**МИНИСТЕРСТВО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ**

**ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ**

**КАФЕДРА УГОЛОВНОГО ПРАВА И ПРОЦЕССА**

**ДИПЛОМНАЯ РАБОТА**

**На тему:** *Особенности квалификации преступлений в сфере компьютерной информации*

Выполнил, *студент гр. 1232, з/о, юр. фак-та Доржиев А.И.*

Научный руководитель:

*Ст. преподаватель*

*Чимытова Т.В.*

Зав. кафедрой:

г. Улан-Удэ 2002 г.

Содержание

1. ВВЕДЕНИЕ 4

2. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ 7

1.1. Правовое регулирование отношений в области компьютерной информации. 7

1.1.1. Основные понятия. 7

1.1.2. Отечественное законодательство в области компьютерного права 18

1.2. Уголовно-правовая характеристика главы 28 УК РФ Преступления в сфере компьютерной информации 20

1.2.1. Общие признаки преступлений в сфере компьютерной информации 20

1.2.2. Уголовно-правовой анализ ст. 272 гл. 28 УК РФ Неправомерный доступ к компьютерной информации 26

1.2.3. Уголовно-правовой анализ ст. 273 гл. 28 УК РФ Создание, распространение и использование вредоносных программ для ЭВМ 32

1.2.4. Уголовно-правовой анализ ст. 274 гл. 28 УК РФ Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети 36

3. КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ 40

1.3. Понятие квалификации преступлений 40

1.4. Особенность квалификации преступлений в сфере компьютерной информации 41

1.4.1. Разграничения ст.ст.272 и 273 УК РФ 42

1.4.2. Разграничения ст.ст.272 и 274 УК РФ 46

1.4.3. Разграничения ст.ст.272 и 146 УК РФ 48

1.4.4. Разграничения ст.ст.272 и 137 УК РФ 50

1.4.5. Разграничения ст.ст.272 и 183 УК РФ 52

1.4.6. Разграничения ст.ст.272 и 165 УК РФ 53

1.5. Значение квалификации преступлений 55

4. Заключение 59

5. БИБЛИОГРАФИЯ 61

# ВВЕДЕНИЕ

Создание электронно-вычислительной техники четвертого и пятого поколения с потенциально неограниченными возможностями, их широкое распространение в экономической, социальной и управленческой сферах, появление в быту значительного количества персональных ЭВМ явились не только новым свидетельством технического прогресса, но и негативными тенденциями развития преступного мира, привели к появлению новых форм и видов преступных посягательств. Преступные группы и сообщества начинают активно использовать в своей деятельности новейшие достижения науки и техники. Для достижения корыстных целей преступники все чаще применяют системный подход для планирования своих действий, создают системы конспирации и скрытой связи, используют современные технологии и специальную технику, в том числе и всевозможные компьютерные устройства и новые информационно-обрабатывающие технологии.

Мировая практика показывает, что ущерб от компьютерных преступлений может исчисляться суммами, составляющими годовые бюджеты крупных городов. В большинстве стран Европы и Америки компьютерная преступность дает доходы, сравнимые с доходами, получаемыми от незаконного оборота наркотиков и оружия.[[1]](#footnote-1)

Вызывает особую тревогу 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-обрабатывающей технологии, - компьютерных преступлений.

В связи с общей криминогенной обстановкой в России и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных познаний, опасность компьютерных преступлений многократно возрастает, когда существует вероятность совершения последних в отношении функционирования объектов жизнеобеспечения, транспортных и оборонных систем, атомной энергетики, что убедительно свидетельствует о действительной остроте проблемы с преступлениями в сфере компьютерной информации.

В настоящее время в отечественной криминалистической науке все еще не существует четкого определения понятия компьютерного преступления, дискутируются различные точки зрения по их классификации. Сложность в формулировках этих понятий существует, на наш взгляд, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны.

Цель данной работы – определить стержневые понятия, особенности квалификации преступлений в сфере компьютерной информации, подвергнуть всестороннему изучению специфики данных преступлений.

При подготовке работы были изучены и проанализированы: нормы действующего уголовного и уголовно-процессуального законодательства Российской Федерации, Федеральные законы, учебники по уголовному праву, журнальные публикации ряда практических и теоретических работников, аналитические материалы, относящиеся к исследуемой проблематике, в том числе из ресурсов сети Интернет, соответствующая отечественная и зарубежная литература; материалы судебной практики ряда городов Российской Федерации, а также собственной преддипломной практики в отделе по борьбе с компьютерными преступлениями при МВД РБ.

# ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## Правовое регулирование отношений в области компьютерной информации.

### Основные понятия.

Научно-техническая революция повлекла за собой серьезные социальные изменения, наиболее важным из которых является появление нового вида общественных отношений и общественных ресурсов — информационных. Последние отличаются от известных ранее сырьевых, энергетических ресурсов целым рядом особенностей, а именно:  
1) они непотребляемы и подвержены не физическому, а моральному износу;

2) они по своей сущности нематериальны и несводимы к физическому носителю, в котором воплощены;

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

4) процесс их создания и использования осуществляется особым способом — с помощью компьютерной техники.

Информация стала первоосновой жизни современного общества, предметом и продуктом его деятельности, а процесс ее создания, накопления, хранения, передачи и обработки в свою очередь стимулировал прогресс в области орудий ее производства: электронно-вычислительной техники (ЭВТ), средств телекоммуникаций и систем связи. Все это в целом входит в емкое понятие определения новой информационной технологии (НИТ), которая является совокупностью методов и средств реализации информационных процессов в различных областях человеческой деятельности, т. е. способами реализации информационной деятельности человека, которого также можно рассматривать как информационную систему.[[2]](#footnote-2)

Иными словами, информация становится продуктом общественных (информационных) отношений, начинает приобретать товарные черты и становится предметом купли-продажи. Следствием протекающих в обществе информационных процессов является возникновение и формирование новых социальных отношений, и изменение уже существующих. Например, уже сейчас можно констатировать значительный объем договорных отношений, связанных с изготовлением, передачей, накоплением и использованием информации в различных ее формах: научно-технической документации, программного обеспечения ЭВТ, баз данных, систем управления базами данных (СУБД) и др.

Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини- и большими ЭВМ, дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными. Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе уголовно-правовые средства защиты.

Так, Уголовный кодекс Франции (1992 г.) пополнил систему преступлений против собственности специальной главой "О посягательствах на системы автоматизированной обработки данных", где предусмотрел ответственность за незаконный доступ ко всей или части системы автоматизированной обработки данных, воспрепятствование работе или нарушение правильности работы такой системы или ввод в нее обманным способом информации, уничтожение или изменение базы данных.

Не остались в стороне от этой проблемы и международные организации, в частности Совет Европы, который счел необходимым изучить и разработать проект специальной конвенции, посвященной проблеме правонарушений в сфере компьютерной информации.

Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматической обработки информации.

Определенным этапом на пути реализации этих пожеланий стало принятие в 1992 г. Закона РФ “О правовой охране программ для электронно-вычислительных машин и баз данных”. Закон содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечет уголовную ответственность.[[3]](#footnote-3) (ст.20)

Однако соответствующих изменений в УК РСФСР так и не было внесено. В 1994 году был принят Гражданский кодекс, который содержит ряд норм, связанных с защитой информации: «информация, составляющая служебную или коммерческую тайну, защищается способами, предусмотренными настоящим Кодексом и другими законами» (ч.2 ст.139 ГК РФ), в 1995 году - Федеральный закон об информации, информатизации и защите информации. Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления.

Определим некоторые основные понятия, используемые в данной работе.

#### Информация

Важно различать информацию как термин обыденной жизни и как правовую категорию. Информация, как таковая, представляет собой категорию идеального, она неосязаема, непотребляема не амортизируется и не может быть объектом правоотношений безотносительно к ее носителю, содержанию, идентифицирующим признакам.

В праве под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащихся в информационных системах. Весьма тесно связано с понятием информации и понятие информационных ресурсов, под которыми понимаются отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах.[[4]](#footnote-4)

#### Компьютерная информация

В соответствии со ст.2 закона “Об информации, информатизации и защите информации” под информацией понимаются - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.[[5]](#footnote-5) Введение законодателем в Уголовный кодекс термина компьютерная информация является новшеством. Ранее в Российском законодательстве, регулирующем информационные правоотношения, определения информации как компьютерной не существовало. Вероятней всего, определение компьютерная применительно к информации возникло для отграничения данного объекта посягательства от информационных преступлений, предусмотренных другими разделами Уголовного кодекса РФ. Крылов предлагает следующее криминалистическое определение компьютерной информации как специального объекта преступного посягательства. Компьютерная информация есть сведения, знания или набор команд программа, предназначенные для использования в ЭВМ или управления ею, находящиеся в ЭВМ или на машинных носителях — идентифицируемый элемент информационной системы, имеющей собственника, установившего правила ее использования.[[6]](#footnote-6) С другой стороны, многие практические работники определяют компьютерную информацию не сами сведения, а форму их представления в машиночитаемом виде, т.е. совокупность символов зафиксированная в памяти компьютера, либо на машинном носителе (дискете, оптическом, магнитооптическом диске, магнитной ленте либо ином материальном носителе) и что при рассмотрении дел следует учитывать, что при определенных условиях и физические поля могут являться носителями информации.

