# Основные данные о работе

|  |  |
| --- | --- |
| Версия шаблона | 1.1 |
| Филиал | Брянский |
| Вид работы | Курсовая работа |
| Название дисциплины | Уголовное право |
| Тема | Понятие преступлений в сфере компьютерной информации |
| Фамилия студента | Короткевич |
| Имя студента | Игорь |
| Отчество студента | Аркадьевич |
| № контракта | 02515070101011 |
| Файл титульного листа |  |

# Содержание

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

1 Понятие и признаки компьютерных преступлений…..…..……………………5

1.1. Понятие и общая характеристика преступлений в сфере компьютерной информации………..……………………...……………………………………………….5

1.2. Общие признаки преступлений в сфере компьютерной информации…..……………………………………………………………………………9

2 Виды компьютерных преступлений…..….……………………………………15

2.1 Неправомерный доступ к компьютерной информации…………………………………………………………...………..………...15

2.2 Создание, использование и распростра­нение вредоносных программ для ЭВМ………………………….……………………………………...……………………18

Заключение………………………………………………………………………...27

Глоссарий………………...….………………………………….…………………30

Список использованных источников…………………………………………….32

Приложения...……………………………………………………………………..34

# Введение

Стремительное развитие компьютерных технологий и широкое использование электронно-вычислительных систем практически во всех сферах жизнедеятельности человека поставили многочисленные проблемы в области правового регулирования отношений, связанных с компьютеризацией общества. Это дает основание поставить вопрос о формировании отрасли компьютерного права, одним из основных аспектов которой являются так называемые компьютерные посягательства. Об актуальности проблемы свидетельствует обширный перечень возможных способов компьютерных преступлений.

Объектами посягательств могут быть сами технические средства (компьютеры и периферия) как материальные объекты, программное обеспечение, базы данных и информация, как таковая.

А сами преступления, где применяются компьютерные технологии, чрезвычайно многогранны и сложны, например, это может быть:

перехват конфиденциальных сигналов пейджинговых и сотовых станций, подделка кредитных карт,

– несанкционированный доступ к информации;

– ввод в программное обеспечение «логических бомб»;

– которые частично или полностью выводят из строя компьютерную систему;

– разработка и распространение компьютерных вирусов;

– хищение компьютерной информации и многое другое.

Одним из наиболее распространенных видов компьютерных посягательств является неправомерный доступ к компьютерной информации. Такие преступления чаще посягают на охраняемую законом информацию и совершаются с умыслом на добычу и неправомерное использование ее в корыстных целях. У данного вида компьютерных преступлений большой потенциал в виду того, что информация растущими темпами приобретает характер основного ресурса человеческой деятельности и опасность неправомерного доступа к ней трудно переоценить.

В России научная среда только в начале 90-х приступила к исследованию компьютерной преступности и на данный момент степень научной разработанности проблемы в отечественное литературе весьма невысока. За последние годы опубликован ряд работ, посвященных, в основном, криминологическим и криминалистическим аспектам компьютерных преступлений.

Уголовно-правовые же аспекты компьютерных правонарушений в настоящее время выражены в научной литературе гораздо слабее. В монографиях и статьях, в основном, затрагивается вопрос об объекте, предмете, орудиях совершения компьютерного деликта и их соотношение между собой. Некоторые работы содержат конструктивную критику главы 28 УК РФ, как с уголовно-правовой, так и с информационной точки зрения.

Но не только в теории, но и на практике в нашей стране нечем было отреагировать на волну компьютерных преступлений.

Преступный мир всегда опережал на шаг вперед правоохранительную систему, беря на вооружение все лучшее, что могло придумать общество, когда как второй, приходилось на ходу изменять средства борьбы с первым. Но даже при имеющихся средствах и методах, борьба с компьютерной преступностью проходит на крайне низком уровне. Причинами недостаточно высокой эффективности работы следственного аппарата и органов внутренних дел по раскрытию компьютерных преступлений являются некомпетентность сотрудников в юридической и технической стороне таких преступлений, слабая научно-техническая вооруженность, низкая эффективность тактики производства следственных действий, выбор ошибочных направлений расследования.

Цель данной работы – исследовать положения, характеризующие понятие компьютерного преступления и уголовно-правового состава неправомерного доступа к информации. Теоретическая и практическая значимость исследования заключается в возможности реального использования его положений и выводов, как в работе правоохранительных органов, так и в правоприменительной практике.

В работе использовались в качестве источников: Конституция Российской Федерации, Уголовный кодекс РФ, Комментарий к Уголовному кодексу РФ, Гражданский кодекс РФ, часть 1, Комментарий к Гражданскому кодексу РФ.

