Оглавление

# Введение

Глава 1. Правовое регулирование информации

1.1 Понятие информации

1.2 Информация как объект правовых отношений

1.3 Порядок правовой защиты информации

Глава 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации

2.1 Понятие и общая характеристика преступлений в сфере компьютерной информации

2.2 Уголовно-правовая характеристика неправомерного доступа к компьютерной информации

2.3 Уголовно-правовая характеристика признаки создания, использования и распространения вредоносных программ для ЭВМ

2.4 Уголовно-правовая характеристика признаки нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети

Заключение

Список источников

## **Введение**

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

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

Еще совсем недавно все, что связано с ЭВМ (компьютерами), было непривычным для широких слоев населения России. Одной из причин возникновения компьютерной преступности явилось информационно-технологическое перевооружение предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных. Другая причина - реальная возможность получения значительной экономической выгоды за противоправные деяния с использованием ЭВМ. Появилась заманчивая возможность как бы обменивать продукт своего неправомерного труда на иные материальные ценности. Страны, уже прошедшие период компьютерного переоснащения, накопили свой криминальный опыт. Например, бухгалтер одной из зарубежных пароходных компаний вычислил, что незначительное искажение отчетности не будет замечено ревизионной службой. Организовав 17 подставных фирм, он похитил значительные суммы без каких-либо видимых нарушений финансовой деятельности компании[[1]](#footnote-1).

В России тоже появились компьютерные преступления. Вспомним хотя бы нашумевшее дело Левина, проникшего в банковские счета зарубежных банков. Двадцатичетырехлетний математик с сообщниками проник в компьютерную систему Ситибанка, похищая денежные средства со счетов вкладчиков[[2]](#footnote-2). Не исключено, что в Российской Федерации компьютерная преступность имеет высокую степень латентности в связи с общей криминогенной обстановкой и отсутствием до недавнего времени соответствующих норм уголовного законодательства, а также специфичностью самой компьютерной сферы, требующей специальных познаний.

Ситуация, сложившаяся в обществе, потребовала принятия норм уголовного права, которые предусматривали бы ответственность за совершение преступлений в сфере компьютерной информации. Поэтому представляется актуальным исследование данной темы.

Целью данной дипломной работы является исследование правового регулирования компьютерной информации как объекта уголовно-правовой охраны и разработка предложений по совершенствованию действующего законодательства.

Поставленная цель ставит перед нами решения следующих задач:

1. Дать понятие информации.
2. Изучить информацию как объект правовых отношений.
3. Проанализировать порядок правовой защиты информации
4. Определить понятие и дать общую характеристику преступлений в сфере компьютерной информации.
5. Проанализировать неправомерный доступ к компьютерной информации.
6. Изучить признаки создания, использования и распространения вредоносных программ для ЭВМ.
7. Выявить и проанализровать признаки нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети.

Данная работа состоит из введения, двух глав, заключения и списка источников. Первая глава посвящена правовому регулированию информационных ресурсов и информации. Вторая глава посвящена уголовно-правовой характеристике преступлений в сфере компьютерной информации.

При написании данной дипломной работы были исследованы комплекс нормативно правовых актов, как Конституция Российской Федерации[[3]](#footnote-3), Уголовный кодекс Российской Федерации[[4]](#footnote-4), Закон РФ «О правовой охране программ для электронных вычислительных машин и баз данных»[[5]](#footnote-5), Закон РФ «Об авторском и смежных правах»[[6]](#footnote-6), Федеральный закон «О связи»[[7]](#footnote-7), Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"[[8]](#footnote-8) и т.д.

Также при исследовании данной работы были использованы труды таких отечественных авторов как Батурин Ю. М., Вехов В. Б., Вехов В., Зверева Е.А., Карпов В., Крылов В. В., Таганцев Н. С. и т.д.

Глава 1. Правовое регулирование информации

**1.1 Понятие информации**

Основным объектом изучения многих наук, и информатики в том числе, является информация. Современный уровень развития научного знания еще не позволяет, а возможно и никогда не позволит, дать точного и законченного определения этого основополагающего понятия. С развитием нашего представления о мире, в котором мы живем, с развитием науки расширяется и углубляется содержание понятия "информация".

Первоисточником данного термина является латинское слово informatio (изложение, истолкование, разъяснение), а вошло оно в русский язык, по мнению П.Я. Черных, в эпоху Петра I[[9]](#footnote-9).

На общелексическом, бытовом уровне понятие "информация" чаще всего толкуется как сведения, сообщения, передаваемые от человека человеку и осведомляющие о каких-то явлениях, событиях, процессах и т.д.

Однако это не исчерпывает всего содержания понятия "информация". Так, существует информация об окружающей действительности, которую человек получает через свои органы чувств, и она далеко не во всех случаях исходит от другого человека (температура окружающей среды, рельеф местности, время суток и т.п.).

Норберт Винер в своей работе "Кибернетика или управление и связь в животном и машине" определяет информацию как "обозначение содержания, черпаемого нами из внешнего мира в процессе приспособления к нему и приведения в соответствие с ним нашего мышления"[[10]](#footnote-10).

Мы видим, что информация определяется через категорию "содержание внешнего мира" и напрямую увязана с человеком, его мышлением и процессом приспособления человека к явлениям и событиям внешнего мира. Иными словами, Винер утверждает, что информация вне человеческого сознания не существует.

Многие современные представления о содержании понятия "информация" связаны с человеком и его способностью мыслить.

"Информация - это сообщение, осведомляющее о положении дел, о состоянии чего-нибудь"[[11]](#footnote-11).

Во всех случаях, когда идет речь о сведениях, следует понимать, что говорится об информации осмысленной, преобразованной человеческим сознанием. Согласно Словарю В.И. Даля, слово "сведения" происходит от "сведать", то есть узнать, получить сведения. Оно также является синонимом слов "знание", "известие", "уведомление"[[12]](#footnote-12).

Отождествление информации со сведениями или фактами, которые теоретически могут быть получены и усвоены, то есть преобразованы в знания, составляет суть антропоцентрического подхода к определению понятия "информация". Этот подход в настоящее время применяется наиболее широко и, в частности, в российском законодательстве.

Правовое регулирование информации осуществляется Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

При этом этот Закон не затрагивает отношений, регулируемых Законом Российской Федерации, "Об авторском праве и смежных правах" (пункт 2 статьи 1)[[13]](#footnote-13).

Согласно ст. 2 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" информация - сведения (сообщения, данные) независимо от формы их представления[[14]](#footnote-14).

За истекшие полвека появилось множество работ, в которых с позиций разных наук, различных научных школ и даже различных идеологических установок исследуются всевозможные подходы к определению этого понятия.

Так, под информацией понимается передача разнообразия, оригинальность, новизна, вероятность выбора, отраженное разнообразие, это мера сложности структур[[15]](#footnote-15).

Действительно, чем сложнее объект или процесс, тем больше информации в нем содержится и тем больше информации необходимо для его описания.

В.М. Глушков: "Информация в самом общем ее понимании представляет собой меру неоднородности распределения материи и энергии в пространстве и во времени, меру изменений, которыми сопровождаются все протекающие в мире процессы"[[16]](#footnote-16).

Энциклопедический словарь под редакцией А.М. Прохорова дает такое определение: "Информация (от латинского informatio - разъяснение, изложение) с середины ХХ века общенаучное понятие, включающее обмен сведениями между людьми, человеком и автоматом, автоматом и автоматом, обмен сигналами в животном и растительном мире, передачу признаков от клетки к клетке, от организма к организму; одно из основных понятий кибернетики".

Информация - это "определенная порция порядка"[[17]](#footnote-17).

Информация - это мера выбора самоорганизующейся системы[[18]](#footnote-18).

Информация, по мнению И.И. Юзвишина, - это "генерализационно-фундаментальная субстанция единого кодово-сотового пространства Вселенной, включающего воздух, воду, землю, солнечные и другие светоносные лучи, поля, их следы и весь спектр космических излучений, материализованных и дематериализованных сред, и выражающаяся через массу, скорость, энергию и другие формы, проявляющиеся в процессе материализации и дематериализации"[[19]](#footnote-19).

Обобщая результаты научных исследований информации[[20]](#footnote-20), можно выделить следующие сущностные характеристики информации, имеющие универсальный характер и проявляющиеся в любых формах ее существования и функционирования:

системный характер информации, проявляющийся в том, что информация выступает средством системной организации материи, а кроме того, и сама предполагает системную организацию;

субстанциональная несамостоятельность информации, проявляющаяся в невозможности для нее существовать и функционировать без материального носителя;

преемственность информации, связанная с ее субстанциональной несамостоятельностью и проявляющаяся в том, что всем изменениям информации сопутствуют изменения в материальных системах, носящие поступательный характер, что обеспечивает преемственность состояний как на физическом, так и на информационном уровне;

неисчерпаемость информации, проявляющаяся в том, что информация при передаче информации от одного носителя к другому может остаться на первом носителе, иными словами, ее количество не уменьшается в результате использования. Вследствие этого информация может иметь неограниченное число пользователей и при этом оставаться неизменной;

трансформируемость информации, т.е. возможность передавать одно и то же содержание в разной форме;

универсальность информации, проявляющаяся в том, что ее содержание может быть связано с любыми явлениями и процессами физической, биологической, социальной реальности;

релевантность информации, понимаемая как комплексное качество, характеризующее степень соответствия информации потребностям системы.

Информационные ресурсы являются объектами отношений физических, юридических лиц, государства, составляют информационные ресурсы России и защищаются законом наряду с другими ресурсами.

Правовой режим информационных ресурсов определяется нормами, устанавливающими[[21]](#footnote-21):

порядок документирования информации;

право собственности на отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах;

категорию информации по уровню доступа к ней;

порядок правовой защиты информации.

Таким образом, информация - универсальная субстанция, пронизывающая все сферы человеческой деятельности, служащая проводником знаний и сведений, инструментом общения, взаимопонимания и сотрудничества, утверждения стереотипов мышления и поведения.

1.2 Информация как объект правовых отношений

В последнее время информация приобретает два важных практических значения. С одной стороны, она рассматривается как экономический ресурс, значение которого постоянно возрастает. Использование информационных ресурсов, грамотная организация информационных процессов могут существенно увеличить рентабельность многих процессов в индустриальном производстве, способствовать в решении социальных проблем.

Необходимо выделить те свойства информации, которые определяют специфику правового регулирования информационных правоотношений.

Среди основных признаков информации, принципиальных для правового регулирования отношений по поводу информации, ученые различают следующие[[22]](#footnote-22):

1. Как уже отмечалось, любая информация обладает свойством идеальности. Право начинает опосредовать информацию лишь тогда, когда она может быть однозначно зафиксирована на материальном носителе. Юридическое свойство, вытекающее из этой особенности, заключается в двуединстве информации и материального носителя, на котором эта информация закрепляется. Необходимо сразу отметить: несмотря на то, что носитель информации является вещью, информация в правовом смысле не может рассматриваться как вещь. Это связано с тем, что когда мы передаем вещь, мы передаем при этом зачастую весь объем прав (владения, пользования и распоряжения). Но когда мы передаем зафиксированную на материальном носителе информацию, мы в правовом смысле передаем сам носитель и сумму каких-то прав по распоряжению содержащейся на нем информацией (например, право ее дальнейшего распространения). Саму же информацию мы лишь сообщаем и, таким образом, можем передать лишь право пользования и право распоряжения. Право владения (господства над вещью) может быть передано лишь на носитель, но не на информацию, которая на нем зафиксирована, ибо она осталась в памяти автора документа и останется в памяти всех, кто прочитает эти сведения.

2. Рассмотренные общие свойства идеальности и неисчерпаемости информации порождают такое юридическое свойство информации, как бесконечный неисчерпаемый ресурс.