#### Конфиденциальная информация

Понятие конфиденциальной информации было введено в отечественную правовую практику с принятием Таможенного кодекса Российской Федерации. В ст. 16 приводится точное и емкое определение, конфиденциальная информация — это информация, не являющаяся общедоступной и могущая нанести ущерб правам и законным интересам предоставившего ее лица**.** В законе Об информации, информатизации и защите информации ст. 2 предлагается другая формулировка: документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации (Указ Президента РФ Об утверждении перечня сведений конфиденциального характера» от 06.03.97г. N188)

Конфиденциальными в соответствии с законом являются, в частности, такие виды информации, как, содержащая государственную тайну Закон РФ О государственной тайне ст.ст. 275, 276, 283, 284 УК РФ; передаваемая путем переписки, телефонных переговоров, почтовых телеграфных или иных сообщений ч. 2 ст. 23 Конституции РФ, ст. 138 УК РФ; касающаяся тайны усыновления ст. 155 УК РФ; содержащая служебную тайну ст. 139 ГК РФ, коммерческую тайну ст. 139 ГК РФ и ст. 183 УК РФ, банковскую тайну ст. 183 УК РФ, личную тайну ст. 137 УК РФ, семейную тайну ст. 137 УК РФ, информация, являющаяся объектом авторских и смежных прав Закон РФ Об авторском праве и смежных правах, ст. 146 УК РФ; информация, непосредственно затрагивающая права и свободы гражданина или персональные данные Федеральный закон Об информации, информатизации и защите информации, ст. 140 УК РФ и др.

#### Информационные ресурсы

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

#### Компьютерное право

Термин компьютерное право возник в промышленно развитых странах в середине нашего столетия в связи с широким использованием средств вычислительной техники и других, связанных с ними технических средств, в различных сферах общественной деятельности и частной жизни и формированием отношений, возникающих в процессе производства и применения новых информационных технологий. В самостоятельную отрасль права оно не выделилось ни в одной стране мира и состоит из нормативно-правовых актов разного уровня, относящихся к различным отраслям права: государственному, административному, гражданскому, уголовному и т л. В России аналогичное законодательство чаще всего называется законодательством в сфере информатизации и охватывает, по разным оценкам, от 70 до 500 НПА включая НПА, которыми предусматривается создание отраслевых или специализированные автоматизированных систем, и не включая НПА. регулирующие на общих основаниях хозяйственную деятельность субъектов на рынке новых информационных технологий.[[7]](#footnote-7)

#### Неправомерный доступ к компьютерной информации

В специальной литературе под неправомерным доступом к компьютерной информации понимается несанкционированное собственником информации ознакомление лица с данными, содержащимися на машинных носителях или в ЭВМ. В. С. Комиссаров, д. ю. н., профессор, определяет под неправомерным доступом к компьютерной информации получение возможности виновным лицом на ознакомление с информацией или распоряжения ею по своему усмотрению, совершаемое без согласия собственника либо иного уполномоченного лица. Самостоятельной формой неправомерного доступа являются случаи введения в компьютерную систему, сеть или в определенный массив информации без согласия собственника этого массива или иного лица заведомо ложной информации, которая искажает смысл и направленность данного блока информации.[[8]](#footnote-8)

#### Уничтожение информации

Уничтожение информации — это приведение ее полностью либо в существенной части в непригодное для использования по назначению состояние.6

#### Блокирование информации

Блокирование информации — это создание недоступности, невозможности ее использования в результате запрещения дальнейшего выполнения последовательности команд либо выключения из работы какого-либо устройства, или выключения реакции какого-либо устройства ЭВМ при сохранении самой информации.[[9]](#footnote-9)

#### Модификация информации

Под модификацией понимается изменение первоначальной информации без согласия ее собственника или иного законного лица.7

#### Копирование информации

Копирование информации — это снятие копии с оригинальной информации с сохранением ее не поврежденности и возможности использования по назначению.7

#### Нарушение работы ЭВМ, системы ЭВМ или их сети

Под нарушением работы ЭВМ, системы ЭВМ или их сетиследует понимать нештатные ситуации, связанные со сбоями в работе оборудования, выдачей неверной информации, отказе в выдаче информации, выходом из строя отключением ЭВМ, элементов системы ЭВМ или их сети и т.д.7 Однако во всех этих случаях обязательным условием является сохранение физической целости ЭВМ, системы ЭВМ или их сети. Если наряду с названными последствиями нарушается и целостность компьютерной системы, как физической вещи, то содеянное требует дополнительной квалификации по статьям о преступлениях против собственности.

#### Машинные носители

Под машинными носителями следует понимать мобильные устройства накопления информации, обеспечивающие взаимодействие ЭВМ с окружающей средой накопители на гибких и жестких, а также записываемых магнитооптических дисках, стримеры и т. д..7

#### Система ЭВМ

Система — это совокупность взаимосвязанных ЭВМ и их обеспечения, предназначенная для повышения эффективности их работы.[[10]](#footnote-10)

#### Сеть ЭВМ

Сеть ЭВМ - совокупность компьютеров, средств и каналов связи, позволяющая использовать информационные и вычислительные ресурсы каждого компьютера включенного в сеть независимо от его места нахождения.

В настоящее время в отечественной криминалистической науке все еще не существует четкого определения понятия компьютерного преступления, дискутируются различные точки зрения по их классификации. Сложность в формулировках этих понятий существует, на наш взгляд, как по причине невозможности выделения единого объекта преступного посягательства, так и множественности предметов преступных посягательств с точки зрения их уголовно-правовой охраны. В настоящее время существуют два основных течения научной мысли. Одна часть исследователей относит к компьютерным преступлениям действия, в которых компьютер является либо объектом, либо орудием посягательства. Исследователи же второй группы относят к компьютерным преступлениям только противозаконные действия в сфере автоматизированной обработки информации. Они выделяют в качестве главного квалифицирующего признака, позволяющего отнести эти преступления в обособленную группу, общность способов, орудий, объектов посягательств. Иными словами, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства. Законодательство многих стран, в том числе и России, стало развиваться именно по этому пути.  
Поскольку уголовное право исходит из материального, правового определения понятия преступления, то суть любого преступления состоит в том, что оно изменяет, разрывает конкретное общественное отношение, представляющее собой определенную связь людей по поводу материальных, социальных и идеологических ценностей, охраняемых уголовно-правовыми нормами.

Относительно объекта преступного посягательства двух мнений быть не может – им, естественно, является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества. Субъект данного вида преступлений может быть как общим так и специальным. Субъективная сторона чаще всего выражается в умысле, но в ряде случаев компьютерное преступление может быть совершено и по неосторожности.  
Итак, под *компьютерными преступлениями*следует понимать предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является объектом преступного посягательства. В данном случае в качестве предмета или орудия преступления будет выступать машинная информация, компьютер, компьютерная система или компьютерная сеть.

### Отечественное законодательство в области компьютерного права

Законодательство России в области компьютерного права начало формироваться с конка 1991 года. Оно базируется на нормах Конституции и Гражданского кодекса и включает следующие основные законы, О средствах массовой информации 27.12.91г. № 2124-1, Патентный закон РФ от 23.09.92г. № 3517.1. О правовой охране топологий интегральных микросхем от 23.09 92г № 3526-1, О правовой охране программ для электронных вычислительных машин и баз данных от 23 09.92г. № 3523-1, О товарных знаках, знаках обслуживания и наименования мест происхождения товаров от 23.09 92г. № 3520-1, Основы законодательства об Архивном фонде РФ и архивах от 7 07 93 г № 5341-1, Об авторском праве и смежных правах от 90793 г. № 5351-1, О государственной тайне от 21.07 93 г. № 5485-1, Об обязательном экземпляре документов от 29.12 94 г. № 77-ФЗ, О связи от 1602 95 г. № 15-ФЗ, Об информации, информатизации и защите информации от 20 02 95 г. № 24-ФЗ. Об участии в международном информационном обмене от 04 07 96 г. № 85-ФЗ. Значительный пласт компьютерного права составляют указы Президента РФ, которые касаются, прежде всего, вопросов формирования государственной политики в сфере информатизации, включая организационные механизмы, создания системы правовой информации и информационно-правового сотрудничества с государствами СНГ, обеспечения информацией органов государственной власти, мер по защите информации в частности, шифрования.[[11]](#footnote-11)

Конституция РФ непосредственно не регулирует отношения в области производства и применения новых информационных технологий, но создает предпосылки для такого регулирования, закрепляя права граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом ч 4 ст. 29, право граждан на охрану личной тайны ч 1 ст 24 и другие, обязанности государства, в частности, по обеспечению возможности ознакомления гражданина с документами и материалами, непосредственно затрагивающими его права и свободы ч 2 ст 24.[[12]](#footnote-12) Соответствующее законодательство формирует механизмы реализации этих норм.