# Основная часть

## 1 Понятие и признаки компьютерных преступлений

**1.1 Понятие и общая характеристика преступлений в сфере компьютерной информации**

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

Под доступом к компьютерной информации подразумевается любая форма проникновения в источник информации с использованием средств электронно-вычислительной техники, позволяющая производить манипуляции с полученной компьютерной информацией.

Неправомерным признается доступ не обладающего правами на это лица к компьютерной информации, в отношении которой принимаются специальные меры защиты, ограничивающие круг лиц, имеющих доступ.

Развитие современного общества, основанного на использовании огромного количества самой разнообразной информации, немыслимо без широкого вне­дрения в управленческий процесс и многие другие сферы электронно-вычисли­тельной техники. Она служит не только для хранения и обработки соответствую­щей информации на уровне органов государственной власти и местного самоуправления или коммерческих организаций, используется как средство связи и коммуникации между гражданами, но и является одним из важнейших элемен­тов в обеспечении внутренней и внешней безопасности государства. Все это обусловливает разработку правовых норм, обеспечивающих регулирование общественных отношений, которые связаны с использованием компьютерной техники (в первую очередь с защитой хранящейся с ее помощью информации).

Определенную роль в этом играют и нормы гл. 28 УК «Преступления в сфере компьютерной информации».

Согласно Уголовному Кодексу преступлениями в сфере компьютерной информации являются: неправомерный доступ к компьютерной информации (ст. 272 УК); создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК). Преступления, содержащиеся в этой главе, представляют собой общественно опасные деяния, посягающие на безопасность информа­ции и систем обработки информации с использованием ЭВМ (видовой объект преступления). Это означает, что преступные деяния, совершаемые с помощью электронно-вычислительной техники (т.е. в качестве средства совершения ка­кого-либо преступления), статьями гл. 28 УК не охватываются и подлежат ква­лификации как самостоятельные посягательства (например, в качестве пре­ступления против собственности – мошенничества, как преступление против основ конституционного строя и безопасности государства – шпионаж).

Физическое повреждение или уничтожение компьютерной техники, незаконное завладение ПЭВМ или ее компонентами, а равно машинными носителями информации (дискетами, CD-R дисками, электронными «накопителями») как предметами, обладающими материальной ценностью, квалифицируется в качестве посягательства на чужую собственность по статьям гл. 21 УК. Преступления в сфере компьютерной информации сопряжены с посягательством на иной своеобразный предмет – информацию, сосредото­ченную внутри компьютера (в файлах, программах или базах данных).

Одна­ко при определенных условиях неправомерное завладение компьютерной ин формацией может дополнительно образовать преступление, предметом кото­рого выступает информация как таковая (например, нарушение неприкосно­венности частной жизни – ст. 137 УК).

Объективная сторона рассматриваемых преступлений по общему правилу представляет собой деяние в форме действия. Бездействие возможно только как несоблюдение установленных правил эксплуатации ЭВМ, систем или сетей ЭВМ (ст. 274 УК). Особенностью конструкции составов этих преступ­лений является то, что преимущественно они сконструированы по типу мате­риальных – предполагают наступление общественно опасных последствий в виде вреда для пользователей ЭВМ. Согласно уголовному закону этот вред состоит в нарушении нормального функционирования ЭВМ или сетей ЭВМ.

Субъектом преступлений в сфере компьютерной информации могут быть не только лица, в обязанности которых входит соблюдение правил хранения и обработки информации либо иных правил безопасности информационных систем (специальный субъект), но и любые иные лица, противоправно получившие до­ступ к информации с помощью персонального компьютера, а также создавшие, использовавшие или распространившие вредоносные программы для ЭВМ.

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

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

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

Основные понятия:

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

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

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

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

Сети ЭВМ - компьютеры, объединенные между собой сетями электросвязи.

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

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

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

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

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

– модификация в виде исправления явных ошибок;

– модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя;

– модификация в виде частичной декомпиляции программы для достижения способности к взаимодействию с другими программами.

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

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

**1.2 Общие признаки преступлений в сфере компьютерной информации**

В Уголовном кодексе Российской Федерации впервые в нашей стране криминализирован такой вид правонарушений, как компьютерные преступления - предусмотренные уголовным законом общественно опасные деяния, в которых машинная информация представляет собой предмет преступного посягательства.

