи между гражданами, но и широко внедряется в целях обеспечения внутренней и внешней безопасности государства. Но развертывание научно-технической революции обусловливает не только коренные прогрессивные изменения в составе факторов экономического развития России, но и негативные тенденции развития преступного мира, приводит к появлению новых форм и видов преступных посягательств. Это ярко проявляется в том, что преступные группы и сообщества начинают активно использовать в своей деятельности новейшие достижения науки и техники. Особую тревогу в этом плане вызывает факт появления и развития в России нового вида преступных посягательств, ранее неизвестных отечественной юридической науке и практике и связанный с использованием средств компьютерной техники и информационно-обрабатывающих технологий, компьютерных преступлений.

Последние потребовали от российского законодателя принятия срочных адекватных правовых мер противодействия этому новому виду преступности. Первыми шагами в этом направлении были: принятие Закона РФ «О правовой охране программ для ЭВМ и баз данных» от 23.09.1992; Федерального закона «Об информации, информатизации и защите информации» от 20.02.1995. Следующим шагом является включение в новый Уголовный кодекс 1996 года специальной главы 28 «Преступления в сфере компьютерной информации».

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

Объект компьютерных преступлений достаточно сложен. В обществе существуют определенные ценностные отношения по поводу использования автоматизированных систем обработки данных. Содержанием этих отношений являются права и интересы лиц, общества и государства относительно компьютерных систем, которые понимаются в качестве подлежащего правовой охране блага. Компьютерные преступления посягают на эти права и интересы, которые и являются видовым (групповым) объектом преступлений в сфере компьютерной информации.

Таким образом, видовым объектом преступлений в сфере компьютерной информации являются общественные отношения, нарушающие формирование и использование автоматизированных информационных ресурсов и средств их обеспечения. Видовой объект является сложным. В него входят в свою очередь другие объекты, направленные на права и законные интересы: а) владельцев (собственников) и пользователей информации, компьютеров, их систем и сетей, средств обеспечения; б) физических и юридических лиц, сведения о которых имеются в автоматизированных информационных ресурсах; в) общества и государства, в том числе и интересов национальной безопасности.[[1]](#footnote-1)

Родовым же объектом является общественная безопасность. Предметом компьютерных преступлений является автоматизированная система обработки данных, которая включает как телесный элемент (ЭВМ и сетевое оборудование), так и элемент не телесный (программы и иная информация).

Объективная сторона компьютерных преступлений характеризуется как действием, так и бездействием. Действие (бездействие) сопряжено с нарушением прав и интересов по поводу пользования компьютерными системами и сетями и, кроме того, совершается во вред иным, более конкретным частным, общественным или государственным благам (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности и конституционному строю).

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

Субъективная сторона компьютерных преступлений в соответствии с буквой закона характеризуется умышленной виной. В ч. 2 ст. 24 УК РФ указано, что деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК. Неосторожная форма вины названа в Особенной части лишь применительно к квалифицированным видам компьютерных преступлений, предусмотренным в ч. 2 ст. 273 УК РФ и ч. 2 ст. 274 УК РФ. Эти преступления имеют две формы вины и согласно ст. 27 УК РФ в целом тоже являются умышленными.

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

Под компьютерной информацией понимается записанные в электронном виде и хранящиеся на машинном носителе или электронно-вычислительной машине сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Преступление в сфере компьютерной информации (компьютерное преступление) - это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных. Которые совершаются во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности и конституционному строю).

* 1. **Информация и информационная безопасность как предмет уголовно-правовой защиты.**

Сегодня нормы, регламентирующие правовые аспекты деятельности электронно-вычислительной техники, предусматриваются в различных отраслях права.

Происходящая компьютеризация на просторах бывшего СССР, в том числе и в России достигла такого уровня, когда общественные отношения в этой сфере объективно требуют надлежащего уголовно-правового регулирования, так как наряду с позитивными она порождает и негативные явления, связанные со злоупотреблениями возможностями и средствами электронно-вычислительной техники.

По свидетельству экспертов из правоохранительных органов, самым лакомым сектором российской экономики для преступников является кредитно-банковская сфера. Анализ совершенных здесь за последнее время преступных деяний с использованием компьютерных технологий, а также неоднократные опросы представителей банковских учреждений позволяют выделить следующие наиболее типичные способы совершения компьютерных преступлений против банков и других финансовых учреждений.

Во-первых, все более распространенными становятся компьютерные преступления, совершаемые путем несанкционированного доступа к банковским базам данных посредством телекоммуникационных сетей.

Во-вторых, за последнее время не отмечено практически ни одного компьютерного преступления, которое было бы совершено одиночкой. Более того, известны случаи, когда организованными преступными группировками нанимались бригады из десятков хакеров, которым предоставлялось отдельное охраняемое помещение, оборудованное по последнему слову вычислительной техники, с тем, чтобы они осуществляли хищение крупных денежных средств путем нелегального проникновения в компьютерные сети крупных коммерческих банков.