Информация не подвержена (в отличие от большинства вещей) физическому старению и обладает такой особенностью, как возможность неограниченного тиражирования.

Это великое свойство информации предопределяет прогресс человечества, ибо благодаря ему осуществляются постепенное наращивание знаний и передача их от поколения к поколению. Однако оно дает и побочный эффект: возможность произвольного распространения сведений, одновременного нахождения их в полном объеме в нескольких местах и одновременного использования любым количеством субъектов (в том числе и конфликтующими сторонами). Свойство информации как бесконечного ресурса предопределяет конструирование в праве систем ограничения на доступ и распространение информации, именуемые институтами тайн. С ним также связано большое количество проблем установления авторства.

3. Следующим факультативным свойством информации, основанным на идеальности, является ее самостоятельность как объекта, независимость от среды, в которой она находится, от носителя, на котором сведения зафиксированы. Ценность сведений также никоим образом не может быть поставлена в зависимость от стоимости их носителя.

4. Для правового регулирования отношений, связанных с информацией, представляет определенный интерес такое ее свойство, как нелинейность - отсутствие зависимости между объемом информации и процессами, которые начинают протекать благодаря ее воздействию. Иными словами, количество информации и ее ценность не тождественны.

5. Следующей качественной характеристикой информации, имеющей принципиальное значение для включения ее в качестве объекта в какие-либо правовые отношения, является ее субъективная ценность, то есть значимость для конкретного субъекта. Причем для различных субъектов информация будет иметь различную ценность.

В праве ценность информации выражается прежде всего в стоимостных характеристиках тех действий, которые следуют за получением информации. В качестве примера здесь можно привести, скажем, факт разглашения сведений, составляющих государственную тайну. В данном случае величина уголовно-правовой санкции ставится в зависимость от материального эквивалента ущерба, нанесенного противоправным распространением указанных сведений.

6. При правовом регулировании важную роль играет увязывание информации с целью, для которой она была получена. Например, факт противоправного доступа к сведениям, составляющим коммерческую тайну, из праздного любопытства может иметь одни правовые последствия, а то же действие с целью их последующей продажи конкурентам - существенно иные последствия.

Таким образом, информация обладает рядом в достаточной мере уникальных свойств, выделяющих ее среди других объектов права. Этим также обусловлена и сложность в обеспечении эффективного правового регулирования тех отношений, в которых она фигурирует.

Согласно ст. 5 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Статья 128 ГК РФ относит информацию к объектам гражданских прав наряду с вещами (включая деньги и ценные бумаги), иным имуществом, в том числе имущественными правами; работами и услугами; результатами интеллектуальной деятельности, в том числе исключительными правами на них (интеллектуальной собственностью); нематериальными благами[[23]](#footnote-23).

Законодатель, как видно из перечня ст. 128 ГК РФ, рассматривает информацию в качестве особого объекта гражданских прав, отличного от имущества, работ и услуг, результатов интеллектуальной деятельности и нематериальных благ.

Этот факт не всегда получает адекватное отражение в специальной литературе и правотворчестве. Точка зрения о том, что информация может в определенном отношении рассматриваться как объект права собственности, высказывается с большей или меньшей категоричностью рядом специалистов[[24]](#footnote-24). Как правило, она вытекает из отрицания необходимости строгого разграничения между такими понятиями, как информация, с одной стороны, и информационные ресурсы, с другой стороны.

Указанная точка зрения находит свое выражение и в правовых актах. Так, например, в п. 1 ст. 2 Закона г. Москвы от 24 октября 2001 г. N 52 "Об информационных ресурсах и информатизации города Москвы"информационные ресурсы г. Москвы определяются как "информация (независимо от способа ее представления, хранения или организации), содержащаяся в информационных системах и относимая в соответствии с настоящим Законом к собственности города Москвы"[[25]](#footnote-25). Тем самым информация, во-первых, отождествлена с информационными ресурсами (в связи с чем утрачивает смысл формулировка "независимо от способа ее представления, хранения или организации"), во-вторых, отнесена к объектам права собственности. Между тем, по смыслу ст. 209 ГК РФ, объектом собственности может быть только имущество, к каковому информация, в соответствии с перечнем видов объектов гражданских прав, данным в ст. 128 ГК РФ, не относится.

Согласно ст. 2 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" информация - сведения (сообщения, данные) независимо от формы их представления[[26]](#footnote-26). (абз. 2); информационные ресурсы - это "отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)" (абз. 7). На первый взгляд здесь информация не отождествляется с информационными ресурсами, которые определяются как документы в составе информационных систем. Однако, вводя в этой же статье Федерального закона понятие "документированная информация", связывающее два предыдущих понятия, законодатель отождествляет его с понятием "документ": "документированная информация (документ) - зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать" (абз. 4), - тем самым фактически становясь на позицию отнесения информации (по крайней мере, в той ее части, которая представлена в виде документов) к объектам имущественных прав. Следовательно, определяя собственника информационных ресурсов, информационных систем, технологий и средств их обеспечения как субъекта, в полном объеме реализующего полномочия владения, пользования, распоряжения указанными объектами (абз. 11), законодатель фактически признает за ним право собственности на информацию[[27]](#footnote-27).

Согласно ст. 6 Федерального закона от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации" обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законам[[28]](#footnote-28).

Физические и юридические лица являются собственниками тех документов, массивов документов, которые созданы за счет их средств, приобретены ими на законных основаниях, получены в порядке дарения или наследования.

Российская Федерация и субъекты Российской Федерации являются собственниками информационных ресурсов, создаваемых, приобретаемых, накапливаемых за счет средств федерального бюджета, бюджетов субъектов Российской Федерации, а также полученных путем иных установленных Законом способов.

Государство имеет право выкупа документированной информации у физических и юридических лиц в случае отнесения этой информации к государственной тайне.

Собственник информационных ресурсов, содержащих сведения, отнесенные к государственной тайне, вправе распоряжаться этой собственностью только с разрешения соответствующих органов государственной власти.

Субъекты, представляющие в обязательном порядке документированную информацию в органы государственной власти и организации, не утрачивают своих прав на эти документы и на использование информации, содержащейся в них. Документированная информация, представляемая в обязательном порядке в органы государственной власти и организации юридическими лицами независимо от их организационно - правовой формы и форм собственности, а также гражданами, формирует информационные ресурсы, находящиеся в совместном владении государства и субъектов, представляющих эту информацию[[29]](#footnote-29).

Информационные ресурсы, являющиеся собственностью организаций, включаются в состав их имущества в соответствии с гражданским законодательством Российской Федерации.

Информационные ресурсы, являющиеся собственностью государства, находятся в ведении органов государственной власти и организаций в соответствии с их компетенцией, подлежат учету и защите в составе государственного имущества.

Информационные ресурсы могут быть товаром, за исключением случаев, предусмотренных законодательством Российской Федерации.

Собственник информационных ресурсов пользуется всеми правами, предусмотренными законодательством Российской Федерации, в том числе он имеет право[[30]](#footnote-30):

назначать лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;

устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;

определять условия распоряжения документами при их копировании и распространении.

Право собственности на средства обработки информации не создает права собственности на информационные ресурсы, принадлежащие другим собственникам. Документы, обрабатываемые в порядке предоставления услуг или при совместном использовании этих средств обработки, принадлежат их владельцу. Принадлежность и режим производной продукции, создаваемой в этом случае, регулируются договором.

Таким образом, в современных условиях информация становится стратегическим ресурсом, от эффективного использования которого зависят перспективы развития экономики, формирование информационного гражданского общества, обеспечение безопасности государства и граждан[[31]](#footnote-31). С другой стороны, информация становится экономическим товаром, что стимулирует во всем мире рост нового сегмента национальной экономики - информационных услуг. Наконец, информация является мощным и эффективным оружием[[32]](#footnote-32). Все это привело к возникновению новых правоотношений, объектом которых является информация.

**1.3 Порядок правовой защиты информации**

Согласно ст. 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа,

3) реализацию права на доступ к информации.

Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Целями защиты являются[[33]](#footnote-33):

предотвращение утечки, хищения, утраты, искажения, подделки информации;

предотвращение угроз безопасности личности, общества, государства;

предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу.

Режим защиты информации устанавливается:

в отношении сведений, отнесенных к государственной тайне, - уполномоченными органами на основании Закона Российской Федерации "О государственной тайне";

в отношении конфиденциальной документированной информации - собственником информационных ресурсов или уполномоченным лицом на основании настоящего Федерального закона;

в отношении персональных данных - федеральным законом.

Органы государственной власти и организации, ответственные за формирование и использование информационных ресурсов, подлежащих защите, а также органы и организации, разрабатывающие и применяющие информационные системы и информационные технологии для формирования и использования информационных ресурсов с ограниченным доступом, руководствуются в своей деятельности законодательством Российской Федерации[[34]](#footnote-34).

Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно - технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством Российской Федерации.

Организации, обрабатывающие информацию с ограниченным доступом, которая является собственностью государства, создают специальные службы, обеспечивающие защиту информации.

Собственник информационных ресурсов или уполномоченные им лица имеют право осуществлять контроль за выполнением требований по защите информации и запрещать или приостанавливать обработку информации в случае невыполнения этих требований.

Собственник или владелец документированной информации вправе обращаться в органы государственной власти для оценки правильности выполнения норм и требований по защите его информации в информационных системах. Соответствующие органы определяет Правительство Российской Федерации. Эти органы соблюдают условия конфиденциальности самой информации и результатов проверки.

Собственник документов, массива документов, информационных систем или уполномоченные им лица в соответствии с настоящим Федеральным законом устанавливают порядок предоставления пользователю информации с указанием места, времени, ответственных должностных лиц, а также необходимых процедур и обеспечивают условия доступа пользователей к информации.

Владелец документов, массива документов, информационных систем обеспечивает уровень защиты информации в соответствии с законодательством Российской Федерации.

Так, согласно п. 4 ст. 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации.

Риск, связанный с использованием несертифицированных информационных систем и средств их обеспечения, лежит на собственнике (владельце) этих систем и средств.

Риск, связанный с использованием информации, полученной из несертифицированной системы, лежит на потребителе информации.

Собственник документов, массива документов, информационных систем может обращаться в организации, осуществляющие сертификацию средств защиты информационных систем и информационных ресурсов, для проведения анализа достаточности мер защиты его ресурсов и систем и получения консультаций.

Владелец документов, массива документов, информационных систем обязан оповещать собственника информационных ресурсов и (или) информационных систем о всех фактах нарушения режима защиты информации[[35]](#footnote-35).

Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причиненного ущерба[[36]](#footnote-36).

Защита прав субъектов в указанной сфере осуществляется судом, арбитражным судом, третейским судом с учетом специфики правонарушений и нанесенного ущерба.

Нарушение требований Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

Ответственность за нарушения международных норм и правил в области формирования и использования информационных ресурсов, создания и использования информационных систем, технологий и средств их обеспечения возлагается на органы государственной власти, организации и граждан в соответствии с договорами, заключенными ими с зарубежными фирмами и другими партнерами с учетом международных договоров, ратифицированных Российской Федерацией.

Отказ в доступе к открытой информации или предоставление пользователям заведомо недостоверной информации могут быть обжалованы в судебном порядке.

Неисполнение или ненадлежащее исполнение обязательств по договору поставки, купли - продажи, по другим формам обмена информационными ресурсами между организациями рассматриваются арбитражным судом.

Во всех случаях лица, которым отказано в доступе к информации, и лица, получившие недостоверную информацию, имеют право на возмещение понесенного ими ущерба.

Суд рассматривает споры о необоснованном отнесении информации к категории информации с ограниченным доступом, иски о возмещении ущерба в случаях необоснованного отказа в предоставлении информации пользователям или в результате других нарушений прав пользователей.