Преступления, имеющие своим предметом только лишь аппаратно-технические средства вычислительных машин (хищение, уничтожение), подпадают под совершенно другой тип уголовных правонарушений, закрепленных в главе 21 “Преступления против собственности”. В принципе, можно предположить случаи, когда вредоносное воздействие на ЭВМ осуществляется путем непосредственного влияния на нее информационных команд. Это возможно, если преступнику удастся ввести движущиеся части машины (диски, принтер) в резонансную частоту, увеличить яркость дисплея или его части для прожигания люминофора, зациклить работу компьютера таким образом, чтобы при использовании минимального количества его участков произошел их разогрев и вывод из строя. В этих случаях квалификация содеянного должна проводиться по совокупности статей глав о преступлениях против собственности и компьютерных преступлениях, поскольку в данной ситуации страдают два объекта уголовно-правовой охраны. Равно и при использовании в качестве орудия совершения противоправного деяния не информационной, а одной аппаратно-технической части (нанесение телесных повреждений принтером и т. п.) последнюю можно расценивать наравне с такими предметами, как нож, пистолет, веревка и другие вещи материального мира. В целом же 28-я глава УК РФ “Компьютерные преступления” имеет своей целью охрану именно информационной безопасности — и только в силу этого защиту и аппаратно технических средств, которые являются материальными носителями информационных ресурсов.

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

Таким образом, 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. Чаще всего непосредственный объект основного состава компьютерного преступления сформулирован альтернативно, в квалифицированных составах количество их, естественно, увеличивается.[[1]](#footnote-1)

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. Однако принять ее означало бы слишком расширить рамки понятия “компьютерное преступление” и затруднить работу, как законодателя, так и правоприменителя. Разработчики УК РФ 1996 г. пошли по первому пути, сформулировав составы главы 28 таким образом, что информация ЭВМ в каждом случае является лишь предметом совершения компьютерного преступления.

Однако при использовании машинной 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 информацией, хранящейся в ЭВМ, 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. (Приложение 1) Даже если не пострадают сведения конкретной ЭВМ, правомерно употребляемые ее законным пользователем, практически неизбежно подвергнутся ущербу те, с которыми она связана сетью. Таким образом, даже при совершении такого классического преступления, как электронное хищение денег, ответственность за это должна наступать по правилам идеальной совокупности преступлений.

Почти все составы главы 28 относятся к преступлениям небольшой и средней тяжести, и только один – к тяжким преступлениям. Характеризуя объективную сторону рассматриваемых составов, заметим, в первую очередь, что даже 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 нельзя не признать, что уничтожение, блокирование, модификация и копирование информации не исключают совершения самостоятельных действий. В учебной литературе указывается, что правильнее было бы рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ сопряжен с уничтожением, блокированием и т.д. (т.е. такому доступу следовало бы придать значение не только причины, но и необходимого условия).[[2]](#footnote-2)

В силу ч. 2 ст. 9 УК РФ 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.

В силу ч. 2 ст. 9 УК РФ 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 УК, 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.[[3]](#footnote-3)

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. Для их применения необходимо обратиться к ст. 35 УК РФ, 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.[[4]](#footnote-4)

Первоначально в проекте УК РФ глава о компьютерных преступлениях содержала 5 статей. Однако в дальнейшем в силу замечаний, высказанных как теоретиками уголовного права, так и практиками компьютерного дела, первые три статьи были объединены, и в настоящее время глава предстает в следующем составе:

ст. 272. Неправомерный доступ к компьютерной информации;

ст. 273. Создание, использование и распространение вредоносных программ для ЭВМ;

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

## 

## 

***2 Виды компьютерных преступлений***

**2.1 Неправомерный доступ к компьютерной информации**

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

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

Как следует из действующего законодательства, использование информационных систем возможно только с явно выраженного согласия их собствен­ников. Любое иное ознакомление с ресурсами системы является неправомерным. Особо следует от­метить компьютерную информацию, собственником которой является государство или его субъекты и образования. К государственной конфиденциальной информации относятся в частности служебная тай­на,

– государственная тайна,

– данные предвари­тельного следствия (ст. 310 УК РФ), сведения о мерах безопасности, применяемых в отношении судьи и участников уголовного процесса (ст. 311 УК РФ), сведения о мерах безопасности, применяемых в отношении должностного лица правоохранитель­ного или контролирующего органа (ст. 320 УК РФ). Подобная информация охраняется государством непосредственно в силу соответствующего закона. Следует различать преступную деятельность по захвату ЭВМ и машинных носителей с целью завладения ими как имуществом, имеющим само­стоятельную материальную ценность, в не связи с тем, какая информация на них находится, и деятель­ность, совершаемую с целью доступа к компьютер­ной информации, связанную с изъятием указанных предметов как носителей этой информации. В пер­вом случае такую деятельность при известных ус­ловиях необходимо отнести к преступлениям в сфе­ре экономики. Преступная деятельность, направленная на противоправное причинение ущер­ба компьютерной информации является неправо­мерным доступом независимо от способа доступа. Поэтому утверждения о том, что «не образует объективной стороны... уничтожение или искаже­ние компьютерной информации путем внешнего воздействия на машинные носители теплом, маг­нитными волнами, механическими ударами...»[[5]](#footnote-5) представляются не верными.