В-третьих, большинство компьютерных преступлений в банковской сфере совершается при непосредственном участии самих служащих коммерческих банков.

В-четвертых, все большее число компьютерных преступлений совершается в России с использованием возможностей, которые предоставляет своим пользователям глобальная компьютерная сеть Internet.

Таким образом, проблемы ответственности за преступления в сфере компьютерной информации порождены научно-техническим прогрессом, который и создал основу для возникновения отношений в области использования электронно-вычислительной техники.

Следует отметить, что «В современном мире информация уже давно приобрела товарный характер и выступает в качестве особого объекта договорных отношений, связанных с ее сбором, хранением, поиском, переработкой, распространением и использованием в различных сферах человеческой деятельности».[[2]](#footnote-2)

Существует довольно много критериев классификации информации.

В 1991 году была предложена следующая классификация коммерческой информации, которую можно «условно разделить на два укрупненных блока:

— научно-техническая, технологическая информация;

— деловая информация.

Каждый из них имеет свои разновидности.

Научно-техническая, технологическая информация включает:

— сведения о конструкции машин и оборудования (в том числе схемы и чертежи отдельных узлов, изделий), используемых материалах, их составах (химических и т.п.), методах и способах производства, дизайне и другие сведения о вновь разрабатываемых или производимых изделиях, технологиях, о путях и направлениях модернизации известных технологий, процессов и оборудования;

— программное обеспечение для ЭВМ и др.

Деловая информация включает:

— сведения о финансовой стороне деятельности предприятия (финансовая отчетность, состояние расчетов с клиентами, задолженность, кредиты, платежеспособность), о размере прибыли, себестоимости производимой продукции и др.;

— стратегические и тактические планы развития производства, в том числе с применением новых технологий, изобретений, ноу-хау и т.п.;

— планы и объемы реализации произведений продукции (планы маркетинга, данные о характере и объемах торговых операций, уровнях предельных цен, наличии товаров на складах и т.п.);

— анализ конкурентоспособности производимой продукции, эффективности экспорта и импорта, предполагаемое время выхода на рынок;

— планы рекламной деятельности;

— списки торговых и других клиентов, представителей, посредников, конкурентов; сведения о взаимоотношениях с ними, их финансовом положении, проводимых операциях и объемах, условиях действующих контрактов и др.)».[[3]](#footnote-3)

Из­вестно большое количество разноплановых угроз безопасности информа­ции различного происхождения. В качестве критериев деления множества угроз на классы могут использоваться виды порождаемых опасностей, степень злого умысла, источники проявления угроз и т.д. Все многообразие существующих классификаций может быть сведено к некоторой системной классификации (см. Приложение №1).

Немаловажную роль играет политика информационной политики безопасности.

Политика информационной безопасности (ПИБ) – совокупность законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проек­тные решения в области защиты информации. На основе ПИБ строится управление, защита и рас­пределение критичной информации в системе. Она должна охватывать все особенности процесса обработки информации, определяя поведение ИС в различных ситуациях.

Для конкретной информационной системы политика безопасности долж­на быть индивидуальной. Она зависит от технологии обработки информации, используемых программных и технических средств, структуры организации и т.д. При разработке и проведении политики безопасности в жизнь целесообразно соблюдать следующие прин­ципы:

1) невозможность миновать защитные средства (все информационные потоки в за­щищаемую сеть и из нее должны проходить через систему защиты информации (СЗИ). Не должно быть «тайных» модемных входов или тес­товых линий, идущих в обход экрана);

2) усиление самого слабого звена (надежность любой СЗИ определяется самым сла­бым звеном. Часто таким звеном оказывается не ком­пьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобре­тает нетехнический характер );

3) недопустимость перехода в открытое состояние (при любых обстоятельствах (в том числе нештатных) СЗИ либо полностью выполняет свои функции, либо должна полностью блокировать доступ);

4) минимизация привилегий (предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполне­ния служебных обязанностей);

5) разделение обязанностей (предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это имеет особое значение для предотвращения злонамеренных или неквали­фицированных действий системного администратора);

6) многоуровневая защита (предписывает не полагаться на один защитный рубеж, каким бы надеж­ным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом и, как последний рубеж, – протоколирова­ние и аудит. Эшелонированная оборона способна по крайней мере, задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, суще­ственно затрудняет незаметное выполнение злоумыш­ленных действий);

7) разнообразие защитных средств (рекомен­дует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального зло­умышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой на­выками преодоления СЗИ);

8) Принцип простоты и управляемости информацион­ной системы в целом и СЗИ в особенности определяет возможность формального или неформального дока­зательства корректности реализации механизмов защи­ты. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное админи­стрирование;

9) обеспечение всеобщей поддержки мер безопасно­сти (носит нетехнический характер. Рекомендуется с само­го начала предусмотреть комплекс мер, направленных на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое).

Основу политики безопасности составляет способ уп­равления доступом, определяющий порядок доступа субъектов системы к объектам системы. Название это­го способа, как правило, определяет название полити­ки безопасности.