Руководители, другие служащие органов государственной власти, организаций, виновные в незаконном ограничении доступа к информации и нарушении режима защиты информации, несут ответственность в соответствии с уголовным, гражданским законодательством и законодательством об административных правонарушениях.

В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

Таким образом, информация - сведения (сообщения, данные) независимо от формы их представления. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения. Информация относится к объектам гражданских прав наряду с вещами (включая деньги и ценные бумаги), иным имуществом, в том числе имущественными правами; работами и услугами; результатами интеллектуальной деятельности, в том числе исключительными правами на них (интеллектуальной собственностью); нематериальными благами[[37]](#footnote-37). Информация является объектом правовой защиты, и порядок его защиты урегулирован законами. Нарушение требований порядка защиты информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

**Глава 2. Уголовно-правовая характеристика преступлений в сфере компьютерной информации**

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

Теория и практика не выработали единого определения компьютерных преступлений. Объясняется это, в первую очередь, различием отечественного и зарубежного законодательства о преступлениях с использованием компьютера. В соответствии с действующим уголовным законодательством Российской Федерации под компьютерными преступлениями понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства. В отечественной литературе высказывалось и более широкое понятие компьютерных преступлений. Так, на заседании постоянно действующего межведомственного семинара "Криминалистика и компьютерная преступность" в 1993 г. компьютерные преступления определялись как "предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства"[[38]](#footnote-38). Такого понятия в основном придерживаются зарубежное законодательство и практика.

Наиболее распространенными преступлениями с использованием компьютерной техники являются: компьютерное «пиратство», компьютерное мошенничество, распространение вредоносных (вирусных) программ и компьютерный саботаж. К компьютерному пиратству относят прежде всего деятельность "хакеров" - неправомерный доступ к компьютерной информации с помощью подбора паролей, кодов, шифров, взломов электронных замков и т.п. Когда результатом подобной деятельности являются модификация информации и утечка денежных средств - она превращается в компьютерное мошенничество. Второй вид компьютерного «пиратства» - незаконное копирование, тиражирование и сбыт компьютерных программ. До 95% программного продукта, реализуемого в России, является «пиратским». В этой статистике Россию опережает только Китай, где незаконный продукт составляет 98%. Подобная деятельность нарушает авторские права создателей и разработчиков программ, причиняет материальный ущерб им и законным владельцам компьютерных программ. К тому же страдают пользователи программного продукта, так как качество копий уступает качеству оригинала[[39]](#footnote-39).

Среди основных мотивов компьютерных преступлений выделяют обычно два: корыстный и желание продемонстрировать собственный профессионализм - так называемый "интеллектуальный вызов". Комплекс причин и условий компьютерной преступности составляют, по мнению большинства авторов, следующие обстоятельства: высвобождение и сложности трудоустройства высокоинтеллектуальной и профессиональной части населения, связанной с наукой, тонкими технологиями, обороной и т.п.; безработица интеллектуальной элиты общества; возможность быстрого обогащения путем компьютерных хищений с незначительной вероятностью разоблачения ввиду высокой латентности компьютерных преступлений; недостаточная защищенность автоматизированных систем обработки данных; отставание технической оснащенности, профессионализма сотрудников правоохранительных органов от действий профессиональных компьютерных преступников; отсутствие обобщенной следственной и судебной практики расследования компьютерных преступлений; лояльное отношение общества к такого рода преступлениям ввиду использования лицами, их совершающими, интеллектуального способа обогащения и т.п. Начиная с 70-х годов, когда появились первые отечественные публикации о необходимости противостояния компьютерной преступности, их авторы указывали еще и на такое условие, как отсутствие законодательной базы подобной борьбы. В настоящее время подобное законодательство существует, но оно не вполне совершенно.

Большинство компьютерных преступлений - это проявления профессиональной и организованной преступности, нередко носящей групповой транснациональный характер. Причем часто в состав группы входит непосредственный работник кредитной организации или иной компании, которая впоследствии оказывается пострадавшей (по некоторым оценкам, при хищениях с использованием компьютерных средств до 80% таких деяний совершались "изнутри").

Транснациональный характер компьютерной преступности, быстрые темпы ее распространения обусловливают неизбежность объединения сил и средств многих государств по противостоянию этому явлению. "В настоящее время создается острая необходимость разработки международно-правовой базы предотвращения инцидентов, связанных с обменом информацией, борьбы против "информационного терроризма", разработки комплекса мер международного характера, предотвращающих деструктивное использование средств воздействия на национальные и глобальные информационные ресурсы"[[40]](#footnote-40).

28 января 1981 г. была принята Конвенция Совета Европы о защите личности в связи с автоматической обработкой персональных данных. В ст. 7 этой конвенции подписавшие ее государства обязались принимать надлежащие меры для охраны персональных данных, накопленных в автоматических базах данных, от случайного или несанкционированного разрушения или случайной утраты, а равно от несанкционированного доступа, изменения или распространения. Определенные меры в этом направлении предпринимаются и государствами-участниками СНГ[[41]](#footnote-41).

Так, 18 октября 1996 г. совет глав правительств Содружества независимых государств принял Концепцию формирования информационного пространства СНГ. В ст. 7 Концепции, в частности, говорится о проблеме обеспечения каждым государством собственной информационной безопасности и защиты информационного суверенитета. Кроме того, Россия участвует в Соглашении между правительствами государств-участников Черноморского экономического сотрудничества о взаимодействии в борьбе с преступностью. Это соглашение подписали Албания, Армения, Азербайджан, Болгария, Грузия, Греция, Молдова, Россия, Румыния, Турция и Украина. Стороны договорились о сотрудничестве в борьбе в первую очередь с некоторыми видами наиболее опасных преступлений, среди которых упоминаются преступления в сфере высоких технологий, включая компьютерные преступления.

На федеральном уровне для развития законодательной базы большое значение имеет утвержденная в сентябре 2000 г. Доктрина информационной безопасности Российской Федерации. В этой доктрине определены главные составляющие информационной безопасности, основные направления противодействия угрозам информационной безопасности в России, а также комплекс практических мероприятий по ее обеспечению.

Родовым объектом компьютерных преступлений является общественная безопасность. В качестве дополнительных объектов в ряде случаев могут выступать права и интересы граждан в сфере обеспечения личной, семейной, врачебной и т.п. тайны, интересы собственности, защищенность государственной, банковской тайны и т.п.

Видовым объектом преступлений, предусмотренных в гл. 28 УК, является совокупность общественных отношений, обеспечивающих состояние защищенности процессов создания, сбора, хранения, передачи и использования компьютерной информации, в которых правомерно участвуют собственники, владельцы и пользователи информации (информационная безопасность). В наименовании гл. 28 законодатель использует термин "информация", что дало основание некоторым авторам считать именно информацию (или компьютерную информацию) объектом данных преступлений. Н.В. Зумакулова[[42]](#footnote-42) и Прохоров считают, относительно объекта преступного посягательства двух мнений быть не может - им, естественно, является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества". Однако нам представляется, что компьютерную информацию следует рассматривать в качестве предмета данных составов, а объектом - информационную безопасность. Кстати, Модельный Уголовный кодекс стран СНГ, принятый позже российского, компьютерные преступления объединил именно в главе о преступлениях в сфере информационной безопасности (разд. ХII, гл. 30)[[43]](#footnote-43).

Информационная безопасность представляет собой состояние защищенности информационной сферы государства, общества, личности, обеспечиваемое комплексом мер по снижению до заданного уровня, предотвращению или исключению негативных последствий от воздействия (или отсутствия такового) на элементы информационной сферы[[44]](#footnote-44). Легальное определение информационной безопасности содержится в Федеральном законе от 4 июля 1996 г. N 85-ФЗ "Об участии в международном информационном обмене"[[45]](#footnote-45). Статья 2 этого закона гласит, что под информационной безопасностью понимается "состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства".

В доктрине информационной безопасности Российской Федерации, утвержденной Президентом РФ 9 сентября 2000 г., это понятие определено уже как состояние защищенности национальных интересов Российской Федерации, определяющихся совокупностью сбалансированных интересов личности, общества и государства[[46]](#footnote-46).

"Современное общество использует четыре основных ресурса: природные богатства, труд, капитал и информацию"[[47]](#footnote-47).

Информация признается одним из прав граждан. Всеобщая декларация прав человека и гражданина, принятая Генеральной Ассамблеей ООН 10 декабря 1948 г., в ст. 19 закрепила право каждого человека на свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Следуя приоритету норм международного права, Конституция РФ в ч. 4 ст. 29 подтвердила и гарантировала это право граждан, ограничив его сведениями, составляющими государственную тайну. Вместе с тем Конституция РФ содержит ряд иных ограничений, связанных с распространением информации. В частности, ст. 23 закрепляет право граждан не неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

Комплексное законодательство об охране информации в Российской Федерации появилось только в середине 90-х годов, до этого времени существовали лишь отдельные законы, содержавшие некоторые нормы об охраняемой информации, например, Закон СССР "Об адвокатуре" 1979 г.

В соответствии с Федеральным законом от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"[[48]](#footnote-48) информация определялась как "сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления" (ст. 2).

Вся информация, объединенная в информационные ресурсы (отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах), подразделяется на открытую (общедоступную) и информацию с ограниченным доступом. Последняя, в свою очередь, делится на информацию, отнесенную к государственной тайне, и конфиденциальную (ст. 10 Закона). Именно информация с ограниченным доступом (а отнесенной к таковой она может быть только на основании закона) является предметом компьютерных преступлений.

Государственная, служебная, коммерческая тайна, а также многие иные виды информации нуждаются в обязательной государственной правовой охране. В некоторых случаях важность тайны информации настолько велика, что ее охрану государство осуществляет мерами уголовного законодательства. Вместе с тем правовая охрана информации не может ущемлять права граждан. Так, в соответствии с ч. 3 ст. 10 Федерального закона "Об информации, информатизации и защите информации" не могут относиться к информации с ограниченным доступом, в частности, сведения о чрезвычайных ситуациях, экологическая, метеорологическая, демографическая, санитарно-эпидемиологическая и другая информация. Подобные положения закреплены и в отраслевых законодательных актах (см., например, Федеральный закон от 21 декабря 1994 г. N 68-ФЗ "О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера"[[49]](#footnote-49) и др.).

В некоторых составах гл. 28 УК РФ помимо информации предметом преступлений являются также компьютеры, их отдельные составляющие, компьютерные сети.

В главе 28 УК РФ предусмотрены следующие виды преступлений в сфере компьютерной информации: неправомерный доступ к компьютерной информации (272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети ( 274 УК РФ).

Большей частью преступления в сфере компьютерной информации могут совершаться только путем действия - неправомерный доступ к компьютерной информации или создание либо использование вредоносных программ для ЭВМ. Однако нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети возможно и путем бездействия - в виде невыполнения обязательных предписаний таких правил.

Неправомерный доступ к компьютерной информации и нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети сформулированы как преступления с материальным составом, а создание либо использование вредоносных программ для ЭВМ - с формальным. В качестве последствий в ст. 272 и 274 УК указываются: уничтожение, модификация, блокирование либо копирование информации, нарушение работы ЭВМ или системы ЭВМ, причинение существенного вреда и т.п.

В зарубежных странах, например, в статье 1030 (мошенничество по отношению к компьютерам) 47-й главы 18-го Свода законов США предусматрены следующие виды компьютерных преступлений:

сбор информации об обороне, международных отношениях или закрытой информации по вопросам атомной энергии при намерении или возможности использования этой информации для причинения ущерба США или в интересах другого государства;

получение информации из финансовых записей финансового эмитента, учреждения или информации о потребителе в файле управления учета потребителей;

воздействие на компьютер, находящийся в исключительном использовании правительственного ведомства США, или нарушение функционирования компьютера, используемого правительством;

совершение мошенничества путем доступа к компьютерам федерального значения и получение каких-либо ценностей, если мошенничество и все, что получено, включает использование компьютера;

беспрепятственное использование компьютера, применяемого для торговли между штатами с сознательной передачей программы, информации, кода или команды компьютерной системы.