Поскольку собственник или владелец информа­ционных ресурсов, обязан обеспечить режим за­щиты информации в том числе и путем установле­ния правил эксплуатации ЭВМ, препятствующих несанкционированному ознакомлению посторонних лиц с принадлежащими ему информационными ре­сурсами и их защиту от неправомерных действий, создается возможность оценки любого неправомер­ного доступа к компьютерной информации со сто­роны лица, имеющего доступ к ЭВМ, системе ЭВМ или к их сети (далее для краткости - «доступ к ЭВМ») как совершения совокупности преступлений (ст. 272 и 274 УК РФ), так как осуществляя неправомерный доступ, такое лицо нарушает правила использова­ния конкретной компьютерной информации.[[6]](#footnote-6) Факти­чески лица, совершая указанные выше деяния, все­гда (правомерно или неправомерно) получают возможность оперировать ресурсами чужого ком­пьютера, нарушая правила их эксплуатации, установленные собственником или владельцем информационного ресурса. Имеются признаки со­вокупности преступлений и в случае незаконного использования объектов авторского права лицами осуществлявшими копирование информации в виде программ для ЭВМ, при проникновении в ЭВМ с целью совершения хищения денежных средств, выявления идентифицирующей информации о фи­зических (например, ПИН - коды кредитных карточек) и юридических (например, коды модемного управ­ления расчетным счетом) лицах для последующе­го завладения их имуществом, шпионажа, дивер­сии и др. В таких случаях применяется правило, предусмотренное ч. 3 ст. 17 УК РФ.

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

Частью 2 ст. 272 УК РФ предусмотрено три ква­лифицирующих признака, состоящих в совершении рассматриваемого преступления: совершение груп­пой лиц по предварительному сговору или органи­зованной группой, совершение лицом с использо­ванием своего служебного положения и совершение лицом, имеющим доступ к ЭВМ. Для использова­ния служебного положения характерно, что лицо, осуществившее неправомерный доступ к ЭВМ, по своей служебной компетенции или трудовому до­говору (контракту) имеющее определенные полномочия, превысило свои права или нарушило свои обязанности или использовало их вопреки интере­сам работодателя. Лицо, имеющее доступ к ЭВМ, может иметь таковой в силу указанных выше со­глашений или договоров в качестве пользовате­ля информационной системы. Умышленное нару­шение достигнутых с собственником договоренностей о порядке пользования информа­цией и нарушение согласованных правил доступа к информационному ресурсу является квалифициру­ющим обстоятельством и соответствует идее законодателя об усилении защиты прав субъектов в сфере информационных процессов «...в целях пре­дупреждения правонарушений, пресечения непра­вомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба».[[7]](#footnote-7)

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

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

Программы для ЭВМ являются разновиднос­тью компьютерной информации. Под «программой для ЭВМ» законодательством понимается объек­тивная форма представления совокупности дан­ных и команд, предназначенных для функциони­рования электронных вычислительных машин и других компьютерных устройств с целью получе­ния определенного результата.[[8]](#footnote-8) Программы фак­тически существует в двух видах - в виде «исход­ного текста», т.е. описанного с помощью языков программирования алгоритма обработки данных или управления ими, и в виде «объектного кода» - исходного текста, компилированного в набор ма­шиночитаемых символов. (Приложение Б) Под про­граммой для ЭВМ подразумеваются также подго­товительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения.[[9]](#footnote-9) Программа, специально разрабо­танная или модифицированная для несанкциони­рованного собственником информационной систе­мы уничтожения, блокирования, модификации либо копирования информации, нарушения обыч­ной работы ЭВМ, является вредоносной. (Приложение 3)

Ранее для обозначения этого явления в лите­ратуре часто использовалось понятие «компьютер­ный вирус» или «информационные инфекции». Так же именовалось данное явление в проекте ныне действующего Уголовного кодекса. Использовав оп­ределение «вредоносные» программы, законода­тель позволил практике расширить существовавшие представления о программах подобного рода.