В настоящее время лучше всего изучены два вида политики безопасности: избирательная и полномочная (мандатная), основанные соответственно на избирательном и пол­номочном способах управления доступом (см. приложение №2).

 Избирательное управление доступом – метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. Мандатное управление доступом – концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности. Кроме того, существует набор требований, усили­вающий действие этих политик и предназначенный для управления информационными потоками в системе.

Следует отметить, что средства защиты, предназна­ченные для реализации какого-либо из названных спо­собов управления доступом, только предоставляют воз­можности надежного управления доступом или информационными потоками. Определение прав дос­тупа субъектов к объектам и/или информационным потокам (полномочий субъектов и атрибутов объектов, присвоение меток критичности и т.д.) входит в компе­тенцию администрации системы.

1. **ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ**
	1. **Неправомерный доступ к компьютерной информации**

Неправомерный доступ к компьютерной информации представляет собой наиболее распространенный тип преступлений в сфере компьютерной информации. Кроме того, является достаточно опасным преступлением, которое приобретает все более угрожающие масштабы. В связи с всеобщей компьютеризацией, сети Internet информация стала доступной практически всем пользователям персональных компьютеров. Данный вид преступления затрагивает интересы всего международного сообщества, причиняет вред и государствам, и народам, и конкретным людям. Поэтому, не случайно данная статья открывает 28 главу Уголовного Кодекса.

Особенность данной статьи состоит в том, предусматривается ответственность за неправомерный доступ к информации, лишь, если она запечатлена на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Из этого можно сделать вывод, что посягательство на информацию, которая предназначена для формирования компьютерной информации, но не была еще перенесена на машинный носитель, не является преступлением.

Объектомнеправомерного доступа к компьютерной информации как преступления являются права на информацию ее владельца и третьих лиц, а также безопасность компьютерной информации, правильная работа электронно-вычислительных машин.

С объективной стороны преступление выражается в неправомерном

доступе к охраняемой законом компьютерной информации, хранящейся на машинном носителе или в электронно-вычислительной машине повлекшем уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Под машинными носителями стоит понимать средства хранения информации, позволяющие воспроизводить ее в ЭВМ (магнитные ленты, магнитные диски, магнитные барабаны, полупроводниковые схемы и др., классифицирующиеся по физическим и конструктивным особенностям).

Под доступом к компьютерной информацииподразумевается всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией (уничтожать ее, блокировать, модифицировать, копировать).[[4]](#footnote-4)

В тоже время не образует объективной стороны данного преступления уничтожение или искажение компьютерной информации путем внешнего воздействия на машинные носители теплом, магнитными волнами, механическими ударами и другими аналогичными методами.

Доступ к компьютерной информации считается неправомерным в том случае, если лицо не имеет право на доступ к данной информации. Либо лицо имеет право на доступ к данной информации, однако осуществляет его помимо установленного порядка, с нарушением правил ее защиты.

Преступное деяние, влекущее ответственность, 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; использование чужого имени (пароля). Содержание предпринимаемых действий состоит в получении и реализации возможности распоряжаться информацией по своему усмотрению без права на это.

Из вышеизложенного можно сделать вывод, что неправомерный доступ- это сложное понятие, которое включает в себя такие действия как:

1) «физическое» проникновение, дающее возможность по своему усмотрению оперировать данным объемом компьютерной информации;

2) несанкционированные операции с компьютерной информацией.

Состав по конструкции материальный. Для квалификации деяния по данной статье как оконченного, необходимо наступления хотя бы одного из последствий указанных в исчерпывающем перечне, который дается в части первой статьи, а именно: уничтожение, блокирование, модификацию, копирование информации либо нарушение работы ЭВМ, системы ЭВМ или их сети.

Уничтожение информации - прекращение существования компьютерной информации, т.е. удаление с машинного носителя либо с ЭВМ. В случае, когда у пользователя существует возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности.

Блокирование информации - это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением.

Модификация информации - это внесение в нее любых изменений без согласия ее собственника (владельца), кроме связанных с адаптацией программы для ЭВМ или базы данных. Адаптация программы для ЭВМ или базы данных *—* «это внесение изменений, осуществляемых исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя».[[5]](#footnote-5)

Копирование компьютерной информации - перенос информации на другой машинный или иной носитель. Копирование компьютерной информации может быть осуществлено путем записи содержащегося во внутренней памяти ЭВМ файла на дискету, его распечатки. В то же время копирование компьютерной информации следует рассматривать как неблагоприятное последствие, предусмотренное данной статьей уголовного закона, лишь в том случае, если она охраняется законом именно от несанкционированного копирования.

Нарушение работы ЭВМ, системы ЭВМ или их сети *—* это временное или устойчивое создание помех в функционировании указанных компьютерных средств, т.е. снижение работоспособности отдельных звеньев либо всей ЭВМ.