## Уголовно-правовая характеристика главы 28 УК РФ Преступления в сфере компьютерной информации

### Общие признаки преступлений в сфере компьютерной информации

В новом 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.[[13]](#footnote-13)

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 нового УК 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. 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[[14]](#footnote-14) 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).

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.[[15]](#footnote-15)

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, 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.[[16]](#footnote-16)

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.

### Уголовно-правовой анализ ст. 272 гл. 28 УК РФ Неправомерный доступ к компьютерной информации

Расположение ст.272 в главе на первом месте было вызвано поистине катастрофическим положением, сложившимся на отечественном рынке компьютерной информации и вызванным свободным доступом пользователей ПК к информационным ресурсами бесконтрольным копированием последних. Около 98 % копий программных продуктов производится в настоящее время у нас в стране именно таким путем.

Эта статья, которая, как и последующие, состоит из 2 частей, содержит достаточно много признаков, обязательных для объекта, объективной и субъективной сторон состава преступления. Непосредственным объектом ее являются общественные отношения по обеспечению безопасности компьютерной информации и нормальной работы ЭВМ, их системы или сети.

Предметом преступления будет компьютерная машинная информация, содержащаяся на машинном носителе, в ЭВМ, их системе или сети, охраняемая законом, т.е. изъятая из открытого оборота на основании закона, иного нормативного правового акта, а также правил внутреннего распорядка, основанных на названных правовых актах.[[17]](#footnote-17)

Состав преступления сформулирован как материальный, причем если деяние в форме действия определено однозначно (неправомерный доступ к охраняемой законом компьютерной информации), то последствия, хотя и обязательны, могут быть весьма разнообразны: 1) уничтожение информации, 2) ее блокирование, 3) модификация, 4) копирование, 5) нарушение работы ЭВМ, 6) то же — для системы ЭВМ, 7) то же— для их сети. Объективную сторону данного преступления составляет неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.  
Деяние, как видно из диспозиции статьи, предполагает наличие двух обязательных признаков: информация должна охраняться законом, а доступ к ней должен быть неправомерен.  
По делам о данном преступлении должно быть установлено, что компьютерная информация, к которой осуществлен доступ, охраняется законодательством о государственной тайне, о собственности, об авторском праве или др., что самим фактом несанкционированного к ней доступа нарушены прерогативы государства, права собственника, владельца, автора или др. юридического либо физического лица. В силу ст. 6 Федерального закона "Об информации, информатизации и защите информации" информационные ресурсы находятся в собственности юридических и физических лиц, включаются в состав их имущества и на них распространяется действие гражданского законодательства.  
Неправомерным следует признать доступ в закрытую информационную систему лица, не являющегося законным пользователем либо не имеющего разрешения для работы с данной информацией. Способы такого доступа: использование чужого имени, изменение физического адреса технического устройства, подбор пароля, нахождение и использование “пробелов” в программе, любой другой обман системы защиты информации.

Несанкционированное проникновение к органам управления ЭВМ или в сеть ЭВМ следует рассматривать как приготовление к доступу к компьютерной информации.

Данная статья уголовного закона предусматривает ответственность за неправомерный доступ к информации, лишь если она запечатлена на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

Машинные носители, к которым относят всякого рода магнитные диски, магнитные ленты, магнитные барабаны, перфокарты, полупроводниковые схемы и др., классифицируются в зависимости от их физических и конструктивных особенностей.

Компьютерная информация может также содержаться в памяти ЭВМ, которая реализуется через перечисленные машинные носители, используемые как запоминающие устройства - внешние, (например, дискета), или внутренние, включенные в конструкцию ЭВМ. Запоминающее устройство, реализующее внутреннюю память ЭВМ, непосредственно связано с процессором и содержит данные, непосредственно участвующие в его операциях.

Компьютерная информация может передаваться по телекоммуникационным каналам из одной ЭВМ в другую, из ЭВМ на устройство отображения (дисплей, например), из ЭВМ на управляющий датчик оборудования. Телекоммуникационные каналы с соответствующим программным обеспечением связывают отдельные ЭВМ в систему или сеть.

Таким образом, данная норма уголовного законодательства оберегает компьютерную информацию, где бы она ни содержалась и ни циркулировала: в памяти ЭВМ, в каналах связи, на обособленных от ЭВМ машинных носителях.

Неправомерный доступ к записям программ для ЭВМ, к первичным документам баз данных и другой подобной информации, выполненной в виде записи рукой человека, отпечатанной на машинке или принтере, набранной типографским способом, не подразумевается в данной норме уголовного закона, и может, в соответствующих случаях, повлечь ответственность лишь по другим статьям Особенной части УК (ст. 137, 138, 183 и др.).

Моментом окончания деяния является момент отсылки пользователя компьютеру последней интерфейсной команды вызова хранящейся информации, независимо от наступления дальнейших последствий. Однако преступлением это деяние станет только лишь при наличии последнего условия. Все действия, выполненные до подачи последней команды, будут образовывать состав неоконченного преступления.

Что касается преступных последствий, то под уничтожением информации следует понимать такое изменение ее состояния, при котором она перестает существовать в силу утраты основных качественных признаков, (имеющаяся у пользователя возможность восстановить уничтоженную информацию с помощью средств программного обеспечения или получить данную информацию от другого пользователя не освобождает виновного от ответственности); под блокированием - невозможность доступа к ней со стороны законного пользователя; под модификацией — видоизменение, характеризующееся появлением новых (очевидно, нежелательных) свойств; под копированием — получение точного пли относительно точного воспроизведения оригинала (опять-таки без соответствующей санкции); под нарушением работы — остановку действия программы, ее зацикливание, замедление работы, нарушение порядка выполнения команд, ущерб самой аппаратной части, разрыв сети и другие последствия.

С субъективной стороны преступление характеризуется только умышленной формой вины. При этом по отношению к действию умысел может быть только прямым, о чем свидетельствует и использование законодателем термина “неправомерный”, а к факту наступления последствий – как прямым, так и косвенным. Лицо должно осознавать общественную опасность своего действия, предвидеть возможность или неизбежность наступления общественно опасных последствий и желать их наступления, либо сознательно допускать их, либо относиться к ним безразлично. Естественно, установление наличия в деянии виновного умысла, а не неосторожности, будет затруднено, хотя бы потому, что при различных состояниях вычислительной системы (причем часто неизвестных преступнику) одни и те же действия могут приводить к разным последствиям.[[18]](#footnote-18)

Необходимо, конечно, отличать уголовное преступление от дисциплинарного проступка. Например, не будут являться преступлением действия работника, нарушившего установленный приказом по предприятию порядок пользования компьютером вне каких-либо корыстных целей.

Субъектом преступления, указанного ч. 1 ст. 272, может быть любое вменяемое физическое лицо, достигшее 16 лет, в том числе и законный пользователь, который не имеет разрешения для работы с информацией определенной категории. Санкция основного состава альтернативно предусматривает три вида наказаний, штраф, исправительные работы и лишение свободы. Первый, в свою очередь, может быть двух видов, кратный минимальному размеру оплаты труда от 200 до 500 и кратный размеру зарплаты или иного дохода осужденного период от 2 до 5 месяцев. Исправительные работы могут быть назначены в размере от 6 месяцев до 1 года, а лишение свободы — от 6 месяцев до 2 лет.

Часть 2 ст. 272 предусматривает в качестве квалифицирующих признаков несколько новых, характеризующих объективную сторону и субъект состава. Это совершение деяния: 1)группой лиц по предварительному сговору; 2) организованной группой; 3) лицом с использованием своего служебного положения; 4) лицом, имеющим доступ к ЭВМ, их системе или сети. Если описание первых двух признаков дано в ст. 35 УК, то специальный субъект двух последних можно трактовать как отдельных должностных лиц, программистов, операторов ЭВМ, наладчиков оборудования, специалистов-пользователей автоматизированных рабочих мест и т.д. Заметим, однако, что вряд ли оправданно отнесение слов “те же действия” — т.е. неправомерный доступ — к лицам, имеющим доступ к ЭВМ, системе, сети, поскольку их обращение к компьютерной информации, чаще всего, правомерно. Санкция за квалифицированные виды данного преступления ужесточена, в нее введен новый вид наказания арест на срок от 3 до 6 мес., размеры остальных увеличены, штраф от 500 до 800 минимальных размеров оплаты труда или зарплаты за период от 5 до 8 месяцев; исправительные работы от 1 года до 2 лет; лишение свободы до 5 лет.