Ра­нее в специальной литературе, посвященной «ком­пьютерной вирусологии» считалось, что в тех слу­чаях, когда в результате действия «вирусов» происходят существенные разрушения файловой системы, уничтожение информации и т.п. - «вирус» является опасным, если же в результате его дей­ствия на экране, например, появляются стихи, брань и т.п., «вирус» считается безопасным. Учитывая определение законодателя, ВП могут быть разде­лены на три больших класса на базе представле­ний о цели создания программы и последствиях ее действия.

Первый класс ВП, обладая свойствами самосто­ятельного размножения в системах и сетях ЭВМ, не всегда приводит к существенным последствиям для информационных ресурсов, хотя в некоторых случаях и модифицирует информацию, а иногда и блокирует ЭВМ, их сети и системы. Разработчики этого класса ВП не рассматривают свою деятель­ность как общественно-опасную, хотя объективно она является таковой. Так, например, 2 мая 1988 г. запущенный неизвестным лицом «безопасный ви­рус» сработал и около 350 000 машин по всему миру после загрузки высветили на экранах сообщение "PEACE" («МИР»). После этого вирус сам себя уда­лил из всех систем. Несколько сложнее обстояло дело с ВП «рождественская открытка» Эта програм­ма распространялась через электронную почту и одновременно с демонстрацией поздравлений на экране скрытно считывала данные о всех имеющих­ся у данного абонента адресах и рассылала по ним аналогичные сообщения. Данная ВП за короткое вре­мя заблокировала своими копиями электронную по­чту почти всей несоциалистической части мира.[[10]](#footnote-10)

Второй класс ВП - «опасные вирусы», разру­шающие информационные системы и приносящие существенный вред. Примером такой программы является саморазмножающаяся программа «SURPRISE», которая при запуске выполняет удаление всех файлов в директории, а затем выводит на экран надпись «SURPRISE !» (Сюрприз !).[[11]](#footnote-11)

Наконец, третий класс ВП предназначен для организации неправомерного доступа к чужим ин­формационным ресурсам. Известные случаи противоправного проникновения в ЭВМ показывают, что злоумышленники обычно вынуждены прежде всего изменять различными способами, в том числе и путем внедрения ВП, программные средства или порядок их работы), обеспечивающие взаимодействие устройств ЭВМ между собой и с пользователем. Такие ВП, обеспечивающие вход в систему или привилегированный режим работы с ней, называют также «люками» («back door»). Известен случай, когда преступная группа смогла договориться с программистом, работающим над банковским программным обеспечением, о том, чтобы он ввел подпрограмму, которая предоставит преступникам доступ в систему после ее установки с целью перемещения денежных средств.[[12]](#footnote-12) К данному классу следует отнести и многочисленные программные изделия», предназначенные для снятия защиты от копирования коммерческих программных продуктов, последние ВП наносят существенный вред авторам и распространителям программ и систем. Предметом рассматриваемого преступления при распространении машинных носителей программ является машинный носитель вредоносной программы, хотя бы одной. О распространенности данного явления свидетельствует тот факт, что на российском рынке программного обеспечения ежемесячно фикси­руется появление от 2 до 10 новых ВП.[[13]](#footnote-13)

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

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

Под распространением программ в соответ­ствии с законом понимается предоставление до­ступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей.[[14]](#footnote-14) Распространением вредоносных программ являет­ся не только передача самих программ в виде на­бора объектных кодов, но и опубликование или ин­дивидуальная рассылка исходных текстов подобных программных продуктов. Указанные действия долж­ны находиться в причинной связи с наступившими последствиями - уничтожением, блокированием, модификацией либо копированием информации, нарушением работы ЭВМ, системы ЭВМ или их сети.

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

Частью 2 статьи 273 УК РФ предусмотрен один квалифицирующий признак - причинение по неосто­рожности тяжких последствий. Под тяжкими послед­ствиями понимается причинение существенного материального ущерба собственнику или собствен­никам информационных систем, пострадавших от действия ВП, а также их пользователям, возникший, в том числе, в связи с восстановлением работоспо­собности информационных систем последействия ВП, утрата важной информации или серьезное на­рушение прав собственников на ее использование, выход из строя крупных систем управления, осно­ванных на работе ЭВМ и др. Известно, что в ре­зультате распространения ВП возникают значитель­ные, и вместе с тем не всегда точно определяемые потери. Так называемый «Пакистанский» вирус за­разил только в США более 18 тыс. компьютеров. «Лехайский» вирус по состоянию на февраль 1989 г. заразил около 4 тыс. компьютеров в США.[[15]](#footnote-15) При подобных воздействиях на компьютерную инфор­мацию весьма сложно определить точный объем причиняемого вреда.