Наказание за данные составы включает штраф, лишение свободы (за 2, 3 и 4 составы - до одного года, в случае повторного совершения - до десяти лет)[[50]](#footnote-50).

В континентальной системе права содержится достаточно богатый арсенал законодательных средств борьбы с компьютерными преступлениями, чем в России.

Уголовный кодекс Франции предусматривает ответственность за посягательства на права человека, связанные с использованием картотек и обработкой данных на ЭВМ, - различные манипуляции с информационными системами, содержащими персональные данные граждан (ст. 226-16-226-22); за незаконный доступ к системе автоматизированной обработки данных, воспрепятствование ее работе, ввод обманным способом данных, изменение информации и т.п. (ст. 323-1-323-3); за сбор и передачу информации, являющейся государственной тайной, находящейся в ЭВМ, для передачи иностранному государству (ст. 411-7-411-11).

Уголовный кодекс Испании устанавливает ответственность за получение и использование сведений, составляющих личную или семейную тайну, находящихся в информационных, электронных или телевизионных картотеках (ч. 2 ст. 197); предусматривает состав распространения полученных таким образом сведений (ч. 3 этой статьи); квалифицированный состав наказания за перечисленные деяния, совершенные лицом, управляющим или ответственным за подобные системы (ч. 4); охраняет объекты авторского права, в том числе программы для ЭВМ (ст. 270); регламентирует завладение и распространение коммерческой информации с использованием средств ЭВТ (ст. 278); говорит о квалификации по совокупности в случае, если одновременно было произведено завладение или разрушение информационных устройств (ч. 3 этой статьи); устанавливает ответственность за изготовление или владение инструментами, материалами, орудиями, веществами, машинами, компьютерными программами или аппаратами, специально предназначенными для совершения преступлений, предусмотренных в предыдущих статьях (ст. 400 УК Испании).

Для зарубежного законодательства очевидна одна тенденция: составы собственно компьютерных преступлений (действия против только охраняемой компьютерной информации) либо просто отсутствуют, либо существуют наряду с традиционными составами (мошенничество, выдача государственной тайны, собирание и распространение персональных данных). Последние либо предусматривают самостоятельный состав, который выступает как специальный по отношению к общему (тому же мошенничеству), либо находятся в той же статье в качестве квалифицированного состава.

Вернемся к исследованию российского законодательства о компьютерных преступлениях.

При определении состава компьютерных преступлений большое значение имеет время совершения преступления. Временем совершения компьютерного преступления (временем совершения общественно опасного деяния независимо от времени наступления последствий - ч. 2 ст. 9 УК) является момент нажатия клавиши клавиатуры компьютера или кнопки "мыши", отсылающей последнюю компьютерную команду, независимо от того, в какое время наступили опасные последствия. Время, отделяющее последствия от деяния, может быть минимальным и составлять несколько секунд, необходимых для прохождения информации по каналам и выполнения компьютером команды. Однако в некоторых случаях этот промежуток времени может быть весьма продолжительным. В основном это относится к ст. 273 и 274 УК. Некоторые вредоносные программы могут начать свое разрушительное действие не сразу, а по истечении длительного времени. Вирус может, выражаясь терминологией программистов, "спать" в компьютере и начать работу после совершения пользователем определенных действий, например, после обращения к тем или иным программам, использования определенных терминов или просто по прохождении некоторого времени.

Значительно сложнее обстоит дело с определением места совершения преступления. Поскольку большое количество компьютерных преступлений совершается в компьютерных сетях, объединяющих несколько регионов или стран, лидирующее место среди которых занимает всемирная компьютерная сеть Интернет, постольку место совершения деяния и место наступления последствий могут отделять многие километры, таможенные и государственные границы. Так, недавно один из московских межмуниципальных судов рассмотрел уголовное дело по факту хищения средств с использованием компьютерной сети Интернет. Гражданин России Г., используя домашний компьютер, в одном из сайтов Интернета обнаружил программу, производящую безналичные расчеты с кредитных карт. Г. скопировал программу на свой компьютер. После этого Г., входя в виртуальный магазин, реальный аналог которого располагался в Канаде, производил заказ и предварительную оплату товаров с чужих кредитных карточек, используя вышеупомянутую программу. После этой трансакции Г. незамедлительно отказывался от приобретения товара, однако для возврата денег указывал уже иные номера кредитных карт - собственных или своих сообщников. При этом последние были как гражданами России, так и Литвы. Деньги либо немедленно обналичивались через банкоматы, либо с помощью кредитных карт производилась покупка товаров в тех магазинах Москвы и Вильнюса, где расчеты возможны также с помощью кредитных карт. На первый взгляд, в данном деянии затронуты три страны. Однако на самом деле их значительно больше, так как пострадавшие лица, с банковских карточек которых незаконно списывались денежные средства якобы в оплату товаров, являлись гражданами различных стран.

Уголовный кодекс РФ не содержит нормы, определяющей место совершения преступления, поэтому им может быть место как совершения деяния, так и наступления последствий, либо то место, в котором деяние окончено либо пресечено. Уголовные кодексы некоторых стран содержат норму о месте совершения преступления. Так, по Уголовному кодексу Литвы "местом совершения преступления является место, в котором лицо действовало либо могло и обязано было действовать, либо место, в котором возникли предусмотренные уголовным законом последствия. Местом совершения преступления соучастников является место, в котором было совершено это преступление, а если соучастник действовал в другом месте - место его действия" (п. 2 ст. 4 УК ЛР). Что признавать местом совершения преступления, в каждом конкретном случае решают судебные органы. Аналогичное определение места совершения преступления содержится в Уголовном кодексе ФРГ (п. 1 и 2 § 9 УК ФРГ).

Если применить по аналогии норму о времени совершения преступления, то местом его совершения надлежит считать место отдачи последней компьютерной команды, однако принцип законности российского законодательства (ч. 2 ст. 3 УК) запрещает применение уголовного закона по аналогии. Следует также учитывать, что преступления с материальными составами считаются оконченными с момента наступления таких последствий. Общественную опасность преступления определяет не само деяние, а тот вред, который оно причинило или могло причинить. Поэтому место наступления последствий может быть определяющим. Такой подход согласуется со ст. 8 УК, где говорится о составе преступления как о единственном основании уголовной ответственности.

Транснациональный характер компьютерных преступлений обусловливает повышение роли международного сообщества при принятии решения по этому вопросу. Определенные шаги в данном направлении уже сделаны. Так, в п. 18 Венской декларации 2000 г. говорится о необходимости разработки программных рекомендаций в отношении преступлений, связанных с использованием компьютеров, и предлагается Комиссии по предупреждению преступности и уголовному правосудию приступить к работе в этом направлении[[51]](#footnote-51). Подобные решения принимались и на региональных уровнях: европейским сообществом, государствами-участниками Черноморского экономического сотрудничества, государствами-участниками СНГ.

Проблема унификации международно-правового уголовного регулирования квалификации компьютерных преступлений чрезвычайно важна. Государство, на территории которого наступили общественно опасные последствия, чьи граждане или организации стали потерпевшими, справедливо может претендовать на то, чтобы под местом совершения преступления признавалось именно данное государство. Однако это может повлечь новые проблемы при решении вопроса о привлечении российского гражданина к уголовной ответственности. В соответствии с ч. 1 ст. 12 УК РФ такое деяние должно одновременно признаваться преступлением на территории другого государства. Если в отношении общеуголовных преступлений законодательство более или менее единообразно, то законодательство о компьютерных преступлениях и практика его применения весьма различаются[[52]](#footnote-52).

О важности определения места совершения преступления говорит следующий пример. С июня по сентябрь 1994 г. российским программистом Л. и его сообщниками, являющимися гражданами других государств, с использованием компьютера, расположенного в Санкт-Петербурге, через электронную компьютерную систему телекоммуникационной связи Интернет вводились ложные сведения в систему управления наличными фондами "City Bank of America", расположенного в Нью-Йорке. В результате такой деятельности было похищено более 10 млн. долларов США со счетов клиентов банка. В организованную преступную группу входили граждане США, Великобритании, Израиля, Швейцарии, ФРГ и России. Однако при привлечении Л. к уголовной ответственности в Лондоне судебная инстанция в августе 1995 г. отложила принятие решения по этому делу на неопределенный срок ввиду того, что подсудимый использовал компьютер, находящийся на территории Российской Федерации, а не на территории США, как того требовало законодательство Великобритании. В результате просьба правоохранительных органов США и России о выдаче Л. была отклонена[[53]](#footnote-53).

С субъективной стороны анализируемое преступление может совершаться с различными формами вины. В ст. 273 УК речь идет о создании и использовании программ, заведомо приводящих к негативным последствиям. Указание на "заведомость" исключает неосторожную форму вины. Напротив, указание на "неосторожность" по отношению к последствиям в ч. 2 ст. 274 УК обусловливает совершение этого преступления только с неосторожной формой вины. Остальные составы возможны с различной формой вины. Большинство авторов указывают только на умышленный характер таких преступлений. Однако их мнение основано на анализе ч. 2 ст. 24 УК в прежней редакции. После изменения редакции этой статьи в 1998 г. составы, в которых не указано только на неосторожность, возможны с любой формой вины. Конечно, криминализация данных составов по неосторожности, особенно ст. 274 УК - нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, значительно расширяет круг их субъектов. Однако этот состав материальный, в качестве последствия предусматривает причинение существенного вреда, так что опасность даже неосторожных действий весьма велика. Во всяком случае, содержание ст. 24 УК допускает две формы вины в данных составах.

Субъект анализируемого преступления по общему правилу - общий.

Например, при совершении кражи чужого имущества (ст. 158 УК РФ) непосредственным объектом могут являться отношения личной собственности, на которые посягает преступник, а роль предмета преступления могут играть автомашина, компьютер, личные вещи, которыми завладевает преступник. Как разъяснил Пленум Верховного Суда РФ в п. 1 постановления N 5 от 25 апреля 1995 г. "О некоторых вопросах применения судами законодательства об ответственности за преступления против собственности"[[54]](#footnote-54), предметом хищения и иных преступлений, ответственность за совершение которых предусмотрена нормами соответствующей главы УК РФ, является чужое, т.е. не находящееся в собственности или законном владении виновного, имущество. Следовательно, если по обстоятельствам дела компьютер является просто вещью, по поводу которой совершается преступление, то такое деяние не может быть отнесено к числу компьютерных преступлений. Таким образом, если компьютерная аппаратура представляет собой предмет преступления против собственности, ее хищение, уничтожение или повреждение надлежит квалифицировать по ст. 158-168 УК РФ.

Предмет преступления следует отличать от орудий и средств совершения преступления. Эти понятия используют, когда требуется указать, с помощью чего (приспособлений, приемов) совершается преступление. Один и тот же предмет материального мира в одном преступлении может играть роль предмета преступления (например, пистолет при его краже), а в другом являться орудием преступления (когда похищенный пистолет использован при вооруженном нападении). "Компьютер как техническое средство совершения преступления рассматривается в ряду с такими средствами, как оружие, транспортное средство, любое техническое приспособление. В этом смысле его использование имеет прикладное значение, например, для хищения, сокрытия налогов и т.д. Такого рода действия не рассматриваются в качестве самостоятельных преступлений, а квалифицируются по различным статьям УК"[[55]](#footnote-55).

Таким образом, в компьютерных преступлениях практически невозможно выделить единый объект преступного посягательства. Налицо также множественность предметов преступных посягательств с точки зрения их уголовно-правовой охраны. Представляется, что к рассматриваемой категории преступлений могут быть отнесены только противозаконные действия в сфере автоматизированной обработки информации. Иными словами, объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства.