Непременным признаком объективной стороны является наличие причинной связи между несанкционированным доступом и наступлением предусмотренных статьей 272 УК последствий, поэтому простое временное совпадение момента сбоя в компьютерной системе, которое может быть вызвано неисправностями или программными ошибками и неправомерного доступа не влечет уголовной ответственности.

Субъектом данного преступления может быть только вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста, в том числе и законный пользователь, не имеющий разрешения (допуска) к информации определенной категории.

Неправомерный доступ к компьютерной информации характеризуется

умышленной формой вины. Совершая это преступление, лицо сознает, что неправомерно вторгается в компьютерную систему, предвидит возможность или неизбежность наступления указанных в законе последствий, желает и сознательно допускает их наступление либо относиться к ним безразлично. Преступление характеризуется наличием прямого умысла (осознание неправомерного доступа, предвидение наступления вредных последствий и желание их наступления) или косвенного умысла (предвидение наступления вредных последствий и сознательное допущение их наступления либо безразличное отношение к наступлению последствий).

Данная статья имеет не только основной, но и квалифицированный состав. Квалифицирующими признаками являются совершение деяния группой лиц по предварительному сговору или совершение его организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети (ч.2 ст.272 УК). Понятие совершения преступления в данном случае ничем не отличается от общеупотребительного.

Под использованием служебного положения понимается здесь использование возможности доступа к ЭВМ, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ. В данном случае субъектом преступления не обязательно является должностное лицо.

Лицом, имеющим доступ к ЭВМ, может быть всякий, кто на законных основаниях работает на ней или обслуживает непосредственно ее работу (программисты, сотрудники, вводящие информацию в память ЭВМ, а также администраторы баз данных, инженеры-электрики, ремонтники, специалисты по эксплуатации вычислительной техники и др.). Лица, имеющие доступ в помещение, где расположена ЭВМ, не считаются имеющими доступ к ЭВМ, если они непосредственно не соприкасаются с компьютерной информацией или с устройством оборудования (операторы, охранники, уборщики).

**2.2. Создание, использование и распространение вредоносных программ для ЭВМ**

Общественная опасность создания, использования или распространения вредоносных программ определяется тем, что вредоносные программы способны в самый неожиданный момент парализовать работу компьютерной системы, что может привести к неблагоприятным последствиям.

Объектом данного преступления является безопасность пользования интеллектуальными и вещественными средствами вычислительной техники, а также правильная работа электронно-вычислительных машин.

Объективная сторона данного преступления выражается в противоправном создании, использовании и распространении вредоносных программ для ЭВМ, или внесение вредоносных изменений в существующие программы (создание компьютерных вирусов).

Прежде чем перейти к понятию «создание программы для ЭВМ», необходимо выяснить, что представляет собой непосредственно сама программа для ЭВМ - это объективная форма представления совокупности данных команд, предназначенных для функционирования ЭВМ с целью получения определенного результата.

Создание программы для ЭВМ – написание алгоритма, т.е. последовательность логических команд, с дальнейшим преобразованием его в машинный язык ЭВМ.

Изменение существующих программ – это изменение алгоритма программы, путем исключения его фрагментов, замены их другими, дополнения его, т.е. модификация уже существующей компьютерной программы.

Использование программы ЭВМ - это выпуск ее в свет, воспроизведение и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме, а также самостоятельное применение этой программы по назначению[[6]](#footnote-6).

Распространение программы для ЭВМ - это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, а равно создание условий для самораспространения программы. Распространение машинного носителя с программой для ЭВМ представляет собой передачу на любых условиях третьим лицам. Оно может осуществляться как по компьютерной сети (локальной, региональной или международной), так и через машинные носители путем их продажи, дарения, дачу взаймы и т.п. Ответственность за преступление наступает как для разработчиков вредоносных программ, так и для других пользователей, которые могут применять их, например, в целях защиты своего программного обеспечения и информации от похитителей либо для заражения других ЭВМ.

Вредоносность программ в настоящей статье определяется как способность несанкционированного уничтожения, блокирования, модификации, копирования информации, а также нарушение работы ЭВМ, их системы или сети. Существует три вида атак на информационные системы: а) атаки на уровне систем управления базами данных; б) атаки на уровне операционных систем; в) атаки на уровне сетевого программного обеспечения. Вредоносные программы представляют собой программы, которые содержат вирусы, либо команды. Существуют также программные закладки – несанкционированно внедренная программа, которая осуществляет угрозу информации. Она может вносить произвольные искажения в коды программ, переносить фрагменты информации из одних областей оперативной или внешней памяти в другие, либо искажать выводимую на внешние компьютерные устройства или в канал связи информацию, полученную в результате работы других программ. Не менее опасным являются и «троянские программы», а также клавиатурные шпионы. Данные программы обладают способностью переходить через коммуникационные сети из одной системы в другую, проникать в ЭВМ и распространяться как вирусное заболевание. Вирусная программа — это специальная программа, способная самопроизвольно присоединяться к другим программам (т.е. «заражать» их) и при запуске последних выполнять

различные нежелательные действия: порчу файлов и каталогов, искажение результатов вычислений, засорение или стирание памяти и т.п. В течение определенного периода времени она не обнаруживает себя, но затем компьютер «заболевает» и внешне беспричинно выходит из строя. Чаще всего сбои в работе компьютера сопровождаются полным или частичным уничтожением информации.