Под охраняемой законом информацией понимается информация, для которой в специальных законах установлен специальный режим её правовой защиты, например – государственная, служебная, коммерческая и банковская тайны, персональные данные и т.д.

Уголовная ответственность за нарушение пра­вил эксплуатации ЭВМ, системы ЭВМ или их сети установлена ст. 274 УК РФ.

Непосредственным объектом данного преступ­ного деяния являются общественные отношения, обеспечивающие внутреннюю безопасность инфор­мационных систем, базирующихся на использо­вании ЭВМ, системы ЭВМ или их сети с точки зре­ния целостности и конфиденциальности содержащейся в них компьютерной информации.[[16]](#footnote-16)

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

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

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

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

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

Субъективная сторона рассматриваемого соста­ва преступления характеризуется виной в форме умысла, прямого или косвенного. Виновный осознает:

– во-первых, нарушает правила эксплуата­ции ЭВМ, системы ЭВМ или их сети и;

– во-вторых, такое нарушение является общественно опасным;

– предвидит возможность или неизбежность альтер­нативно уничтожения, блокирования или модифи­кации охраняемой законом информации ЭВМ и во всех случаях причинения существенного вреда и желает наступления этих последствий либо созна­тельно их допускает или относится к ним безраз­лично.

По данным правоохранительных органов, имеются сведения о фактах несанкционированного доступа к ЭВМ вычислительного центра железных дорог России, а также к электронной информации систем учета жилых и нежилых помещений местных органов управления во многих городах, что в наше время попадает под ответственность, предусмотренную ст. 272 УК РФ, либо ст. 274 УКРФ в зависимости от действий лица, осуществившего посягательство и правил эксплуатации конкретной сети.

# Заключение

С повышение роли информации во всех сферах человеческой деятельности повышается роль и значение компьютерной информации как одной из популярных форм создания, использования, передачи информации. А с повышением роли компьютерной информации требуется повышать уровень ее защиты с помощью технических, организационных и особенно правовых мер.

С 1992 года законодатель начал вводить правовое регулирование в сфере использования компьютерной информации, но как показали исследования данной работы, не всегда последовательное. В частности, несоответствие терминологии различных законов, например, несоответствие сути термина «информация» употребленного в Законе об информации и Уголовном законе. Отсутствие, законодательного закрепления некоторых терминов употребляемых в Уголовном законе, например, «ЭВМ», «система ЭВМ», «сеть ЭВМ», «копирование информации» и других. Непоследовательность обнаруживается и в самом Уголовном законе, например, при нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети упоминается о последствиях в виде уничтожения, блокирования или модификации информации, но ничего не говорится о нарушении работы ЭВМ, системы ЭВМ, их сети, хотя это, как и в двух других составах предусмотренных Уголовным кодексом, может принести собственнику ущерб. Также нужно сказать о непоследовательном подходе к формированию квалифицирующего признака о неосторожном причинении тяжких последствий. Такой признак предусмотрен в двух статьях 273 и 274 УК РФ, а это нельзя признать верным, т.к. неосторожное причинение тяжких последствий в равной степени может быть следствием всех трех незаконных деяний.

Проведенные исследования подводят к выводу необходимости внесения значительного массива дополнений и изменений в действующее законодательство. Также издания новых законов вносящих правовое регулирование в информационные отношения, обусловленные распространением на территории России глобальной сети Интернет.

Также проведенные в работе исследования показали, что проработка вопросов в юридической литературе об информационных отношениях, в общем, и компьютерных преступлений в частности, находится на низком уровне. Многие суждения, как в техническом плане, так и в юридическом плане, далеки от практики. Некоторые приводимые мнения только запутывают, нежели помогают разобраться. В связи с чем, в работе приведены собственные мнения по некоторым вопросам, в частности, по формулировке понятия «ЭВМ», «системы ЭВМ», «компьютерного преступления», «неправомерного доступа» и других.

В настоящее время крайне необходимо более глубокое теоретическое осмысление нового законодательства об информационных отношениях, в частности об ЭЦП, внесённых новелл и практики применения. Необходимо поднять многие дискуссионные вопросы для обсуждения, как в рамках специализированных конференций, так и в Интернет - конференциях и Интернет - форумах.