В этом отношении применение соответствующих положений УК РФ 1996 г. является более сложным. Практика применения существующих составов весьма невелика, что позволило некоторым авторам утверждать, "что надежды, возлагаемые многими на существенное усиление борьбы с пиратством в связи с новым Уголовным кодексом, не оправдались"[[56]](#footnote-56).

Таким образом, под компьютерными преступлениями понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

**2.2 Неправомерный доступ к компьютерной информации**

Неправомерный доступ к компьютерной информации (ст. 272 УК). Данная статья предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

Объектом преступления является информационная безопасность.[[57]](#footnote-57).

Предмет преступления, предусмотренного ст. 272 УК, - охраняемая законом компьютерная информация. Однако невозможно представить себе покушение на информацию саму по себе. Если эта информация охраняется законом, то она является либо государственной, либо коммерческой, либо личной тайной и т.п.. Следовательно, речь может идти о государственных преступлениях либо преступлениях против конституционных прав и свобод человека и гражданина. Единственное исключение в этом плане составляет оценка действий, направленных на отношения, охраняющие коммерческую и, в ряде случаев, служебную тайну. В связи с этим возникает вопрос: если совершается покушение на охраняемую законом информацию, охватываемое иными статьями УК, достаточно ли будет квалификации по статьям гл. 28 Кодекса либо необходима квалификация по совокупности.

Основными действиями, предусмотренными ст. 272 УК, являются две разновидности компьютерного пиратства - незаконное копирование и распространение программного продукта для ЭВМ и хищение из разного рода финансовых институтов с помощью подбора паролей и "ключей" к чужим счетам. Относительно первой разновидности действий возникает конкуренция между ст. 272 и 146 УК. Программы для ЭВМ являются объектами авторских прав. Л.С.Симкин даже не упоминает о нормах гл. 28 УК. Автор последовательно[[58]](#footnote-58) проводит линию о признании нарушения только авторского права и соответствующей квалификации по ст. 146 УК (нарушение авторских и смежных прав), а в некоторых случаях и по совокупности со ст. 180 (незаконное использование товарного знака).

При компьютерном мошенничестве в юридической литературе проводится мысль о необходимости квалификации только по ст. 159 УК (мошенничество) либо, в зависимости от обстоятельств дела, по ст. 158. Приоритет отдается преступлениям против собственности, в которых компьютер (компьютерные сети) является лишь орудием, средством.. В вышеупомянутом деле Г. органы предварительного следствия и судебные органы квалифицировали деяние по ч. 3 ст. 159 - мошенничество, совершенное в крупном размере. О квалификации по совокупности вопроса не стояло. Оценивать содеянное только как преступление против собственности нет достаточных оснований, поскольку информация сама по себе не может служить предметом преступлений против собственности ввиду несоответствия обязательным признакам предмета. К тому же обман компьютера, машины невозможен.

Одним из проблемных вопросов квалификации преступлений со сложными составами является, в частности, вопрос о том, охватываются ли ими перечисленные простые составы либо требуется квалификация по совокупности. В литературе отмечалось, что "составляющие сложные составные деяния не могут выходить за пределы родового объекта посягательства и быть по категории и связанной с ней наказуемостью опаснее, нежели единое сложное преступление"[[59]](#footnote-59). Поэтому будет ли правомерным «пиратское» тиражирование компьютерных программ квалифицировать только по ст. 146 УК либо хищение денежных средств с использованием компьютерных сетей - только по ст. 159 или 158 УК даже при наличии в этих статьях такого квалифицирующего признака, как использование компьютерных средств (что, кстати, предусматривалось в проекте Уголовного кодекса РФ, а сегодня существует в Кодексах Республик Узбекистан и Кыргызстан, а также в Модельном Уголовном кодексе стран-участниц СНГ). Одни авторы считают, что в данных случаях компьютер является только средством, техническим инструментом, поэтому нельзя говорить о квалификации по совокупности; другие отстаивают иную точку зрения[[60]](#footnote-60). На наш взгляд, именно она представляется предпочтительной. При незаконном проникновении в компьютерную сеть и модификации или копировании охраняемой информации преступник не только посягает на отношения собственности или личности, но и нарушает информационную безопасность, которая является видовым объектом по отношению к родовому - общественной безопасности. Этот объект не охватывается составами преступлений против собственности, государства или личности. Ведь если лицо совершает какое-то деяние с использованием оружия, то в большинстве случаев речь пойдет о квалификации по совокупности этого преступления и незаконного ношения (хранения и т.п.) оружия, так как в данном случае страдает еще один объект - отношения общественной безопасности.

Таким образом, представляется, что при посягательстве на различные объекты (собственность, права граждан, государственная безопасность и т.п.), совершенном посредством компьютера или компьютерных сетей, при реальном выполнении виновным нескольких составов квалификация должна осуществляться по совокупности соответствующих статей, предусматривающих ответственность за преступления против собственности, прав граждан и т.п., и статей, предусмотренных гл. 28.

Точно так же необходимо поступать и в случаях с компьютерным «пиратством». При незаконном тиражировании и распространении компьютерных программ не только страдают права автора, но и затрагиваются отношения информационной безопасности. В ряде случаев, когда дело не имеет большого общественного значения, государство не в состоянии при отсутствии заявления автора компьютерной программы привлечь преступника к уголовной ответственности.

Компьютерная информация представляет собой сведения, содержащиеся на одном из носителей машинной информации (жестком диске типа Винчестер, внешних носителях - накопители на гибких магнитных дисках (дискетах), на кассетных магнитных лентах, на магнитооптических дисках и оптических дисках), которая может передаваться по каналам компьютерной связи и манипулирование этой информацией возможно только с помощью ЭВМ.

Уголовно-правовой охране, как следует из диспозиции ст. 272 УК, подлежит лишь охраняемая законом информация. Диспозиция этой статьи является бланкетной, поэтому для определения объема такого рода информации необходимо обратиться к иному законодательству. Так, вся охраняемая информация (следуя терминологии Федерального закона " Об информации, информационных технологиях и о защите информации", - информация с ограниченным доступом) подразделяется на информацию, отнесенную к государственной тайне, и конфиденциальную. Государственная тайна - это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации[[61]](#footnote-61).

Определить объем конфиденциальной информации несколько сложнее. Указом Президента РФ от 6 марта 1997 г. N 188 "Об утверждении перечня сведений конфиденциального характера" утвержден Перечень сведений конфиденциального характера[[62]](#footnote-62). Эти сведения подразделяются на несколько групп.

1. Сведения о фактах, событиях и обстоятельствах частной жизни граждан, позволяющие идентифицировать их личность (персональные данные). Защита персональных данных закреплена в ст. 24 Конституции РФ, и они не подлежат разглашению без согласия лица, о котором идет речь. Запрет на распространение информации такого рода закреплен и в других законодательных актах. В частности, Федеральный закон от 15 ноября 1997 г. N 143-ФЗ "Об актах гражданского состояния"[[63]](#footnote-63) запрещает работнику органа записи актов гражданского состояния разглашать сведения, ставшие ему известными в связи с государственной регистрацией акта гражданского состояния (ст. 12).

Этим же законом закреплено право граждан на охрану тайны усыновления. В ст. 47 содержится запрет сообщения работниками органов записи актов гражданского состояния каких-либо сведений об усыновлении.

Право граждан на сохранность в тайне персональных данных может быть ограничено лишь в необходимых случаях, например при проведении оперативно-розыскных мероприятий. Однако и в этом случае на органы (должностных лиц), осуществляющие подобные мероприятия, возлагается обязанность неразглашения сведений, ставших известными им при осуществлении оперативно-розыскных мероприятий[[64]](#footnote-64).

2. Сведения, составляющие тайну следствия и судопроизводства. Недопустимость разглашения данных предварительного следствия закреплена в ст. 139 УПК РСФСР. Такие сведения могут быть преданы гласности лишь с разрешения следователя или прокурора.

3. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом РФ и федеральными законами (служебная тайна). Гражданский кодекс определяет служебную тайну как информацию, имеющую действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и обладатель которой принимает меры к охране ее конфиденциальности (ст. 139). Перечень сведений, отнесенных к служебной тайне, определяется соответствующим органом или организацией и обязателен для неразглашения служащими этих организаций.

4. Сведения конфиденциального характера: сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами. К таким сведениям, в частности, относятся:

- врачебная тайна (информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении)[[65]](#footnote-65);

- нотариальная тайна (сведения или документы, которые стали известны нотариусу при исполнении служебных обязанностей, а также лицам, работающим в нотариальной конторе)[[66]](#footnote-66);

- адвокатская тайна (сведения, сообщенные адвокату доверителем в связи с оказанием юридической помощи)[[67]](#footnote-67);

- тайна исповеди[[68]](#footnote-68).

По нашему мнению, отнесение последних сведений к информации с ограниченным доступом не вполне бесспорно. С одной стороны, федеральные законы действительно указывают на правовую охрану подобных сведений. Однако в большинстве своем в них речь идет о "специальном субъекте", ответственность за разглашение на которого возлагается не только по правовым, но чаще моральным нормам. К этой категории можно отнести тех лиц, к которым граждане обращаются за духовной, врачебной или правовой помощью, - священников, врачей, адвокатов, нотариусов. Вполне обоснованно, что лица, распространившие конфиденциальную информацию, ставшую известной им при названных обстоятельствах, должны нести правовую ответственность, базирующуюся в первую очередь на ответственности моральной. Не случайно для некоторых категорий такого рода работников в качестве этапа вступления в должность предусмотрено принятие клятвы (ритуал присяги моральным принципам и правилам), содержащей положения о неразглашении тайны конфиденциальных сведений. Однако возможна постановка вопроса: можно ли говорить о подобной ответственности, если сведения были незаконно получены третьим лицом, которому они не доверялись гражданами в сложных обстоятельствах. Указ Президента РФ от 12 января 1998 г. N 61 "О перечне сведений, отнесенных к государственной тайне" положительно решает этот вопрос, не упоминая о субъекте разглашения. В данном случае законодатель встал на позицию строгой охраны прав граждан, которым безразлично, произошло ли разглашение сведений в результате неправомерных действий специального субъекта, скажем, врача, которому эта доверительная информация была сообщена в трудную минуту, или впоследствии похищена кем-либо из его компьютера, в котором он составлял картотеку больных. Нарушение тайны исповеди, адвокатской, врачебной, нотариальной, тайны усыновления и др. причиняет равный ущерб гражданам независимо от того, кто конкретно нарушил эту тайну;

- иные сведения. К ним относятся сведения об используемых при проведении негласных оперативно-розыскных мероприятий силах, средствах, источниках, методах, планах и результатах оперативно-розыскной деятельности, о лицах, внедренных в организованные преступные группы, о штатных негласных сотрудниках органов, осуществляющих ОРД, и о лицах, оказывающих им содействие на конфиденциальной основе и пр[[69]](#footnote-69).

5. Сведения, связанные с коммерческой деятельностью (коммерческая тайна). Определение коммерческой тайны совпадает с определением служебной тайны. Существуют, однако, некоторые ограничения по объему информации, составляющей коммерческую тайну. В частности, постановлением Правительства РФ от 5 декабря 1991 г. N 35 "О перечне сведений, которые не могут составлять коммерческую тайну"[[70]](#footnote-70), определен перечень сведений, которые не могут составлять коммерческую тайну. Представляется обоснованным отнесение к подобного рода сведениям и банковской тайны. Ее охрана предусмотрена ст. 857 ГК и ст. 26 Закона от 2 декабря 1990 г. N 395-1 "О банках и банковской деятельности" в ред. Федерального закона от 3 февраля 1996 г. N 17-ФЗ с последующими изменениями и дополнениями[[71]](#footnote-71). В последнем нормативном акте банковская тайна определяется как сведения об операциях, о счетах и вкладах своих клиентов и корреспондентов, а также иные сведения, устанавливаемые кредитной организацией.

6. Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о нем. Подобная тайна охраняет законные права изобретателя и установлена Патентным законом Российской Федерации от 23 сентября 1992 г. N 3517-1[[72]](#footnote-72).

К информации с ограниченным доступом относятся также тексты произведения, охраняемого законодательством об авторском праве, и тексты программ для ЭВМ, базы данных, до того момента, когда появится возможность свободного использования таких сведений.

Объективная сторона преступления - неправомерный доступ к компьютерной информации. Под неправомерным доступом подразумеваются такие способы получения либо просмотра информации, которые совершаются в обход установленного порядка обращения к охраняемой информации, а также вопреки воле собственника или законного владельца.

Способы незаконного ознакомления с компьютерной информацией можно классифицировать по различным основаниям. Однако в основном они сводятся к двум большим группам:

неправомерный доступ без использования компьютерных программ (традиционные способы);

неправомерное проникновение к компьютерной информации путем использования достижений науки и техники.

К первой группе относятся: а) похищение самих носителей информации (магнитных, оптических дисков), а также аппаратных средств, хранящих информацию. Таким образом в 1994 г. в Волгоградской области преступники, проникнув в операционный зал сберегательного банка, похитили два системных блока, в которых хранился банк данных на всех вкладчиков сбербанка; б) способ физической "маскировки" - "проход за спиной" или "за дураком". В подобных случаях лицо проникает на охраняемый объект (центр, предприятие, операционный зал) вслед за человеком, который имеет туда правомерный доступ. При этом преступник, как правило, несет в руках средство, относящееся к компьютерной технике (дисплей, процессор), и под видом работника, не вызывая особых подозрений, проникает на охраняемую территорию. Под физической "маскировкой" понимают также использование средств идентификации законного пользователя - чужих паролей, кодов, личного идентификационного номера, записей в журнале регистрации или чужого голоса в системе распознавания голосов. Однако для этой категории преступных действий характерно то, что коды, пароли и т.п. становятся известными преступнику без использования компьютерных каналов - они были похищены традиционным тайным способом, подсмотрены, подделаны и т.п.; в) физическая "уборка мусора" - исследование отработанных носителей компьютерной информации, физическим образом выброшенных пользователем. совершение преступных деяний таким способом возможно лишь на предприятиях, где система безопасности имеет существенные пробелы. По мере совершенствования охранных систем количество деяний, совершаемых таким образом, будет постоянно сокращаться.

Ко второй группе незаконного ознакомления с компьютерной информацией относится перехват информации: электромагнитный (использование электромагнитного излучения при работе компьютерных систем без непосредственного контакта с ними); в кабельных линиях; аудио- и видеоперехват.

Большинство способов незаконного доступа к компьютерной информации происходит с использованием программ. К незаконному доступу с использованием компьютера непосредственно (по его прямому назначению) можно отнести:

электронную "маскировку" - использование чужих паролей, кодов и т.п. Здесь есть много разновидностей, например: "компьютерный абордаж" (несанкционированный доступ к компьютерной системе с использованием линий телефонной связи и модема), неспешный выбор (нахождение слабых мест в системе защиты компьютерной сети), "брешь" (поиск заведомо слабых мест в системе защиты компьютерной сети), "люк", "черный вход" или "лазейка" (проникновение через обнаруженные слабые места защиты и внедрение собственных компьютерных команд);

электронную "уборку мусора" - исследование компьютерных файлов, которые стерты пользователем, но еще не исчезли полностью из компьютерной памяти;

несанкционированное подключение к каналам компьютерной связи и незаконный перехват компьютерной информации. В качестве одной из разновидностей последнего способа является перехват "за хвост" - когда преступник подключается к линии связи пользователя, дожидается окончания сеанса связи, а затем "переключает" сигнал на себя, получая в дальнейшем доступ к системе;

иные способы незаконного доступа к компьютерной информации[[73]](#footnote-73).

Состав преступления, предусмотренный ч. 1 ст. 272 УК, является материальным. Для признания его оконченным необходимо наступление одного из последствий, альтернативно перечисленных в статье: уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Под уничтожением информации признается не поддающаяся восстановлению потеря информации, в результате которой утрачивается возможность ее прочтения и использования. Блокирование информации - это невозможность доступа и использования компьютерной информации при реальном, физическом ее сохранении. Модификация информации означает полное либо частичное изменение ее первоначального содержания. Копирование представляет собой создание хотя бы одной копии независимо от характера ее физического носителя - бумажного, магнитного, лазерного или иного при сохранении оригинала информации. В теории факт ознакомления с информацией некоторыми авторами также признается копированием. Последнее утверждение представляется не бесспорным. Не является копированием и автоматическое создание архивной копии файла в той же компьютерной системе.

Под ЭВМ (электронно-вычислительной машиной) имеется в виду "комплекс электронных устройств, позволяющих производить предписанные программой и/или пользователем операции (последовательности действий по обработке информации и управлению устройствами) над символьной и образной информацией, в том числе осуществлять ее ввод - вывод, уничтожение, копирование, модификацию, передачу информации в сети ЭВМ и другие информационные процессы". Под "системой ЭВМ следует понимать комплексы, в которых хотя бы одна ЭВМ является элементом системы либо несколько ЭВМ составляют систему", а под сетями ЭВМ - "компьютеры, объединенные между собой линиями электросвязи"[[74]](#footnote-74).

Нарушением работы ЭВМ будет сбой в работе одной ЭВМ либо нескольких, объединенных в систему или сеть, существенно затрудняющий либо делающий невозможным выполнение компьютером тех задач, для решения которых он конструктивно предназначен.

С субъективной стороны преступление характеризуется как умышленной, так и неосторожной формами вины.

Субъект - общий, т.е. вменяемое лицо, достигшее 16-летнего возраста.

Квалифицированный вид неправомерного доступа к компьютерной информации (ч. 2 ст. 272 УК) представляет собой деяние, предусмотренное частью первой этой статьи, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Понятие "группа лиц по предварительному сговору и организованная группа" содержится в ст. 35 УК РФ. Следует отметить, что значительное число компьютерных преступлений относится к групповым, причем чаще всего речь идет о таких формах группового взаимодействия, как организованная группа или преступное сообщество. При этом не обязательно, чтобы все члены группы были профессиональными программистами. В группу может входить всего один такой профессионал, а остальные ее члены могут выполнять иные элементы объективной стороны.

Под использованием служебного положения понимается осуществление преступных действий лицом, которое в силу занимаемой должности либо выполняемых трудовых обязанностей может использовать ЭВМ, их систему либо сеть. При этом понятие "с использованием служебного положения" шире, нежели понятие "должностное положение", обусловленное понятием "должностное лицо", определение которого содержится в примечании к ст. 285 УК, так как использование служебного положения включает в себя должностные полномочия, должностной авторитет, иные возможности, предоставленные трудовым договором и административной практикой в той или иной организации.

Лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети, - это такие лица, которые в силу выполнения трудовых или иных обязанностей в принципе имеют право работать на данных компьютерах либо выполнять их обслуживание. Как правило, речь идет либо о законных пользователях (программисты, операторы ЭВМ, операционисты и др.), либо об обслуживающем персонале (наладчики, лица, осуществляющие сервисное обслуживание, электронщики и др.). Все названные категории лиц обладают определенными правомочиями по использованию данной компьютерной техники. Однако в данном случае они осуществляют действия с нарушением установленных правил либо установленного порядка. Как правило, эти лица не имеют доступа к конкретной информации, в отношении которой установлен определенный режим использования или ознакомления. Например, программист, отвечающий за одну часть программного обеспечения, скажем, за операции по конвертации иностранной валюты в коммерческом банке, внедряется в банк данных, содержащий сведения о клиентах банка. Возможны и такие ситуации, когда лицо вправе работать с некоторой информацией в не обусловленное для него время.

Субъект преступления может быть общим - при совершении преступления в составе группы лиц по предварительному сговору или организованной группе. При этом все лица должны быть исполнителями деяния, т.е. полностью либо частично выполнять объективную сторону последнего. В остальных случаях состав ч. 2 ст. 272 УК предусматривает специального субъекта - лицо, использующее свое служебное положение либо имеющее доступ к ЭВМ, системе ЭВМ или их сети.

Статья 272 УК РФ с успехом применяются отечественной судебной системой. Так, в конце лета 1997 года на российском рынке стали распространяться лазерные компакт-диски с базами данных: абонентов компаний сотовой связи; о недвижимости; о юридических лицах Санкт-Петербурга с указанием подробных сведений об учредителях, виде деятельности и уставном капитале и др. Было выяснено, что директор и заместитель директора "Орлов и К0", а также сотрудник "СПб таксофоны" в результате обобщения конфиденциальной информации, полученной из различных источников, создали и распространили базу данных "Весь Питер", в общей сложности реализовав дисков на сумму более 43 млн. рублей. Они приобрели информацию о номерах и кодах доступа к 1000 голосовым почтовым ящикам, которая продавалась различным гражданам[[75]](#footnote-75).

В апреле 1999 года Выборгский суд Санкт-Петербурга приговорил директора "Орлов и К0" к 1 году и 3 месяцам лишения свободы в колонии общего режима, а заместителя директора "Орлов и К0" и сотрудника "СПб таксофоны" - к 1 году исправительных работ. И хотя их тут же амнистировали, прецедент был создан[[76]](#footnote-76).

Таким образом, неправомерный доступ к компьютерной информации является основанием уголовной ответственности. Объектом данного преступления является информационная безопасность, объективной стороной является неправомерный доступ к компьютерной информации, с субъективной стороны преступление характеризуется как умышленной, так и неосторожной формами вины, субъект - общий, т.е. вменяемое лицо, достигшее 16-летнего возраста.

**2.3 Признаки создания, использования и распространения вредоносных программ для ЭВМ**

Это преступление отнесено к наиболее общественно опасным деяниям из числа преступлений, посягающих на компьютерную информацию, что выражается в размере санкций и в конструировании ч. 1 ст. 273 УК в виде формального состава. Наибольший вред собственникам, владельцам и законным пользователям компьютерных средств и информационных ресурсов приносят именно вредоносные программы.

Закон РФ от 23 сентября 1992 г. N 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных"[[77]](#footnote-77) определяет программу для ЭВМ как "объективную форму представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определенных результатов", а также "подготовительные материалы, полученные в ходе ее разработки и порождаемые ею аудиовизуальные отображения" (ст. 1 закона). В соответствии с описанием диспозиции статьи под вредоносной понимается такая программа, которая заведомо приводит к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети. В подобных случаях нарушается нормальный порядок работы отдельных программ, что внешне, в первую очередь, выражается в невыполнении команд, задаваемых с помощью клавиатуры либо мыши, в выполнении иных команд, в невозможности вызова тех или иных программ или файлов и иных негативных последствий..

В ст. 273 УК речь идет об уголовной ответственности за создание и распространение так называемых компьютерных "вирусов". На самом деле предмет статьи несколько шире и включает в себя также иные вредоносные программы.

Программу-вирус называют так потому, что ее функционирование внешне схоже с существованием биологического вируса, который использует здоровые клетки, инфицируя их и заставляя воспроизводить вирус. Компьютерный вирус не существует сам по себе, он использует иные программы, которые модифицируются и, выполняя определенные функции, воспроизводят вирус[[78]](#footnote-78).

В современном мире существует несколько тысяч программ-вирусов, и их количество ежегодно возрастает. По некоторым данным, в мире ежедневно создается от трех до восьми новых вирусных программ[[79]](#footnote-79).