### Уголовно-правовой анализ ст. 273 гл. 28 УК РФ Создание, распространение и использование вредоносных программ для ЭВМ

Статья 273 явилась преемницей ст. 269 проекта УК “Создание, использование и распространение вирусных программ”. Смена дефиниций произошла не случайно: дело в том, что под “компьютерным вирусом” в теории программирования понимается такая совокупность машинного кода, которая сама может создавать свои копии и внедрять их в файлы, системные области ЭВМ, вычислительные сети и т. д. При этом копии не обязательно полностью совпадают с оригиналом, могут становиться совершеннее его и сохраняют способность дальнейшего самораспространения.

В случае принятия только такого типа программ в качестве средства совершения данного преступления произошло бы неоправданное смещение в понимании такового средства. Во-первых, компьютерный вирус может быть безвредным, и карать за его внесение при помощи уголовного закона было бы бессмысленным, а во-вторых, существует множество программ другого типа, приводящих к столь же нежелательным последствиям, как и в случае действия вредоносных вирусов. Они используются для хищения денег с банковских счетов, шпионажа, в хулиганских целях, из мести и т. д.

Общественная опасность рассматриваемого преступления состоит, с одной стороны, в возможности наступления в результате его всех последствий, которые мы называли, говоря о вредоносности компьютерной преступности вообще, а с другой стороны, в том, что существующие операционные системы MS-DOS и WINDOWS практически прозрачны для программ такого типа. С распространением персональных компьютеров вирусы поистине стали их бедствием. В настоящее время в мире существует порядка 20 тыс. только активно действующих вирусов, и число их постоянно растет, вызывая создание новых и новых антивирусных программ.

Преступление, предусмотренное ст. 273, наиболее опасное из содержащихся в главе 28, что отражено в санкции за него.

Непосредственным объектом данного преступления являются общественные отношения по безопасному использованию ЭВМ, ее программного обеспечения и информационного содержания. Состав части первой формальный и предусматривает совершение одного из действий: 1) создание программ (очевидно, вернее — “программы”) для ЭВМ, заведомо приводящих (приводящей) к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы аппаратной части; 2) внесение в существующие программы изменений, обладающих аналогичными свойствами; 3) использование двух названных видов программ; 4) их распространение; 5) использование машинных носителей с такими программами; 6) распространение таких носителей. Создание и изменение программы — это изготовление и преобразование описанного на языке ЭВМ машинного алгоритма.

Использование программы для 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. Использование вредоносной программы для ЭВМ для личных нужд (например, для уничтожения собственной компьютерной информации) не наказуемо.

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 также создание условий для самораспространения программы.

Последствия всех этих действий (равно как и момент окончания деяния) аналогичны таковым для предыдущей статьи, однако в данном случае для признания деяния преступлением не обязательно их наступление. Дело в том, что внесенная в компьютер вредоносная программа может благополучно “спать” в нем в течение многих лет и сработать тогда, когда ее автор будет вне пределов досягаемости закона, да и установление самого авторства будет практически невозможно. Кроме того, само совершение перечисленных действий уже столь опасно, что излишне дожидаться наступления вреда от них.

Обязательными признаками объективной стороны ч. 1 ст. 273 будут два, характеризующих способ и средство совершения преступления. Это, во-первых, то, что последствия должны быть несанкционированными, во-вторых, наличие самой вредоносной программы или изменения в программе. Последними, кроме названного компьютерного вируса, могут быть хорошо известные программистам “троянский конь”, “логическая бомба”, “люк”, “асинхронная атака” и другие.

С субъективной стороны состав данного преступления характеризуется виной в форме прямого умысла: когда виновный осознавал общественную опасность своих действий, предвидел возможность либо даже неизбежность наступления опасных последствий, но, тем не менее, желал эти действия совершить. Субъект преступления — общий (лицо достигшее 16 лет).   
Частью 2 ст. 273 криминализируется более опасное преступление: те же деяния, повлекшие тяжкие последствия. Это — преступление с материальным составом и с двумя формами вины: по отношению к действиям присутствует умысел, а к общественно опасным последствиям — неосторожность, легкомыслие или небрежность.

“Тяжкие последствия” — оценочное понятие, наличие их в каждом конкретном случае определяется, исходя из особенностей дела. Согласно п.8 постановления Пленума Верховного Суда Российской Федерации от 29 апреля 1996г. №1 суд, признавая подсудимого виновным в совершении преступления по признакам, относящимся к оценочным категориям (тяжкие или особо тяжкие последствия, крупный или значительный ущерб, существенный вред и др.), не должен ограничиваться ссылкой на соответствующий признак, а обязан привести в описательной части приговора обстоятельства, послужившие основанием для вывода о наличии в содеянном указанного признака. В данном случае под тяжкими последствиями можно понимать смерть одного или нескольких человек, причинение тяжкого вреда здоровью, катастрофы, серьезную дезорганизацию работы, крупный материальный ущерб и т. п.[[19]](#footnote-19)

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

### Уголовно-правовой анализ ст. 274 гл. 28 УК РФ Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Целью действия ст. 274 должно быть предупреждение неисполнения пользователями своих профессиональных обязанностей, влияющих на сохранность хранимой и перерабатываемой информации. Непосредственный объект преступления, предусмотренного этой статьей,— отношения по соблюдению правил эксплуатации ЭВМ, системы или их сети, т. е. конкретно аппаратно-технического комплекса. Под таковыми правилами понимаются, во-первых, Общероссийские временные санитарные нормы и правила для работников вычислительных центров, во-вторых, техническая документация на приобретаемые компьютеры, в-третьих, конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка. Применительно к данной статье под сетью понимается только внутренняя сеть ведомства или организации, на которую может распространяться его юрисдикция. В глобальных сетях типа Интернет отсутствуют общие правила эксплуатации, их заменяют этические "Кодексы поведения", нарушения которых не могут являться основанием для привлечения к уголовной ответственности.   
Нарушение правил эксплуатации ЭВМ может быть осуществлено путем, как активного действия, так и бездействия. Состав ч.1 сформулирован как материальный. При этом общественно опасные последствия заключаются в одновременном наличии двух факторов: 1) уничтожения, блокирования или модификации охраняемой законом информации ЭВМ; 2) вызванного этим существенного вреда. Поскольку речь идет о правилах эксплуатации именно ЭВМ, т. е. аппаратно-технической структуры, то и нарушение их должно затрагивать только техническую сторону несоблюдения требований безопасности компьютерной информации, а не организационную или правовую.[[20]](#footnote-20) К таковым можно отнести: блокировку системы защиты от несанкционированного доступа, нарушение правил электро- и противопожарной безопасности, использование ЭВМ в условиях, не отвечающих тем, которые установлены документацией по ее применению (по температурному режиму, влажности, величине магнитных полей и т. п.), отключение сигнализации, длительное оставление без присмотра и многие другие.

Однако все эти действия будут интересовать нас не самостоятельно, а только лишь в связи с угрозой безопасности хранимой в ЭВМ и охраняемой законом информации. Правонарушение может быть определено как преступление только при наступлении существенного вреда. Под последним следует понимать, прежде всего, вред, наносимый информации в ее значимой, существенной части. Это, например, уничтожение, блокирование, модификация ценной информации (относящейся к объектам особой важности, либо срочной, либо большого ее объема, либо трудно восстановимой или вообще не подлежащей восстановлению и т.д.); уничтожение системы защиты, повлекшее дальнейший ущерб информационным ресурсам; широкое распространение искаженных сведений и т.п.

В случае если нарушение правил эксплуатации ЭВМ повлекло также и совершение лицом другого преступления, деяния должны быть квалифицированы по совокупности, если другое преступление наказывается более строго. Если другое преступление наказывается более мягко, то следует считать, что наступившие неблагоприятные последствия уже подразумеваются данной нормой уголовного закона.  
Ю. Ляпунов и В. Максимов считают, что данное преступление совершается лишь с прямым или косвенным умыслом.[[21]](#footnote-21) Однако, с точки зрения многих авторов, например учебника уголовного права[[22]](#footnote-22), преступление, предусмотренное ч.1 ст. 274 УК может быть совершено (и чаще всего совершается) по неосторожности.

Мотив и цель виновного для квалификации содеянного значения не имеют, но могут быть учтены при назначении наказания. Субъект данного преступления специальный — лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети программист, оператор ЭВМ, техник по обслуживанию и т. п..[[23]](#footnote-23)

Квалифицирующим признаком ч.2 ст. 274 УК является наступление тяжких последствий. Их содержание, очевидно, аналогично таковому для ч. 2 ст. 273. Это состав с двумя формами вины. Субъективная сторона характеризуется неосторожной формой вины по отношению к последствиям. Санкция нормы существенно отличается от предыдущей, только лишение свободы до 4 лет.

Очевидно, что введение уголовной ответственности за компьютерные преступления – необходимое, но недостаточное условие для эффективной борьбы с ними.