Анализ судебной и следственной практики показал, что следователи и суды практически не имеют знаний в юридических и технических вопросах компьютерных преступлений и действуют по аналогии, что приводит к неправильной квалификации и необоснованным приговорам. Хотя при территориальных органах управления внутренних дел созданы подразделения по борьбе с преступлениями в сфере высоких технологий, но работают там сотрудники по большей части недостаточно квалифицированные либо в технической стороне, либо в юридической стороне компьютерного преступления. В связи с чем, требуется осуществить организационные и правовые меры:

— по подбору в данные подразделения только специалистов в обоих областях, либо подготовке таких специалистов и дальнейшее постоянное и динамичное повышение их квалификации;

— закрепить, в рамках подведомственности, дела о компьютерных преступления только за этими подразделениями;

— разработать научные методики, программные средства и технические устройства для получения и закрепления доказательств совершения компьютерного преступления;

— и другие меры.

Итогом проведенных исследований в работе является разработка ключевых положений, характеризующих понятие компьютерного преступления и неправомерного доступа к компьютерной информации. Данные положения могут служить базой для дальнейших исследований или методическим материалом в правоприменительной практике.

# Глоссарий

|  |  |  |
| --- | --- | --- |
| № п/п | Понятие | Определение |
| 1 | **Защита информации** | совокупность методов и средств, обеспечивающих целостность, конфиденциальность, достоверность, аутентичность и доступность информации в условиях воздействия на нее угроз естественного или искусственного характера. |
| 2 | **Информационная безопасность** | по законодательству РФ - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.  Информационная безопасность имеет три основные составляющие:  – конфиденциальность - защита чувствительной информации от несанкционированного доступа;  – целостность - защита точности и полноты информации и программного обеспечения;  – доступность - обеспечение доступности информации и основных услуг для пользователя в нужное для него время. |
| 3 | **Конфиденциальная информация** | информация, доступ к которой ограничивается в соответствии с законодательством страны и уровнем доступа к информационному ресурсу. Конфиденциальная информация становится доступной или раскрытой только санкционированным лицам, объектам или процессам. |
| 4 | **Компьютерный вирус** | фрагмент исполняемого кода, который копирует себя в другую программу (главную программу), модифицируя ее при этом. Дублируя себя, вирус заражает другие программы. Вирус выполняется только при запуске главной программы и вызывает ее непредсказуемое поведение, приводящее к уничтожению и искажению данных и программ. |
| 5 | **Компьютерные преступления** | в уголовном праве РФ - преступления, посягающие на нормальное, безопасное функционирование компьютерных информационных систем:  - неправомерный доступ к компьютерной информации;  - создание, использование и распространение вредоносных программ для ЭВМ;  - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. |
| 6 | **Логическая бомба** | программа, выполняемая периодически или в определенный момент времени с целью исказить, уничтожить или модифицировать данные. |
| 7 | **Передача файлов** | копирование файлов с одного компьютера на другой в сетевой среде. |
| 8 | **Пересылка данных** | перемещение данных между компонентами системы. При пересылке данные в одном компоненте стираются, а в другом - записываются.  Процедуры, используемые для пересылки данных, отличаются от процессов передачи данных, происходящих между системами. |
| 9 | **Хакер** | лицо, совершающее различного рода незаконные действия в сфере информатики: - несанкционированное проникновение в чужие компьютерные сети и получение из них информации;  - незаконные снятие защиты с программных продуктов и их копирование;  - создание и распространения компьютерных вирусов и т.п. |
| 10 | **Хранение данных** | Хранение данных - процесс обеспечения целостности, доступности и защищенности данных. Различают три режима хранения данных:  – хранение в оперативном режиме, основанное на использовании постоянно доступных запоминающих устройств;  – хранение в почти оперативном режиме, основанное на использовании устройств, которые могут стать доступными автоматически;  – хранение в автономном режиме, основанное на использовании устройств, носители данных в которые вставляются вручную. |