Начало 2000 г., в частности, ознаменовалось появлением вируса "I love you", который приходил в послании по электронной почте и срабатывал в случае открытия такого послания. Вирус дестабилизировал работу многих пользователей и компаний. Вообще, как велико количество вирусных программ, так и разнообразно их действие. Вирус "Микеланджело", например, вызывает аварийную остановку компьютера или потерю данных в результате ошибок программы. Среди известных вирусов можно назвать: "Рождественская елка", "Вирус Морриса", "666", "Иван Грозный", "Пинг Понг", "Янки Дуддль" и др[[80]](#footnote-80).

Помимо вирусов, по характеру своего действия выделяют следующие вредоносные программы:

"троянский конь", когда под известную программу вуалируется другая, которая, проникнув в информационно-вычислительные системы, внедряется в иные программы (иногда методом вставки операторов), начинающие работать неожиданно для законного пользователя по-новому;

"троянская матрешка" (вредоносные команды формируются опосредованно через другие команды), "салями" и другие разновидности "троянского коня", "салями" применяется к программам, используемым в бухгалтерии. С помощью этой программы осуществляются компьютерные хищения. Принцип ее работы заключается в изъятии малых средств с каждого большого числа при совершении определенных операций, например, зачислении денег на счет или конвертации из одного вида валюты в другой. Программа названа так ввиду сходства с процессом отрезания тонких ломтиков одноименной колбасы. Программа эта весьма удобна для преступников, так как хищение оказывается высоко латентным ввиду того, что пропажу мизерных сумм выявить весьма сложно. Вместе с тем, учитывая скорость работы компьютера и частоту совершаемых операций (например, в пределах крупного банка), суммы, похищенные таким образом, оказываются в результате достаточно велики;

"логическая бомба" - срабатывание определенных команд, неправомерно внесенных в какую-либо программу при определенных обстоятельствах, часто направленных на уничтожение данных. Иногда выделяют такой подвид, как "временная бомба", когда вредоносная программа или команда срабатывает по истечении определенного времени;

компьютерные "черви". По характеру эта программа схожа с компьютерными вирусами. Отличие состоит в том, что "червь" - это самостоятельная программа.

Объемы и характеристики вредоносных программ разнообразны. Объединяющим является их разрушительное воздействие на информационные ресурсы, а в некоторых случаях и на саму ЭВМ.

Выполнение объективной стороны данного преступления возможно только путем совершения активных действий. Создание, использование и распространение вредоносных программ для ЭВМ будет выполнено с момента создания такой программы, внесения изменений в существующие программы, использования либо распространения подобной программы. Наступление определенных последствий не предусмотрено объективной стороной состава. Однако такие программы должны содержать в себе потенциальную угрозу уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Для признания деяния оконченным достаточно совершения одного из действий, предусмотренных диспозицией статьи, даже если программа реально не причинила вреда информационным ресурсам либо аппаратным средствам. К таким действиям относятся:

создание программ для ЭВМ, т.е. разработка компьютерных программ, основанных на оригинальных, новых алгоритмах, изобретенных и реализованных разработчиком;

внесение изменений в существующие программы, т.е. различного рода переработка, модификация созданной ранее программы, в результате чего последняя становится вредоносной и может привести к негативным общественно опасным последствиям;

использование программы или базы данных, т.е. выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модифицированной форме (Закон РФ от 23 сентября 1992 г. N 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных");

распространение, т.е. 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;

использование либо распространение машинных носителей с такими программами. В данном пункте в основном речь идет о так называемых устройствах внешней памяти. Общественная опасность подобных действий заключается в том, что при работе с такими устройствами, особенно содержащими вирусные программы, практически неизбежен перенос вредоносных программ на ЭВМ либо в сеть ЭВМ (их "заражение").

Относительно характера субъективной стороны анализируемого преступления в специальной литературе высказываются различные мнения. Одни авторы считают, что данное преступление возможно только с прямым умыслом[[81]](#footnote-81), другие - только по неосторожности, третьи - с косвенным умыслом. При установлении прямого умысла преступления надлежит квалифицировать по иным статьям Уголовного кодекса в зависимости от поставленных целей и наступивших последствий.

В диспозиции ст. 273 УК не содержится указания на неосторожность, и, следовательно, в соответствии с ч. 2 ст. 24 УК действия могут совершаться как умышленно, так и по неосторожности. Однако включение в диспозицию признака "заведомости" для виновного вредных последствий исключает неосторожность в качестве формы вины в данном преступлении. Вместе с тем ограничивать субъективную сторону только прямым умыслом тоже, вероятно, не стоит. Возможны случаи, когда лицо не желает, но сознательно допускает наступление последствий или безразлично к ним относится. Это, в частности, может иметь место в случае использования машинного носителя с вредоносными программами. Дело в том, что в силу специфики работы электронно-вычислительной техники дальнейшее распространение такой программы вероятно, но не неизбежно. Поэтому субъективная сторона преступления может характеризоваться как прямым, так и косвенным умыслом.

Субъект общий - вменяемое лицо, достигшее 16-летнего возраста.

Квалифицированный вид создания, использования и распространения вредоносных программ для ЭВМ предусмотрен в ч. 2 ст. 273 УК. В отличие от простого состава, квалифицированный сконструирован как материальный состав преступления и для него необходимым является причинение по неосторожности тяжких последствий. Именно с момента наступления таких последствий преступление будет оконченным.

Законодатель в диспозиции ст. 273 УК не раскрывает понятия "тяжкие последствия", оно является оценочным и должно определяться судом в каждом конкретном случае. Очевидно, что к тяжким должны быть отнесены случаи внедрения вредоносных программ в системы, регулирующие безопасность жизни и здоровья граждан (например, в диспетчерские системы на транспорте, особенно воздушном, системы, обеспечивающие обороноспособность страны, отвечающие за экологическую безопасность), случаи гибели людей либо причинения тяжкого вреда здоровью, а также значительного экономического ущерба государству, юридическим и физическим лицам в результате дезорганизации работы производственных комплексов, нарушения организованной работы транспорта, уничтожения или повреждения имущества. При этом возможна квалификация по совокупности с иными тяжкими преступлениями, предусматривающими аналогичные последствия по неосторожности. Так, создание, использование и распространение вредоносных программ, в результате которых по неосторожности наступила смерть человека, например в силу нарушения технологического процесса на производстве, должны квалифицироваться по совокупности.

Субъективная сторона преступления характеризуется неосторожной формой вины. Лицо предвидит возможность наступления тяжких последствий, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение либо не предвидит возможность их наступления, хотя при необходимой внимательности и предусмотрительности должно было и могло их предвидеть. Некоторые авторы рассматривают данное преступление как преступление с двойной формой вины - умыслом по отношению к деянию и неосторожностью по отношению к последствиям. "Специфика квалифицированного вида преступления заключается в том, что оно совершается с двумя формами вины, то есть характеризуется умыслом относительно факта создания, использования или распространения вредоносной программы для ЭВМ и неосторожностью (легкомыслием либо небрежностью) относительно наступления тяжких последствий"[[82]](#footnote-82). Однако в соответствии со ст. 27 УК двойная форма вины характеризуется такими обстоятельствами, когда в результате совершения умышленного преступления причиняются тяжкие последствия, которые по закону влекут более строгое наказание и не охватывались умыслом лица. Подобные случаи имеют место, как правило, в квалифицированных составах, когда и простой, и квалифицированный являются материальными и формальный (ч. 4 ст. 111, ч. 2 ст. 167 УК). В данной же статье простой состав преступления является формальным, поэтому в квалифицированном составе нельзя говорить о тяжких последствиях, которые по закону влекут более строгое наказание. Следовательно, в данном преступлении форма вины - неосторожность.

**2.4 Признаки нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети**

Общественная опасность нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети заключается в том, что это может привести к уничтожению, блокированию или модификации охраняемой законом компьютерной информации и причинению существенного вреда собственнику, владельцу или пользователю ЭВМ, системы ЭВМ или их сети[[83]](#footnote-83).

Объектом рассматриваемого преступления является состояние защищенности ЭВМ, системы ЭВМ или их сети от угроз, связанных с нарушением правил их эксплуатации.

Предметом этого преступления являются электронно-вычислительные машины (ЭВМ), системы ЭВМ или их сети[[84]](#footnote-84).

С объективной стороны данное преступление выражается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети. Эти нарушения могут выражаться в несоблюдении правил эксплуатации аппаратного обеспечения ЭВМ, системы ЭВМ или их сети либо правил эксплуатации программного обеспечения, предназначенного для функционирования ЭВМ, системы ЭВМ или их сети. Обязательным признаком объективной стороны рассматриваемого преступления является наступление определенного последствия нарушения правил эксплуатации ЭВМ и других устройств в виде уничтожения, блокирования или модификации охраняемой законом компьютерной информации — существенного вреда их собственнику, владельцу или пользователю. Понятие уничтожения, блокирования и модификации информации ЭВМ уже подробно раскрывалось применительно к составу, предусмотренному ст. 272[[85]](#footnote-85).

Существенность вреда собственнику, владельцу или пользователю компьютерной информации определяется с учетом фактических обстоятельств совершенного преступления и является вопросом факта. Например, причиненный вред следует признавать существенным, если в результате нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети утрачена важная компьютерная информация, повлекшая дезорганизацию производственной деятельности государственной или коммерческой организации, или оно вызвало сложный и дорогостоящий ремонт вычислительной техники, повлекло продолжительный перерыв в обмене информацией между ЭВМ, объединенными в систему ЭВМ или их сеть. Между нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети и наступившими последствиями, о которых говорится в законе, должна быть установлена причинная связь. Рассматриваемое преступление относится к материальным составам преступлений и считается оконченным с момента наступления указанных в законе последствий.

С субъективной стороны данное преступление может быть совершено как умышленно, так и по неосторожности.

Субъектом этого преступления может быть любое лицо, достигшее 16-летнего возраста и имеющее доступ к ЭВМ, системе ЭВМ или их сети. Под имеющим доступ к ЭВМ, системе ЭВМ или их сети понимается лицо, которое по характеру своей работы либо в связи с эксплуатацией ЭВМ и других устройств, либо с их техническим обслуживанием может беспрепятственно пользоваться названными выше устройствами[[86]](#footnote-86).

Это деяние при отсутствии квалифицирующих признаков (ч. 1 ст. 274) относится к категории преступлений небольшой тяжести.

Квалифицирующим признаком данного преступления является наступление по неосторожности тяжких последствий в результате нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети (ч. 2 ст. 274). Понятие тяжких последствий является оценочным. Тяжесть последствий определяется с учетом всех фактических обстоятельств содеянного. Например, тяжким последствием можно считать безвозвратную утрату особо ценной компьютерной информации, уничтожение системы ЭВМ или их сети, несчастные случаи с людьми и т. п[[87]](#footnote-87).

Рассматриваемое преступление при наличии указанного квалифицирующего признака относится к категории преступлений средней тяжести.

Таким образом, нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети является основанием уголовной ответственности. Объектом рассматриваемого преступления является состояние защищенности ЭВМ, системы ЭВМ или их сети от угроз, связанных с нарушением правил их эксплуатации. С объективной стороны данное преступление выражается в нарушении правил эксплуатации ЭВМ, системы ЭВМ или их сети. Эти нарушения могут выражаться в несоблюдении правил эксплуатации аппаратного обеспечения ЭВМ, системы ЭВМ или их сети либо правил эксплуатации программного обеспечения, предназначенного для функционирования ЭВМ, системы ЭВМ или их сети. С субъективной стороны данное преступление может быть совершено как умышленно, так и по неосторожности. Субъектом этого преступления может быть любое лицо, достигшее 16-летнего возраста и имеющее доступ к ЭВМ, системе ЭВМ или их сети

**Заключение**

Дипломная работа, посвященная правовому регулированию компьютерной информации как объекта уголовно-правовой охраны , позволяет сформулировать следующие выводы:

1. Информация - сведения (сообщения, данные) независимо от формы их представления.