Наряду с уголовно-правовой, гражданско-правовой и административно-правовой охраной программного обеспечения ЭВМ существенным элементом в искоренении такого рода правонарушений стало создание специальных подразделений (в рамках правоохранительных органов) по борьбе с компьютерной преступностью, в частности ОБКП при МВД РБ.

# КВАЛИФИКАЦИЯ ПРЕСТУПЛЕНИЙ

## Понятие квалификации преступлений

Проблема квалификации преступления является не только одной из наиболее сложных в уголовном праве, но и наиболее значимой для практики расследования и судебного разбирательства.

Под квалификацией преступления понимается установление и юридическое закрепление точного соответствия между физическими признаками совершенного деяния и признаками состава преступления, предусмотренного уголовно-правовой нормой.[[24]](#footnote-24)

То есть квалификация – это последовательный логический процесс, направленный на установление признаков, предусмотренных применяемой уголовно – правовой нормой, в совершенном деянии.

Предпосылками правильной квалификации можно назвать:

точное и полное установление фактических обстоятельств дела;

глубоко профессиональное их изучение;

определение примерного круга норм, под действие которых может подпадать совершенное деяние;

сопоставление признаков преступлений, названных в диспозициях выделенных для анализа статей УК, с признаками совершенного деяния;

разграничение смежных составов преступлений;

построение вывода и закрепление в процессуальном документе окончательной квалификации, заключающейся в указании соответствующей статьи или пункта, части статьи Особенной части УК, предусматривающий уголовную ответственность за данный вид преступления, в указании (в случае необходимости) статьи Общей части УК, устанавливающей ответственность за неоконченную преступную деятельность, соучастие, множественность преступлений и т.д.[[25]](#footnote-25)

Таким образом, необходимым и решающим условием правильной квалификации является точный правовой анализ признаков совершенного преступления и установления тождества фактических обстоятельств преступления и признаков соответствующей уголовно-правовой нормы.

## Особенность квалификации преступлений в сфере компьютерной информации

При квалификации преступлений в сфере компьютерной информации могут возникнуть многочисленные вопросы, касающиеся отграничений этих преступлений как между собой, так и от иных видов преступных посягательств, предметом которых является информация, находящаяся на машинном носителе, в ЭВМ, системе ЭВМ или их сети. К числу таких преступлений следует отнести: нарушение неприкосновенности частной жизни (ст. 137 УК РФ); нарушение авторских и смежных прав (ст. 146 УК РФ); незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ), продажа, сдача в прокат и иное незаконное использование экземпляров произведений или фонограмм (ст. 150.4 КОАП РСФСР) и некоторые другие.

### Разграничения ст.ст.272 и 273 УК РФ

Сложность разграничения ст. ст. 272 и 273 УК РФ в том, что неправомерный доступ к компьютерной информации и создание, использование и распространение вредоносных программ для ЭВМ ведут к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ или их сети. Причем создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к указанным выше вредным последствиям, вполне могут сочетаться с неправомерным доступом к компьютерной информации, что свидетельствует о прикладном характере разграничения этих преступлений.[[26]](#footnote-26)

Первым критерием разграничения ст.ст. 272 и 273 УК РФ является предмет преступления. В ст. 272 УК РФ предметом преступления выступает та информация, которая охраняется законом, а в ст. 273 УК РФ – любая информация (как охраняемая законом, так и не охраняемая), содержащаяся на машинном носителе, в ЭВМ, системе ЭВМ или их сети. По соответствующей части ст. 273 УК РФ следует квалифицировать действия виновного, совершившего неправомерный доступ к программе ЭВМ, не имеющей специального правового статуса, т.е. не охраняемой законом, если это деяние было связано с ее модификацией, заведомо приводящей к вредным последствиям, указанным в диспозиции ст. 273 УК РФ. Признаки состава неправомерного доступа к компьютерной информации в этом случае отсутствуют.

Вторым критерием разграничения ст.ст. 272 и 273 УК РФ является содержание общественного опасного деяния. Ст. 273 предполагает совершение хотя бы одного из следующий действий: создание вредоносной программы (вредоносных программ) для ЭВМ, внесение изменений в существующие программы для ЭВМ, с доведением их до качества вредоносных, использование вредоносных программ для ЭВМ, использование машинных носителей, содержащих вредоносные программы для ЭВМ, распространение вредоносных программ для ЭВМ, распространение машинных носителей, содержащих вредоносные программы для ЭВМ. Состав, предусмотренный ч.1 ст. 273 УК РФ, сконструирован как формальный. Для признания преступления оконченным не требуется реального наступления вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения общественно опасного деяния, если оно создавало реальную угрозу одного из перечисленных выше последствий. Для преступления, предусмотренного ст. 272 УК РФ, суть общественно опасного деяния заключается в неправомерном доступе к компьютерной информации, причем состав неправомерного доступа сконструирован как материальный. Оконченным это преступление будет тогда, когда наступят вредные последствия, находящиеся в причинной связи с поведенческим актом виновного.

В том случае, если виновный умышленно создает вредоносную программу для ЭВМ или вносит изменения в существующую программу, доводя ее до качества вредоносной, а равно использует либо распространяет такие программы или машинные носителя с такими программами и при этом не совершает неправомерного доступа к охраняемой законом компьютерной информации, то его действия подлежат квалификации по ст. 273 УК РФ.

В случае, когда виновный в целях создания вредоносной программы для ЭВМ, неправомерно вызывает существующую программу, являющуюся, например, объектом авторского права, а значит охраняемую законом и вносит в нее соответствующие изменения, иными словами, модифицирует компьютерную информацию, налицо совокупность преступлений, предусмотренных ст.ст. 272 и 273 УК РФ. Например, в настоящее время, в сети Интернет можно свободно переписать программу-взломщик правовой базы данных «Консультант-Плюс» стоимостью около $1000 и при помощи нее взломать систему защиты этой программы, другими словами модифицировать – вот простой пример совокупности преступлений, предусмотренных ст.ст.272 и 273 УК РФ.

Так как диспозиция ст. 273, говоря о создании программ для ЭВМ, внесении изменений в существующие программы, использование либо распространение таких программ или машинных носителей с такими программами, не охватывает содержанием факт неправомерного доступа к компьютерной информации, то деяние виновного подлежат дополнительной квалификации по ст. 272 УК РФ.

Как покушение на создание, использование, распространение вредоносных программ для ЭВМ и оконченный состав неправомерного доступа к компьютерной информации следует оценивать поведение лица, который неправомерно вызвав существующую программу для ЭВМ и внеся в нее ряд изменений, не сумело в силу различного рода причин, выходящих за рамки сознания и воли виновного, довести эту программу до качества вредоносной.

Если же действия виновного были пресечены на более ранней стадии, например в момент неправомерного доступа к компьютерной информации, и не были связаны с ее модификацией, налицо приготовление к созданию, использованию и распространению вредоносных программ для ЭВМ и покушение на неправомерный доступ к компьютерной информации.

С субъективной стороны преступление, предусмотренное ч.1 ст.273 УК РФ, может быть совершено как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям. Неправомерный доступ к компьютерной информации может быть совершен только с прямым умыслом, мотивы преступления могут быть корыстные или хулиганские побуждения, месть, зависть и т.п.[[27]](#footnote-27)

Итак, отличие ст. 272 УК РФ от ст. 273 УК РФ следует искать в юридической характеристике предмета преступления, посягательства, содержании общественно – опасных действий, приводящих к вредным последствиям, и субъективной стороне, дающей представление об отношении субъекта к содеянному и его последствиям.

### Разграничения ст.ст.272 и 274 УК РФ

Ст. 272 УК РФ и ст. 274 УК РФ содержат следующие отличия. Согласно ст. 272 УК РФ виновный не имеет права доступа к компьютерной информации, знакомиться с ней и распоряжаться, то есть действует несанкционированно. По ст. 274 УК РФ, виновный, в силу занимаемого служебного положения или выполнения функциональных обязанностей, вызывает компьютерную информацию правомерно, т.е. действует в этом плане на законных основаниях. По ст. 274 УК РФ субъект посягательства – законный пользователь компьютерной информации.

Неправомерный доступ к компьютерной информации – преступление, совершаемое только путем активных действий, в то время как нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети может быть совершено как действием, так и путем бездействия (например, виновный не включает систему защиты информации от несанкционированного доступа к ней, оставляет без присмотра свое рабочее место и т.д.).[[28]](#footnote-28)

Необходимым признаком объективной стороны обоих преступлений выступают общественно опасные последствия, которые по своему содержанию и объему неравнозначны. Ответственность по ст. 274 УК РФ наступает в том случае, если уничтожение, блокирование или модификация охраняемой законом компьютерной информации причинило существенный вред потерпевшему. Что касается существенности ущерба, причиненного нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети, то это оценочное понятие, которое зависит в каждом конкретном случае от многих показателей, относящихся к применяемым техническим средствам, к содержанию информации, степени повреждения и многим другим показателям, которые должны оцениваться следователем и судом.[[29]](#footnote-29) Для привлечения к ответственности по ст. 272 УК РФ причинение существенного вреда не требуется, достаточно установить сам факт уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети.