# Список использованных источников

|  |  |
| --- | --- |
| 1 | Российская Федерация. Конституция (1993). Конституция Российской Федерации [Текст]: офиц. текст. – М.: Феникс, 2008.–92с.- ISBN: 978-5-222-13533-4. |
| 2 | Гражданский кодекс Российской Федерации [Текст]: части первая, вторая, третья и четвертая: офиц. текст по состоянию на15.06.09 – М.: Омега-Л, 2009. – 368 с. – ISBN 978-5-370-01431-4. |
| 3 | Российская Федерация. Законы. "Об авторском праве и смежных правах" [Текст] : федер. закон. – М.: Омега-Л, [2007]. – 16, [1] с. – ISBN: 978-5-370-00378-3. |
| 4 | Уголовный кодекс Российской Федерации [Текст]: офиц. – М.: Ось-89, 2009. – 191 с. – ISBN 978-5-9957-0097-5. |
| 5 | Андреев, Б. В. Расследование преступлений в сфере компьютерной информации: [Текст] / Б. В. Андреев, П. Н. Пак, В. П. Хорст. – М.: Юрлитинформ, 2004. –152 с. – ISBN 5-93295-037-4. |
| 6 | Вехов, В. Б. Тактические особенности расследования преступлений в сфере компьютерной информации: [Текст] / В. Б. Вехов, В. В. Попова, Д. А. Илюшин. – М.: ЛексЭст, 2004. – 160 с. – ISBN 5-901638-54-9. |
| 7 | Гаврилин, Ю. В. Преступления в сфере компьютерной информации: квалификация и доказывание. Учебное пособие: [Текст] / Ю. В. Гаврилин. – М.: ЮИ МВД РФ, 2003. – 240 с. – ISBN 5-8041-0135-8. |
| 8 | Козаченко, И.Я. Уголовное право. Особенная часть: [Текст] / Козаченко И.Я., Новоселов Г.П. – М.: Норма, 2008. – 1008 с. – ISBN 978-5-468-00175-2. |
| 9 | Комиссаров, В.С. Российское уголовное право. Особенная часть: [Текст] / Комиссаров В.С. – М.: Питер, 2008. – 718 с. – ISBN 978-5-469-01524-6. |
| 10 | Комментарий к Уголовному кодексу Российской Федерации (постатейный). Особенная часть. Том 1: [Текст] / – М.: Дашков и Ко, 2005. – 912 с. – ISBN 5-94798-729-5. |
| 11 | Комментарий к Уголовному кодексу Российской Федерации (постатейный). Особенная часть. Том 2: [Текст] / – М.: Дашков и Ко, 2005. – 1068 с. – ISBN 5-94798-729-5. |
| 12 | Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: [Текст] / В. Ф. Шаньгин. – М.: Инфра-М, 2008. – 416 с. – ISBN 978-5-8199-0331-5, 978-5-16-003132-3. |

# Приложения

|  |  |
| --- | --- |
| А |  |
| Б |  |
| В |  |

1. Симкин, Л. Как остановить компьютерное пиратство. М., 1996. 10. –С. 37-39. [↑](#footnote-ref-1)
2. Козаченко, И. Я. Уголовное право. Особенная часть. М., 2008. - С. 114. [↑](#footnote-ref-2)
3. Комиссаров, В.С. Российское уголовное право. Особенная часть. М., 2008. - С.374. [↑](#footnote-ref-3)
4. Гаврилин, Ю.В. Преступления в сфере компьютерной информации: квалификация и доказывание. М., 2003. - С. 34. [↑](#footnote-ref-4)
5. Комментарий к Уголовному кодексу Российской Федерации (постатейный). Особенная часть.М., 2005. - С. 523. [↑](#footnote-ref-5)
6. Федеральный Закон Российской Федерации N 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 14.07.2006года, гл.5. [↑](#footnote-ref-6)
7. Федеральный Закон Российской Федерации N 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 14.07.2006года, ст.23. [↑](#footnote-ref-7)
8. Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» (в ред. Федеральных законов от 24.12.2002 N 177-ФЗ, от 02.11.2004 N 127-ФЗ, от 02.02.2006 N 19-ФЗ). 2006г. ст. 11. [↑](#footnote-ref-8)
9. Там же. [↑](#footnote-ref-9)
10. Файтс, Ф. Компьютерный ви­рус проблемы и прогноз. Пер. с англ. М., 1994. - С.30-31. [↑](#footnote-ref-10)
11. Там же. [↑](#footnote-ref-11)
12. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей.М., 2008. - С. 253. [↑](#footnote-ref-12)
13. Овчинский, B.C. Основы борьбы с организованной преступностью. М., 1996. – С.206. [↑](#footnote-ref-13)
14. Закон Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» (в ред. Федеральных законов от 24.12.2002 N 177-ФЗ, от 02.11.2004 N 127-ФЗ, от 02.02.2006 N 19-ФЗ). 2006г. ст. 16. [↑](#footnote-ref-14)
15. Лебедев, В.М. Комментарий к Уголовному кодексу Российской Федерации. М., 2006. – С. 696. [↑](#footnote-ref-15)
16. Федеральный Закон Российской Федерации N 149-ФЗ «Об информации, информационных технологиях и о защите информации» от 14.07.2006года, ст.16. [↑](#footnote-ref-16)