 Окончанием данного преступления будет момент создания, использования или распространения вредоносных программ, создающих угрозу наступления указанных в законе последствий вне зависимости от того, наступили реально эти последствия или нет.

Субъектомданного преступления является только вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста. Закон не требует, чтобы это лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование.

С субъективной стороны ст. 273 УК характеризуется прямым либо косвенным умыслом. Виновное лицо сознает, что его действия по созданию, использованию или распространению соответствующих программ носят общественно опасный характер, предвидит возможность или неизбежность наступления несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети и желает их наступления или не желает, но сознательно допускает эти последствия либо относится к ним безразлично. Цели и мотивы действий виновного могут быть различными. Они не обозначены законодателем в качестве признаков данного состава, но их знание необходимо для индивидуализации наказания. В случае, если действие вредоносной программы условием совершения лицом другого преступления, деяния должны быть квалифицированны по совокупности вне зависимости от степени тяжести другого преступления.

Наказывается данное преступление лишением свободы на срок до трех лет со штрафом в размере от двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

«Данное преступление считается квалифицированным, если соответствующие деяния повлекли по неосторожности тяжкие последствия (ч. 2 ст. 273 УК).»[[7]](#footnote-7). Под тяжкими последствиями создания, использования или распространения вредоносных программ для ЭВМ понимаются безвозвратная утрата особо ценной информации, выход из строя важных технических средств (например, систем оборонного назначения, аэронавигационной техники), повлекший несчастные случаи с людьми, аварии, катастрофы. Тяжкие последствия — это оценочное понятие, содержание которого должно определяться судебно следственными органами в каждом конкретном случае с учетом всей совокупности обстоятельств дела, как правило, с привлечением соответствующих экспертов. К тяжким последствиям можно отнести, например, причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование, модификацию или копирование информации особой ценности, например, составляющей государственную тайну и т.п.

Особенностью квалифицированного вида данного преступления является то обстоятельство, что в соответствии с законом субъективное отношение виновного лица к тяжким последствиям может характеризоваться только неосторожной формой вины.

Учитывая характер последствий, законодатель предусматривает в случае совершения квалифицированного вида искомого преступления значительно более суровое наказание в виде лишения свободы на срок от трёх до семи лет.

**2.3. 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 установление определенных правил эксплуатации ЭВМ, системы ЭВМ или их сети преследует цель сохранности информации и компьютерного оборудования, обеспечения возможности их длительного использования в интересах собственников и пользователей. Информация, в отношении которой наступают негативные последствия, должна охраняться законом, о чем уже говорилось ранее.

Объектом рассматриваемого преступления является совокупность общественных отношений, обеспечивающих эксплуатацию ЭВМ, их сети или системы таким образом, что сохраняется их исправность. Кроме того, осуществляется безопасность пользования интеллектуальными и вещественными средствами вычислительной техники.

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.

Объективная сторона выражается в действии или бездействии направленные на нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, которое имеет доступ к ЭВМ, системе ЭВМ или их сети, повлекшем уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

Диспозиция ч.1 ст.274 носит бланкетный характер. Здесь имеется ввиду вся совокупность норм, установленных:1) компетентными государственными органами; 2) изготовителем относительно параметров и условий нормальной работы; 3) разработчиками программ; 4) собственником или иным законным владельцем компьютером, системы или сети[[8]](#footnote-8).

Правила эксплуатации ЭВМ определяются соответствующими техническими нормативными актами. Они также излагаются в паспортах качества, технических описаниях и инструкциях по эксплуатации, передаваемых пользователю при приобретении вещественных средств компьютерной техники (ЭВМ и периферийных устройств), в инструкциях по использованию программ для ЭВМ. Соответствующие инструкции могут излагаться на бумажных и машинных носителях; в последнем случае они обыкновенно встраиваются в программу, которая обеспечивает к ним доступ при желании пользователя. Кроме того, правила могу быть установлены компетентным государственным органом, а также правила, установленные владельцем компьютерной системы или по его полномочию, конкретные, принимаемые в одном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка.

Поэтому нарушение соответствующих правил должно касаться именно технических правил, но никак не организационных форм работы ЭВМ или их правовой регламентации.

Нарушение правил эксплуатации может выражаться в трех формах:

1. в несоблюдении установленных правил, обеспечивающих безопасность эксплуатации ЭВМ, системы ЭВМ или их сети (нарушении правил электро- и противопожарной безопасности, игнорировании предписаний соответствующих инструкций и т.п.);
2. в ненадлежащем соблюдении указанных правил (например, неполном соблюдении параметров работы ЭВМ, нарушении алгоритма программы);
3. в прямом нарушении данных правил, например, в отключении системы защиты от неправомерного доступа.