Закон не предусматривает ответственности за нарушение правил эксплуатации ЭВМ или их сети, если это деяние повлекло копирование информации, даже причинившее существенный вред. Это свидетельствует о неравнозначном подходе законодателя к объему преступных последствий, выступающих в качестве обязательных признаков для составов преступлений, предусмотренных ст.ст. 272 и 274 УК РФ.

### Разграничения ст.ст.272 и 146 УК РФ

Ст. 272 УК РФ и ст. 146 УК РФ можно разграничить по следующим признакам. В первую очередь, по объекту преступления: в ст. 272 УК РФ – это общественные отношения по обеспечению безопасности компьютерной информации ЭВМ, системы ЭВМ или их сети; в ст. 146 УК РФ – общественные отношения, обеспечивающие авторские и смежные права, регулируемые нормами гражданского и международного права.

Предметом посягательства в ст. 272 УК РФ является компьютерная информация, охраняемая законом, а в ст. 146 УК РФ – только объекты авторского права, к которой действующее законодательство России относит, в частности, программы для ЭВМ и базы данных.

Так, например, 6 отделом УРОПД при ГУВД Санкт-Петербурга и области 2 сентября 1998 г. было возбуждено уголовное дело по признакам преступления, предусмотренного ст.273 УК РФ по факту распространения компакт-дисков с программами, предназначенными для снятия защиты с программных продуктов, а также "взломанных" версий программ, "крэки " (программы-взломщики) в данном случае были признаны следствием вредоносными программами. Также обвинение было в ходе следствия дополнено статьей 146 УК.[[30]](#footnote-30) Однако, мы не знаем, всех обстоятельств данного уголовного дела и поэтому трудно делать выводы о правильности дополнительной квалификации по ст. 146 УК РФ, т.к. неизвестно – являлись ли «взломанные» программы контрафактными или нет и причинили ли виновные крупный ущерб автору эти программ.

Потерпевший по ст. 272 УК РФ – любое физическое или юридическое лицо, общество, государство, а по ст. 146 УК РФ – только автор (физическое лицо или группа физических лиц) того или иного объекта авторского права.

Объективная сторона нарушения авторских и смежных прав в качестве необходимого признака включает наступление общественно – опасных последствий в виде причинения крупного ущерба автору объекта авторского права в форме упущенной выгоды или морального вреда. Наступление же общественно - опасных последствий (предусмотренных ст. 146 УК РФ) не является обязательным для привлечения к уголовной ответственности по ст. 272 УК РФ. Здесь достаточно установить реально объективированные последствия в виде уничтожения, блокирования, модификации либо копирования информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Нарушение авторских и смежных прав связано либо с присвоением авторства, либо с незаконным использованием объектов авторского права. При неправомерном доступе к компьютерной информации ее дальнейшее использование виновным не обязательно.

Если виновный, желая нарушить охраняемые законом права автора, вызывает компьютерную программу, копирует ее и воспроизведенные копии использует в своих преступных целях, содеянное виновным необходимо квалифицировать по совокупности ст. 146 и 272 УК РФ, если законному автору программы был причинен крупный ущерб, так как диспозиция ст. 272 УК РФ не охватывает своим содержанием факт незаконного использования объектов авторского права или присвоение авторства, равно как и диспозиция ст. 146 УК РФ – факт неправомерного доступа к охраняемой законом компьютерной информации. Однако на практике, по крайней мере, в Республике Бурятия, ст. 146 УК РФ по отношению к использованию программных продуктов без имеющегося лицензионного соглашения применяется крайне редко, в 98% данные правонарушения квалифицируются по ст.150.4 КОАП РСФСР «Продажа, сдача в прокат и иное незаконное использование экземпляров произведений или фонограмм», т.к. это в основной массе контрафактными оказываются программы зарубежных производителей и доказывать причинение крупного ущерба, скажем, корпорации Microsoft не представляется возможным. По статистике, из 81 проверенной на использование нелецензионного программного обеспечения организаций, 15 – оштрафованы на 5-10 МРОТ, остальным вынесено предупреждение.

### Разграничения ст.ст.272 и 137 УК РФ

Объектом преступления ст. 137 УК РФ является неприкосновенность личного суверенитета человека, сфера его частной жизни и личных отношений. Неправомерный доступ к компьютерной информации, содержащей сведения о частной жизни лица, составляющие его личную или семейную тайну, представляет собой специфическую разновидность сбора этих сведений – иными словами, совершение действий, образующих оконченный состав нарушения неприкосновенности частной жизни.

Неправомерный доступ к компьютерной информации, содержащей сведения о частной жизни лица, совершенный с прямым умыслом и из корыстной или иной личной заинтересованности, при условии причинения вреда правам и законным интересам граждан, квалифицируется по совокупности со ст. 137 УК РФ. Виновный здесь, наряду с неприкосновенностью частной жизни, посягает и на общественные отношения по обеспечению безопасности компьютерной информации. Кроме того, санкция ст. 137 УК РФ гораздо мягче санкции, предусмотренной ст. 272 УК РФ, что свидетельствует о необходимости квалифицировать подобное проявление преступной деятельности по совокупности преступлений.[[31]](#footnote-31)

По ст. 137 УК РФ следует квалифицировать лишь такие действия лица, которые были связаны с незаконным ознакомлением с компьютерной информацией, содержащей сведения о личной жизни или семейной тайне потерпевшего. В этом случае дополнительной квалификации по ст. 272 УК РФ не требуется. Но если виновный не только ознакомился, но и уничтожил такую информацию, то содеянное надлежит квалифицировать по совокупности со ст. 272 УК РФ, т.к. в этом случае виновный нарушает не только конституционные права потерпевшего (право на неприкосновенность частной жизни), но и посягает на отношения по обеспечению безопасности компьютерной информации.

Неправомерный доступ к компьютерной информации, содержащей сведения о частной жизни лица, совершенный по иным мотивам, например из чувства сострадания к потерпевшему, не образует признаков преступления, предусмотренного ст. 137 УК РФ – в этом случае есть все основания привлекать виновного к ответственности по ст. 272 УК РФ при условии наступления перечисленных в диспозиции статьи вредных последствий.

### Разграничения ст.ст.272 и 183 УК РФ

В ст. 183 УК РФ обязательным признаком субъективной стороны данного преступления является цель – разглашение либо незаконное использование сведений, составляющих коммерческую или банковскую тайну (ч.1 ст. 183 УК РФ), или мотив преступления - корыстная или иная личная заинтересованность (ч.2 ст. 183 УК РФ). Неправомерный доступ к указанным в ст. 183 УК РФ сведениям, содержащимся на машинном носителе, в ЭВМ, системе ЭВМ или их сети, совершенный без цели их дальнейшего использования или разглашения, а равно без корысти или иной личной заинтересованности, влечет ответственность по ст. 272 УК РФ. Признаки состава преступления, предусмотренного ст. 183 УК РФ в этом случае отсутствуют.

Ярким примером может послужить уголовное дело, рассмотренное Тагилстроевским районным судом города Нижнего Тагила Свердловской области по обвинению Р. по ст. 159, 183, 272, 273 УК. В октябре-ноябре 1998 года Р., пользуясь своим служебным положением, совершил изменение ведомости начисления заработной платы на предприятии так, что у работников, которым начислялось более ста рублей, списывалось по одному рублю, эти средства поступали на счет, откуда их впоследствии снял Р. Изменения в программе были квалифицированы по статье 273, сбор сведений о счетах лиц, данные о которых были внесены в базу предприятия, - по статье 183, модификация этих данных - по статье 272, а получение начисленных денежных средств - по статье 159 УК. Р. был приговорен к 5 годам лишения свободы условно с лишением права заниматься профессиональной деятельностью программиста и оператора ЭВМ сроком на 2 года.[[32]](#footnote-32)

### Разграничения ст.ст.272 и 165 УК РФ

Рассматриваемые преступные деяния зачастую являются способом совершения корыстных преступлений: причинение имущественного ущерба путем обмана или злоупотребления доверием, мошенничества, присвоения или растраты и др. В таких случаях имеет место идеальная совокупность преступлений, что, прежде всего, определяется различием объектов посягательства. Причинение имущественного ущерба путем обмана или злоупотребления доверием, совершенное путем неправомерного доступа к компьютерной информации, следует квалифицировать по совокупности преступлений, предусмотренных ст. 165 и ст.272 УК РФ.

Такие преступления наиболее часто встречаются на практике из-за широкого распространения сети Интернет.

Например, 18 апреля 2000 года Шадринским городским судом был осужден к штрафу в 3000 рублей П., по статьям 272 и 165 (Причинение имущественного ущерба путем обмана или злоупотребления доверием) УК РФ. П. получал доступ к сети Интернет за чужой счет, пользуясь чужими логином и паролем для доступа к сети. Логин и пароль он получил, прислав программу - "троянца" на компьютер-"жертву". В рассматриваемом примере суд квалифицировал несанкционированный доступ к чужому компьютеру с целью кражи пароля по статье 272, а пользование услугой доступа к интернет - по статье 165 УК. В данном случае обращает на себя внимание тот факт, что "троянскую" программу П., согласно его же собственным показаниям, послал на компьютер с предназначенной специально для этого страницы на сервере в Интернет, адреса которой он "не помнит".[[33]](#footnote-33) Можно предположить, что, говоря про такую страницу, П. просто избежал обвинения еще и по статье 273 УК в распространении вредоносных программ, что, впрочем, доказать уже невозможно.

Злоупотребление доверием также не остается без внимания преступников: Октябрьским районным судом г. Улан-Удэ было рассмотрено уголовное дело по обвинению Б. и Р. в совершении преступлений предусмотренных ст.ст. 272 ч.2., 165 ч.2 УК РФ. Р. воспользовавшись доверием главного врача ГСЭН, попросившей его устранить неисправность компьютерной техники, получил доступ к компьютеру ГСЭН, узнал не подлежащий разглашению логин и пароль выхода в сеть Интернет и сообщил эти данные своему знакомому Б., который за счет ГСЭН осуществлял фактическое пользование услугами сети, кроме этого Б. совершил неправомерный доступ в сеть и, воспользовавшись ошибкой администратора сети, скопировал конфиденциальную информацию, содержащую пароли пользователей (в виде файла master.password), после чего предпринял попытку дешифрования паролей с помощью компьютерных программ для взлома паролей. В свою очередь Р., проходя практику и имея доступ к компьютеру, блокировав пароль для защиты доступа, совершил неправомерный доступ к компьютерной информации и скопировал на внешнее устройство файлы, содержащие сведения конфиденциального характера. Казалось бы налицо совокупность преступлений предусмотренных ст. 165 и ст.272 УК РФ, однако, что касается Б. то файлы имеющие конфиденциальный характер находились в сети Интернет без какой-либо должной защиты, наряду с любыми другими файлами (из-за ошибки администратора сети) и могли быть скопированы любым пользователем сети Интернет. А Б., при этом, не применял при специальных программ для взлома. Таким образом в действиях Б. отсутствует состав преступления предусмотренный ст. 272 ч.2 УК РФ. Действия же подсудимого Р. квалифицированы по ст. 272 УК РФ правильно, т.к. он осуществил неправомерный доступ к охраняемой законом компьютерной информации, что повлекло ее копирование.

Таким образом, суд правильно квалифицировал данные деяния и признал Б. – виновным по ст. 165 ч.2 УК РФ и назначил наказание в виде штрафа 2400 руб., Р. – по ст. 272 ч.2 УК РФ и назначил ему наказание в виде штрафа 3000 руб.[[34]](#footnote-34)

## Значение квалификации преступлений

Правильная квалификация преступления имеет важное значе­ние. Она обеспечивает реализацию принципов уголовного права и прежде всего законности. Неверная квалификация нарушает принцип законности, равно как и принципы справедливости, личной и виновной ответственности. Цели наказания, его инди­видуализация и справедливость могут быть достигнуты только при верной квалификации преступления. Ошибочность ее может по­влечь, и зачастую влечет, самые тяжкие последствия, в числе которых, например, применение необоснованно суровых мер на­казания (длительных сроков лишения свободы).

Правильная квалифи­кация в то же время является гарантией соблюдения прав лица, совершившего преступления. Неверное применение нормы Осо­бенной части влечет не только назначение несправедливого на­казания, но и другие негативные последствия. Неверная оценка действий как создание, использование и распространение вредоносных программ для ЭВМ (ч. 2 ст. 273 УК), относяще­гося по закону к тяжким преступлениям (ч. 4 ст. 15 УК), означает, как правило, неприменение условного осуждения, отсрочки ис­полнения приговора, определение более сурового вида режима отбывания наказания, существенное увеличение сроков для ус­ловно-досрочного освобождения от него и т.п. Наконец, верная квалификация дает возможность более точно и обоснованно вы­явить состояние, уровень и динамику преступности и ее отдель­ных видов как в целом по Российской Федерации, так и по отдельным регионам. Ошибочная квалификация ведет к искаже­нию действительной картины и негативно влияет на разработку и реализацию профилактических мер.

Рассматривая же судебную практику по статьям УК о преступлениях в сфере компьютерной информации, стоит отметить прежде всего ее несформированность и, вследствие этого, неоднородность. В настоящее время Верховным судом не принято ни одного постановления или определения по вопросам применения статей о компьютерных преступлениях. Приговоры, вынесенные различными судами по однотипным уголовным делам, зачастую расходятся в вопросах квалификации действий преступника и размеров наказания.

В ниже приведенных примерах представляется, что квалифицированы действия обвиняемых по ним были не совсем правильно. В подобного рода делах несформированность практики применения статей УК о компьютерных преступлениях становится особенно заметной.

9 ноября 1998 года УРОПД ГУВД Московской области было возбуждено уголовное дело по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах одного из частных предпринимателей города Павловский Посад. По статье 272 УК в ходе следствия было квалифицировано изменение информации в контрольно-кассовых аппаратах, при которых записанная в них сумма выручки за смену искусственно занижалась. Контрольно-кассовые аппараты были признаны следствием разновидностью электронно-вычислительной машины.

1 сентября 1999 года следственной частью следственного управления при УВД Южного административного округа г. Москвы было возбуждено уголовное дело по признакам преступления, предусмотренного ст.272 УК, по обвинению П.   
В ходе следствия обвинение было дополнено статьями 273, 165, 327 (Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков), 183. По статье 272 было квалифицировано пользование телефоном-"двойником", позволяющим производить бесплатные звонки за чужой счет. В рассматриваемом примере сотовый телефон был признан следствием разновидностью ЭВМ, а написание программы, с помощью которой обычный телефон превращался в "двойник", - по статье 273. Информация о серийном и абонентском номерах телефона была признана органами следствия коммерческой тайной, что и обусловило появление в обвинении статьи 183.

Особенно часто попытки вменять статьи о компьютерных преступлениях в случаях, когда совершаются совершенно, казалось бы, не относящиеся к компьютерам действия предпринимаются в случаях мошенничества с сотовыми телефонами. Так, органами предварительного следствия (Ленинский РОВД г. Ставрополя) статья 272 была вменена обвиняемому, пользовавшемуся доработанным сотовым телефоном-"сканером", который позволял производить звонки за чужой счет. Аналогичный случай в 1998 году в Воронеже следователем УРОПД Воронежского УВД по сходному делу, но уже за изготовление подобных телефонов, обвиняемым на предварительном следствии также была вменена 272 статья УК[[35]](#footnote-35), хотя правильнее было бы квалифицировать преступления в обоих случаях по той же 165 статье.

# Заключение

Подводя итоги, нужно отметить, что количество уголовных дел, возбужденных по статьям 272-274 УК РФ, относительно невелико. Однако объясняется это не отсутствием фактов правонарушений или неудовлетворительной работой правоохранительных органов, а их высокой латентностью. Также определенные преграды создают и сами потерпевшие, т.к. многие коммерческие структуры не заинтересованы в разглашении сведений, которые поставят под сомнение надежность их информационных систем. Сложность компьютерной техники и, как мы убедились, неоднозначность квалификации, а также трудность сбора доказательственной информации тормозят пока формирование судебной практики по статьям главы 28 УК.

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

Хотя предусмотренные составы компьютерных преступлений не охватывают полностью всех видов возможных компьютерных посягательств, в целом, они вполне работоспособны и уже сейчас выполняют свою роль. Больным вопросом остается на сегодняшний день защита авторских прав на программы и базы данных, т.к. почти все используемое программное обеспечение в России – нелецензионное, хотя, уже сейчас, многие коммерческие организации предпочитают приобретение лицензионного программного обеспечения - общению с правоохранительными органами. Так что, позитивные шаги в этом направлении налицо.