Нарушение правил эксплуатации компьютерной системы должно повлечь уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, кроме того, причинить существенный вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства.

Под существенным вредом в диспозиции данной нормы уголовного закона понимаются утрата важной информации, перебои в производственной деятельности, необходимость сложного или длительного ремонта средств вычислительной техники, их переналадки, длительный разрыв связей между ЭВМ, объединенными в систему или сеть.

 Существенность вреда оценивается с помощью таких параметров как размер материального ущерба, характер вреда здоровью, объем негативных последствий для пользователей информацией, продолжительность и сложность работ по восстановлению нормальной деятельности ЭВМ, системы или сети и восстановлению утраченной либо искаженной информации.

Оконченным данное преступление является если, во-первых, имело место нарушение правил, во-вторых, оно повлекло уничтожение, блокирование или модификацию компьютерной информации, и наконец, если причинен существенный вред.

Субъектом рассматриваемого преступления является только вменяемое физическое лицо, достигшее ко времени совершения преступления 16-летнего возраста. Закон не требует, чтобы это лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование. Главное, чтобы оно имело доступ к ЭВМ.

Субъективная сторона преступления характеризуется умышленной формой вины. Виновный сознает, что нарушает правила эксплуатации,
предвидит возможность или неизбежность уничтожения, блокирования или модификации охраняемой законом информации и причинения существенного вреда, желает или сознательно допускает причинение такого вреда или относится к его наступлению безразлично.

Наказывается данное преступление лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет, либо обязательными работами на срок от ста-восьмидесяти до двухсот-сорока часов, ли6о ограничением свободы на срок до двух лет.

Часть 2 ст. 274 предусматривает ответственность за те же деяния, повлекшие по неосторожности тяжкие последствия. Под тяжкими последствиями нарушения правил эксплуатации ЭВМ понимаются безвозвратная утрата особо ценной информации, выход из строя важных технических средств (например, систем оборонного назначения, аэронавигационной техники), повлекшие несчастные случаи с людьми, аварии, катастрофы. Наказывается преступление в этом случае лишением свободы на срок до четырех лет.

**ЗАКЛЮЧЕНИЕ**

Время, в которое мы живем, характеризуется крайней интенсивностью развития всех форм общественной деятельности, в том числе политической жизни и предпринимательства. Одни политики быстро сменяют других, одни бизнесмены мгновенно зарабатывают состояние, другие — разоряются. Страницы периодической печати пестрят сообщениями о мошенничествах, крупных махинациях, злоупотреблением служебным положением, вымогательстве, воровстве, заказных убийствах предпринимателей и т. д. Все эти неприятные моменты современной жизни объединяет одно — в основе каждого преступления лежит добытая тем или иным путем конфиденциальная информация, без обладания которой порой совершить преступление или избежать наказания невозможно.

В уголовном законодательстве сделана первая попытка реализации уголовно-правовой политики в новой для нее области - сфере компьютерных правоотношений. Насколько она является успешной, на сколько эффективно может защитить права заинтересованных лиц – все это зависит от многих факторов политического, экономического, научно-технического, организационного характера.

Хотелось бы подчеркнуть, что абсолютную надёжность и безопасность в компьютерных сетях не смогут гарантировать никакие аппаратные, программные и любые другие решения. Хотя в наши дни люди обеспокоены проблемой компьютерной безопасности, в защитной броне любой системы существует немало прорех. Системные администраторы могут бесконечно усиливать защиту, но способ обойти ее все равно найдется. Существует так называемое правило хакерства: то, до чего додумался один человек, додумается и другой, что один скрыл — другой раскроет. Но в тоже время возможно свести риск потерь при комплексном подходе к вопросам безопасности

В заключении хотелось бы сказать о том, что на сегодняшний день уголовное законодательство в сфере компьютерной информации не идеально. Предусмотренные составы компьютерных преступлений не охватывают полностью всех видов компьютерных посягательств, которые совершаются на сегодняшний день.

Из вышеизложенного можно сделать выводы о том, что сложность компьютерной техники, неоднозначность квалификации, а также трудность сбора доказательственной информации привод к тому, что большинство компьютерных преступлений остаются безнаказанными. В настоящее время уголовный кодекс РФ предусматривает всего лишь три состава преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных программ для ЭВМ; нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети, что естественно не охватывает всех видов преступлений в данной сфере.

В связи с этим думается, что было бы целесообразно с учетом новейших технологий и мнений специалистов в области компьютерных технологий на законодательном уровне расширить состав преступлений, которые предусматривают ответственность за другие виды общественно -опасных деяний в сфере компьютерной информации.