# БИБЛИОГРАФИЯ

*Нормативно правовые акты:*

1. Конституция Российской Федерации: Принята всенародным голосованием 12 декабря 1993 г.—М: «Проспект». 2000. – 48 с.
2. Уголовный Кодекс Российской Федерации: Федеральный закон РФ от 1 января 1997 г. СПС «КонсультантПлюс»
3. ФЗ "Об информации, информатизации и защите информации" от 20 февраля 1995 г. № 24-ФЗ (СЗ РФ, 1995, № 8, ст.2);

*Учебная и научная литература:*

1. Уголовное право. Особенная часть. Учебник. Под ред. д.ю.н. проф. А.С. Михлина, М.: Юриспруденция, 2000. – с. 289
2. Крылов В. Информационные преступления — новый криминалистический объект Российская юстиция.— 1997.— 4, с. 22
3. Гостев И.М. Информационное право. Вопросы законодательного регулирования Технологии и средства связи,—1997.—май-июнь, с. 98-100
4. Ляпунов Ю., Максимов В. «Ответственность за компьютерные преступления» Юридический консультант.— 1997.— 10, с. 9-15
5. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность Юридический мир.—№ 2 -1998.— февраль, с. 9-19
6. Волчинская Е.К. Есть ли в России компьютерное право; Российская юстиция.— 1997.— 6, с. 9-19
7. Симкин Л. Как остановить компьютерное пиратство; Российская юстиция.— 1996.— 10, с. 37-39
8. Уголовное право. Особенная часть. Учебник. Под ред. И.Я. Козаченко, М.: ИНФРА-М-НОРМА, 1997.
9. Российское уголовное право. Особенная часть Под редакцией В.Н. Кудрявцева, А.В. Наумова.- М., Юрист, 1997.- 496 с.
10. Гульбин Ю. Преступления в сфере компьютерной информации Российская юстиция.— 1997.— 10, с. 24-25
11. Уголовное право России. Особенная часть, Учебник Отв. ред. доктор юридических наук, профессор Б.В. Здравомыслов.- М., Юрист, 1996.- 560 с.
12. Уголовное право России. Особенная часть, Учебник Под ред. проф. А. И. Рарога.- М., Институт международного права и экономики. Издательство “Триада, Лтд”, 1996.- 480 с.
13. Уголовное право Российской Федерации. Особенная часть, Учебник Под ред. Г.Н. Борзенкова и В.С. Комиссарова.- М., Олимп; ООО “Издательство АСТ”, 1997.- 752 с.
14. Уголовное право. Общая часть. Учебник для вузов. Под ред. И.Я.Козаченко, З.А.Незнамова-2 изд.,стер.-М: Издательство НОРМА, 2000. – 124 с.
15. Крылов В.В. Информационные компьютерные преступления. Квалификация. Методика расследования. Основные нормативные акты. Учеб. И практич. Пособие.-М.:Изд. Группа «Инфра-М-Норма»., 1997. – 23 с.
16. Комментарий к УК РФ/ отв. ред. А.В.Наумов.- 2 изд.,перераб. и доп.-М.:Юрист, 2000.-864 с
17. Компьютерная преступность:
18. уголовно-правовые и криминологические проблемы (международная научно-практическая конференция). Государство и право.-2000.-№9.-с.101-106
19. Судебная практика по компьютерным преступлениям (краткий обзор). Протасов П. – <http://law.bugtrag.ru>

1. Уголовное право. Особенная часть. Учебник. Под ред. д.ю.н. проф. А.С. Михлина, М.: Юриспруденция, 2000. – с. 289 [↑](#footnote-ref-1)
2. Гостев И.М. Информационное право. Вопросы законодательного регулирования Технологии и средства связи,—1997.—май-июнь, с. 98-100 [↑](#footnote-ref-2)
3. Закон РФ " О правовой охране программ для электронно-вычислительных машин и баз данных" от 23 сентября 1992 г. № 3523-1 (ст.20); [↑](#footnote-ref-3)
4. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность Юридический мир.— 1998.— февраль, с. 9-19 [↑](#footnote-ref-4)
5. ФЗ "Об информации, информатизации и защите информации" от 20 февраля 1995 г. № 24-ФЗ (СЗ РФ, 1995, № 8, ст.2); [↑](#footnote-ref-5)
6. Крылов В. Информационные преступления — новый криминалистический объект Российская юстиция.— 1997.— 4, с. 22 [↑](#footnote-ref-6)
7. Ляпунов Ю., Максимов В. «Ответственность за компьютерные преступления» Юридический консультант.— 1997.— 10, с. 9-15 [↑](#footnote-ref-7)
8. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность Юридический мир.— 1998.— февраль, с. 9-19 [↑](#footnote-ref-8)
9. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность Юридический мир.— 1998.— февраль, с. 9-19 [↑](#footnote-ref-9)
10. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность Юридический мир.—№ 2 -1998.— февраль, с. 9-19 [↑](#footnote-ref-10)
11. Волчинская Е.К. Есть ли в России компьютерное право; Российская юстиция.— 1997.— 6, с. 9-19 [↑](#footnote-ref-11)
12. Конституция Российской Федерации: Принята всенародным голосованием 12 декабря 1993 г.—М: «Проспект». 2000. – 48 с. [↑](#footnote-ref-12)
13. Симкин Л. Как остановить компьютерное пиратство; Российская юстиция.— 1996.— 10, с. 37-39 [↑](#footnote-ref-13)
14. Уголовное право. Особенная часть. Учебник. Под ред. И.Я. Козаченко, М.: ИНФРА-М-НОРМА, 1997. [↑](#footnote-ref-14)
15. Российское уголовное право. Особенная часть №Под редакцией В.Н. Кудрявцева, А.В. Наумова.- М., Юрист, 1997.- 496 с. [↑](#footnote-ref-15)
16. Гульбин Ю. Преступления в сфере компьютерной информации Российская юстиция.— 1997.— 10, с. 24-25 [↑](#footnote-ref-16)
17. Симкин Л. Как остановить компьютерное пиратство; Российская юстиция.— 1996.— 10, с. 37-39 [↑](#footnote-ref-17)
18. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления Юридический консультант.— 1997.— 10, с. 9-15 [↑](#footnote-ref-18)
19. Уголовное право России. Особенная часть, Учебник Отв. ред. доктор юридических наук, профессор Б.В. Здравомыслов.- М., Юрист, 1996.- 560 с. [↑](#footnote-ref-19)
20. Уголовное право России. Особенная часть, Учебник Под ред. проф. А. И. Рарога.- М., Институт международного права и экономики. Издательство “Триада, Лтд”, 1996.- 480 с. [↑](#footnote-ref-20)
21. Ляпунов Ю., Максимов В. «Ответственность за компьютерные преступления» Юридический консультант.— 1997.— 10, с. 9-15 [↑](#footnote-ref-21)
22. Уголовное право. Особенная часть. Учебник. Под ред. И.Я. Козаченко, М.: ИНФРА-М-НОРМА, 1997. [↑](#footnote-ref-22)
23. Уголовное право Российской Федерации. Особенная часть, Учебник Под ред. Г.Н. Борзенкова и В.С. Комиссарова.- М., Олимп; ООО “Издательство АСТ”, 1997.- 752 с. [↑](#footnote-ref-23)
24. Уголовное право. Общая часть. Учебник для вузов. Под ред. И.Я.Козаченко, З.А.Незнамова-2 изд.,стер.-М: Издательство НОРМА, 2000. – 124 с. [↑](#footnote-ref-24)
25. Уголовное право. Общая часть. Учебник для вузов. Под ред. И.Я.Козаченко, З.А.Незнамова-2 изд.,стер.-М: Издательство НОРМА, 2000. – 124 с. [↑](#footnote-ref-25)
26. Крылов В.В. Информационные компьютерные преступления. Квалификация. Методика расследования. Основные нормативные акты. Учеб. И практич. Пособие.-М.:Изд. Группа «Инфра-М-Норма»., 1997. – 23 с. [↑](#footnote-ref-26)
27. Комментарий к УК РФ/ отв. ред. А.В.Наумов.- 2 изд.,перераб. и доп.-М.:Юрист, 2000.-864 с. [↑](#footnote-ref-27)
28. Компьютерная преступность: уголовно-правовые и криминологические проблемы (международная научно-практическая конференция). Государство и право.-2000.-№9.-с.101-106 [↑](#footnote-ref-28)
29. Комментарий к УК РФ/ отв. ред. А.В.Наумов.- 2 изд.,перераб. и доп.-М.:Юрист, 2000.-864 с. [↑](#footnote-ref-29)
30. Судебная практика по компьютерным преступлениям (краткий обзор). Протасов П. – http://law.bugtrag.ru [↑](#footnote-ref-30)
31. Крылов В.В. Информационные компьютерные преступления. Квалификация. Методика расследования. Основные нормативные акты. Учеб. И практич. Пособие.-М.:Изд. Группа «Инфра-М-Норма»., 1997. – 23 с. [↑](#footnote-ref-31)
32. Судебная практика по компьютерным преступлениям (краткий обзор). Протасов П.Н. – http://law.bugtrag.ru [↑](#footnote-ref-32)
33. Судебная практика по компьютерным преступлениям (краткий обзор). Протасов П.Н. – http://law.bugtrag.ru [↑](#footnote-ref-33)
34. Материалы собраны во время прохождения преддипломной практики в отделе по борьбе с компьютерными преступлениями при МВД РБ [↑](#footnote-ref-34)
35. Судебная практика по компьютерным преступлениям (краткий обзор). Протасов П.Н. – http://law.bugtrag.ru [↑](#footnote-ref-35)