**ГЛОССАРИЙ**

|  |  |  |
| --- | --- | --- |
| №п/п |  Новые понятия | Содержание |
| 1. | Блокирование информации | это искусственное затруднение доступа пользователей к компьютерной информации, не связанное с ее уничтожением. |
| 2. | Доступ к компьютерной информации | подразумевается всякая форма проникновения к ней с использованием средств (вещественных и интеллектуальных) электронно-вычислительной техники, позволяющая манипулировать информацией  |
| 3. | Избирательное управление доступом  | метод управления доступом субъектов системы к объектам, основанный на идентификации и опознавании пользователя, процесса и/или группы, к которой он принадлежит. |
| 4. | Изменение существующих программ | это изменение алгоритма программы, путем исключения его фрагментов, замены их другими, дополнения его, т.е. модификация уже существующей компьютерной программы. |
| 5. | Использование программы ЭВМ | это выпуск ее в свет, воспроизведение и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме, а также самостоятельное применение этой программы по назначению. |
| 6. | Компьютерная информация | записанные в электронном виде и хранящиеся на машинном носителе или электронно-вычислительной машине сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.  |
| 7. | Копирование компьютерной информации | перенос информации на другой машинный или иной носитель. |
| 8. | Мандатное управление доступом | концепция доступа субъектов к информационным ресурсам по грифу секретности разрешенной к пользованию информации, определяемому меткой секретности |
| 9. | Машинные носители | средства хранения информации, позволяющие воспроизводить ее в ЭВМ (магнитные ленты, магнитные диски, магнитные барабаны, полупроводниковые схемы и др., классифицирующиеся по физическим и конструктивным особенностям). |
| 10. | Модификация информации | это внесение в нее любых изменений без согласия ее собственника (владельца), кроме связанных с адаптацией программы для ЭВМ или базы данных. |
| 11. | Нарушение работы ЭВМ, системы ЭВМ или их сети | это временное или устойчивое создание помех в функционировании указанных компьютерных средств, т.е. снижение работоспособности отдельных звеньев либо всей ЭВМ. |
| 12. | Политика информационной безопасности (ПИБ) | совокупность законов, правил, практических рекомендаций и практического опыта, определяющих управленческие и проек­тные решения в области защиты информации. |
| 13. | Преступление в сфере компьютерной информации (компьютерное преступление) | это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в отношении автоматизированных систем обработки данных. Которые совершаются во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства (личным правам и неприкосновенности частной сферы, имущественным правам и интересам, общественной и государственной безопасности и конституционному строю). |
| 14. | Распространение программы для ЭВМ | это предоставление доступа к воспроизведенной в любой материальной форме программе для ЭВМ, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, а равно создание условий для самораспространения программы. |
| 15. | Создание программы для ЭВМ | написание алгоритма, т.е. последовательность логических команд, с дальнейшим преобразованием его в машинный язык ЭВМ. |
| 16. | Уничтожение информации | прекращение существования компьютерной информации, т.е. удаление с машинного носителя либо с ЭВМ. |

**БИБЛИОГРАФИЧЕСКИЙ СПИСОК**

1. **Нормативно-правовые акты:**
2. Конституция Российской Федерации от 12.12.93 г.
3. Уголовный кодекс РФ от 13 июня 1996 г. №63-ФЗ (с изм. и доп. на

 05. 07.2006 г.)

1. Федеральный Закон РФ «О правовой охране программ для ЭВМ и баз данных» от 23.09.1992г. (в ред. от 02.11.2004 г.)
2. Федеральный закон «Об информации, информатизации и защите информации» от 20.02.1995г.

**2. Научная, учебная литература:**

1. Ветров Н.И. Уголовное право. Общая и особенная части. Учебное пособие. - М.: Книжный Мир, 2000 (2-е изд.).
2. Гражданское право. Часть I. Учебник. Под ред. Ю.К. Толстого, А.П. Сергеева. - М.: «Издательство ТЕИС», 1996.
3. Егоров В.С. Особенная часть уголовного права. Учебное пособие. Альбом схем. - М.: МПСИ, 1998.
4. Комментарий к Уголовному кодексу РФ / Под ред. Ю.И. Скуратова и В.М. Лебедева. М-1999г. изд. группа ИНФРА.
5. Курс уголовного права: Особенная часть. Т. 3-5 / Под ред.
Г.Н. Борзенкова, В.С. Коммисарова. - М.: Зерцало-М, 2002.
6. Максимов В.Ю. Компьютерные преступления (Вирус. аспект). Ставрополь: Кн. изд-во, 1999.
7. Миньковский Г.М. , Магомедов А.А., Ровин В.П. Уголовное право России. Учебник. Общая и Особенная части. М. 1998г. Изд. «Бандес», «Альянс».
8. Основы защиты коммерческой информации и интеллектуальной собственности в предпринимательской деятельности. Под ред. А.В. Назарова. - М.: «Научно-информационная внедренческая фирма «ЮКИС», 1991.
9. Прохоров Л.А., Прохорова М.Л.Уголовное право: Учебник. — М.: Юристъ, 1999.
10. Российское уголовное право. В 2-х томах. Том 2. Особенная часть. / Под ред. А.И. Рарога. - М.: Полиграф Опт, 2002.
11. Уголовное право Российской Федерации. Особенная часть / Под ред. Б.В. Здравомыслова. 2-е изд., - М.: Юристъ, 1999.
12. Уголовное право России: Учебник для вузов. В 2 т. Т. 2. Особенная часть. Под ред. А. Н. Игнатова и Ю. А. Красикова. — М.: Издательство «НОРМА» (Издательская группа НОРМА-ИНФРА М), 2000.

**ПРИЛОЖЕНИЕ 1**

**Системная классификация угроз безопасности информации**

|  |  |  |
| --- | --- | --- |
| Критерии классификации | Значение критериев | Содержание значения критериев |
| 1. Виды угроз  | 1.1. Физическая целостность1.2. Логическая структура1.3. Содержание1.4. Конфиденциальность1.5. Право собственности | Уничтожение (искажение).Искажение структуры.Несанкционированная модификация.Несанкционированное получение.Присвоение чужого права. |
| 2. Природа происхождения угроз | 2.1. Случайная2.2. Преднамеренная | Отказы, сбои, ошибки, стихийные бедствия, побочные влияния.Злоумышленные действия людей. |
| 3. Предпосылки появления угроз | 3.1. Объективные3.2. Субъективные | Количественная недостаточность элементов системы, качественная недостаточность элементов системы.Разведорганы иностранных государств, промышленный шпионаж, уголовные элементы, недобросовестные сотрудники. |
| 4. Источники угроз | 4.1. Люди4.2. Технические устройства4.3. Модели, алгоритмы, программы4.4. Технологические схемы обработки4.5. Внешняя среда | Посторонние лица, пользователи, персонал.Регистрации, передачи, хранения, переработки, выдачи.Общего назначения, прикладные, вспомогательные.Ручные, интерактивные, внутримашинные, сетевые.Состояние атмосферы, побочные шумы, побочные сигналы. |

**ПРИЛОЖЕНИЕ 2**

**Виды политики безопасности**

Политика безопасности

Мандатная политика

Избирательная политика



Все субъекты и объекты системы должны быть однозначно идентифицированы.

Все субъекты и объекты системы должны быть идентифицированы.

Каждому объекту системы присвоена метка критичности, определяющая ценность содержащийся в нем информации.

Права доступа субъекта к объекту системы определяются на основании некоторого правила свойство избирательности.

Каждому объекту системы присвоен уровень прозрачности, определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

**ПРИЛОЖЕНИЕ 3**

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

Создание, использование и распространение вредоносных программ для ЭВМ

Неправомерный доступ к компьютерной информации

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

 ОБЪЕКТ

 СУБЪЕКТ

ОБЪЕКТИВНАЯ СТОРОНА

сами технические средства (компьютеры и периферия); материальные объекты, программное обеспечение и базы данных, для которых технические средства являются окружением

Вменяемое, физическое лицо, достигшее 16 летнего возраста

Действие (бездействие) повлекшее нарушение прав и интересов по поводу пользования компьютерными системами или сетями.

Умышленная форма вины

СУБЪЕКТИВНАЯ СТОРОНА

1. Миньковский Г.М. , Магомедов А.А., Ровин В.П. Уголовное право России. Учебник. Общая и Особенная части. М. 1998г. Изд. «Бандес», «Альянс». с.388 [↑](#footnote-ref-1)
2. Гражданское право. Часть I. Учебник. Под ред. Ю.К. Толстого, А.П. Сергеева. - М.: «Издательство ТЕИС» 1996. С. 190. [↑](#footnote-ref-2)
3. Основы защиты коммерческой информации и интеллектуальной собственности в предпринимательской деятельности. Под ред. А.В. Назарова. - М.: «Научно-информационная внедренческая фирма «ЮКИС» , 1991. С. 34. [↑](#footnote-ref-3)
4. Уголовное право России**:** Учебник для вузов. Т. 2 Особенная часть**.** Под ред. А. Н. Игнатова и Ю. А. Красикова**.** — М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА М), 2000. [↑](#footnote-ref-4)
5. ч. 1 ст.1 Закона РФ от 23 сентября 1992г. «О правовой охране программ для электронных вычислительных машин и баз данных». [↑](#footnote-ref-5)
6. Уголовное право России**:** Учебник для вузов. Т. 2 Особенная часть**.** Под ред. А. Н. Игнатова и Ю. А. Красикова**.** — М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА М), 2000.с. 358

 [↑](#footnote-ref-6)
7. Уголовное право России**:** Учебник для вузов. Т. 2 Особенная часть**.** Под ред. А. Н. Игнатова и Ю. А. Красикова**.** — М.: Издательство НОРМА (Издательская группа НОРМА-ИНФРА М), 2000. с. 358 [↑](#footnote-ref-7)
8. Миньковский Г.М. , Магомедов А.А., Ровин В.П. Уголовное право России. Учебник. Общая и Особенная части. М. 1998г. Изд. «Бандес», «Альянс». с.396 [↑](#footnote-ref-8)