Правовое регулирование информации осуществляется Федеральным законом от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации".

2. Согласно ст. 5 Согласно ст. 2 Федерального закона от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации" информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Статья 128 ГК РФ относит информацию к объектам гражданских прав наряду с вещами (включая деньги и ценные бумаги), иным имуществом, в том числе имущественными правами; работами и услугами; результатами интеллектуальной деятельности, в том числе исключительными правами на них (интеллектуальной собственностью); нематериальными благами.

3. Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу. Целями защиты являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение угроз безопасности личности, общества, государства; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности; защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах; сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством; обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

4. В главе 28 Уголовного кодекса РФ предусмотрены три состава преступлений: неправомерный доступ к компьютерной информации (ст. 272), создание, использование и распространение вредоносных программ для ЭВМ (ст. 273) и нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274).

Родовым объектом компьютерных преступлений является общественная безопасность. В качестве дополнительных объектов в ряде случаев могут выступать права и интересы граждан в сфере обеспечения личной, семейной, врачебной и т.п. тайны, интересы собственности, защищенность государственной, банковской тайны и т.п.

Видовым объектом преступлений, предусмотренных в гл. 28 УК, является совокупность общественных отношений, обеспечивающих состояние защищенности процессов создания, сбора, хранения, передачи и использования компьютерной информации, в которых правомерно участвуют собственники, владельцы и пользователи информации (информационная безопасность).

Большей частью преступления в сфере компьютерной информации могут совершаться только путем действия - неправомерный доступ к компьютерной информации или создание либо использование вредоносных программ для ЭВМ. Однако нарушение установленных правил эксплуатации ЭВМ, системы ЭВМ или их сети возможно и путем бездействия - в виде невыполнения обязательных предписаний таких правил.

С субъективной стороны анализируемые преступления могут совершаться с различными формами вины.

Субъект анализируемых преступлений по общему правилу - общий.

А также исследование данной темы позволило сформулировать следующие предложения по совершенствованию законодательства в сфере компьютерной информации:

1. В ч. 2 ст. 273 и ч. 1 и ч. 274 УК РФ указаны такие понятия как тяжкие последствия и существенный вред (ст. 274 УК РФ). Но Уголовный кодекс не дает разъяснений того, что понимается под существенным вредом или тяжкими последствиями, равно как и не дает разъяснений, чему или кому причинен вред: информации, бизнесу, репутации фирмы или гражданина.

Эффективность норм о посягательствах в сфере компьютерной информации значительно снижается из-за оценочного характера понятия тяжких последствий. На практике его содержание определяется в каждом конкретном случае с учетом всей совокупности обстоятельств дела. Разумеется, к тяжким последствиям следует относить, например, причинение крупного материального ущерба, серьезное нарушение деятельности предприятий, организаций и учреждений, наступление аварий и катастроф, причинение вреда здоровью людей.

Однако даже в случае привлечения к оценке тяжести причиненного вреда специалистов и экспертов она в конечном счете определяется усмотрением судебно-следственных органов, а не буквой закона.

Поэтому для облегчения правоприменения, предлагаем внести изменения в ч. 2 ст. 273 и 274 УК РФ, вместо «тяжкие последствия» изменить на «крупный размер», а также предлагаем изменить ч. 1 ст. 274 УК РФ, вместо «существенный вред» изменить на «значительный ущерб», определения которых дано в примечании ст. 158 УК РФ. А также предлагаем дополнить ст. 273 и 274 УК РФ частью третей в котором будет предусмотрено в «особо крупном размере», определение которого тоже дано в примечании ст. 158 УК РФ.

2. Совершение деяния, описанного в ч.1 ст.272 УК РФ, специальным субъектом (лицом с использованием своего служебного положения) предусмотрено в качестве квалифицированного состава.

Представляется, что законодатель под специальным субъектом понимал отдельных лиц, занимающих соответствующие руководящие должности в сфере применения компьютерной техники, программистов, операторов ЭВМ, наладчиков оборудования и т.д. Однако неконкретизированность формулировок уголовного закона, отсутствие в нем толкования понятия "служебное положение" не позволяют однозначно утверждать, что речь идет о статусе лица по месту работы, сопряженном исключительно с использованием компьютерной техники. Рассматриваемое квалифицирующее обстоятельство должно толковаться шире. В частности, так должно расцениваться использование лицом своих властных или иных служебных полномочий, форменной одежды и атрибутов, служебных удостоверений, а равно сведений, которыми оно располагает в связи со своим служебным положением.

3. Форма вины для основного состава компьютерных преступлений по ст. 273 и 274 УК РФ - прямой либо косвенный умысел. Форма вины, предусмотренная для квалифицированного состава данной категории преступлений (т.е. для состава преступления, совершенного при обстоятельствах, отягчающих ответственность, и влекущего применение более суровых мер воздействия по сравнению с основным составом), является крайне любопытной. Дело заключается в том, что квалифицированные составы практически всех преступных деяний характерны усилением степени вины правонарушителя по сравнению с формой вины, необходимой для квалификации действий правонарушителя по основному составу (например, основной состав преступления - убийство, квалифицированный - убийство из корыстных побуждений). Но в данном случае при форме вины, установленной для основного состава преступления в виде умысла, для его квалифицированного состава Кодексом предусмотрена форма вины исключительно в виде неосторожности: неосторожное причинение тяжких последствий при создании или использовании вирусных программ и неосторожное причинение тяжких последствий в результате нарушения правил эксплуатации влекут за собой лишение свободы соответственно на срок до 7 и до 4 лет. Умышленное причинение тяжких последствий при этом наказывается в рамках основного состава, за который санкции предусмотрены гораздо более легкие по сравнению с квалифицированным.

Поэтому надо статьи 273 и 274 УК РФ добавить частью третьей, в котором будет предусмотрено ответственность за умышленные причинения тяжких последствий, и в которых санкции будут более суровыми.

### Список источников

1. Конституция Российской Федерации. Принятая всенародным голосованием 12 декабря 1993 года// Российская газета, 25 декабря, 1993.

2. Гражданский кодекс Российской Федерации(часть первая) от 30 ноября 1994 г. N 51-ФЗ// Собрание законодательства Российской Федерации от 5 декабря 1994 г. N 32 ст. 3301; 2006 г. N 31 (часть I) ст. 3437; Парламентская газета, 8 января, 2007

3. Уголовный кодекс Российской Федерации от 13.06. 1996. № 63-ФЗ// Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954; 2006, № 31, 3152; Российская газета, 10 января 2007.

4. Закон РФ от 23.09.1992. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»// Ведомости СНД РФ и ВС РФ, 22.10.1992, N 42, ст. 2325; Собрание законодательства Российской Федерации от 6 февраля 2006 г. N 6 ст. 636.

5. Закон РФ от 9.07.1993. № 5351-1 «Об авторском и смежных правах»// Ведомости СНД и ВС РФ, 12.08.1993, N 32, ст. 1242; Собрании законодательства Российской Федерации от 26 июля 2004 г. N 30 ст. 3090

6. Закон РФ от 21 июля 1993 г. N 5485-1 "О Государственной тайне"// Собрании законодательства Российской Федерации от 13 октября 1997 г., N 41, ст. 4673; 2004 г. N 35 ст. 3607; 1997 г., N 41, ст. 4673.

7. Федеральный закон от 15 ноября 1997 г. N 143-ФЗ "Об актах гражданского состояния"// Собрании законодательства Российской Федерации от 24 ноября 1997 г., N 47, ст. 5340; 2006 г. N 31 (часть I) ст. 3420

8. Федеральный закон от 7 июля 2003 г. N 126-ФЗ "О связи"// Собрании законодательства Российской Федерации от 14 июля 2003 г. N 28 ст. 2895; 2006 г. N 31 (часть I) ст. 3452.

9. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// Собрании законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448

10. Указ Президента РФ от 24 января 1998 г. N 61 "О перечне сведений, отнесенных к государственной тайне"// Собрании законодательства Российской Федерации от 2 февраля 1998 г. N 5 ст. 561

11. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. N Пр-1895)// "Российской газете" от 28 сентября 2000 г. N 187, в "Парламентской газете" от 30 сентября 2000 г., N 187

1. Зумакулов Д., Прохоров Л. Квалификация компьютерных преступлений//Российская юстиция. 2000. N 8. С. 36 [↑](#footnote-ref-1)
2. Виктимилогическая практика //Под ред. А.К. Лазарева. –М., 2002.С.34. [↑](#footnote-ref-2)
3. Конституция Российской Федерации. Принятая всенародным голосованием 12 декабря 1993 года// Российская газета, 25 декабря, 1993. [↑](#footnote-ref-3)
4. Уголовный кодекс Российской Федерации от 13.06. 1996. № 63-ФЗ// Собрание законодательства РФ, 17.06.1996, N 25, ст. 2954; Российской газете" - 10.01.2007 [↑](#footnote-ref-4)
5. Закон РФ от 23.09.1992. № 3523-1 «О правовой охране программ для электронных вычислительных машин и баз данных»// Ведомости СНД РФ и ВС РФ, 22.10.1992, N 42, ст. 2325. [↑](#footnote-ref-5)
6. Закон РФ от 9.07.1993. № 5351-1 «Об авторском и смежных правах»// Ведомости СНД и ВС РФ, 12.08.1993, N 32, ст. 1242. [↑](#footnote-ref-6)
7. Федеральный закон «О связи» от 16.02.1995. № 15-ФЗ// Собрание законодательства РФ. 1995. № 8.Ст.600. [↑](#footnote-ref-7)
8. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// Собрании законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448 [↑](#footnote-ref-8)
9. См.: Черных П.Я. Историко-этимологический словарь русского языка. М., 1993, с. 335. [↑](#footnote-ref-9)
10. Норберт Винер. Кибернетика или управление и связь в животном и машине. –М., 1989г.С,22. [↑](#footnote-ref-10)
11. См.: Ожегов С.И. Словарь русского языка. М., 1952, с. 220. [↑](#footnote-ref-11)
12. См.: Даль В.И. Толковый словарь живого великорусского языка. Т. 4. М., 1994, с. 155. [↑](#footnote-ref-12)
13. п.1 Письмо Высшего Арбитражного Суда РФ от 7 июня 1995 г. N С1-7/оз-316 О Федеральном законе "Об информации, информатизации и защите информации"// Вестник Высшего Арбитражного Суда Российской Федерации, 1995, N 9 [↑](#footnote-ref-13)
14. Батурин Ю. М. Проблемы компьютерного права. М., 1999.С.32 [↑](#footnote-ref-14)
15. Правовая информатика /Под ред. А.Б. Новиков. –М.,2004.С.25. [↑](#footnote-ref-15)
16. Глушков К.В. Правовая информатика. –М., 2003. [↑](#footnote-ref-16)
17. См.: Б. Кадомцев. Динамика и информация//Успехи физических наук. 1994, N 5, с. 164. [↑](#footnote-ref-17)
18. См.: Мелик-Гайказян И.В. Информационные процессы и реальность. М., 1997. [↑](#footnote-ref-18)
19. Чубукова С.Г. Элькин В.Д. Основы правовой информатики (юридические и математические вопросы информатики): Учебное пособие/Под ред. доктора юридических наук, профессора М.М. Рассолова, кандидата технических наук, профессора В.Д. Элькина. - "Юридическая фирма "Контракт", 2004 г. [↑](#footnote-ref-19)
20. См: Бачило И.Л. Информация как объект правоотношений // НТИ. Сер. 1. М., 1997; Информационные ресурсы как объект права и отношений, регулируемых ГК РФ // Информационные ресурсы России. 1999. N 1; Информация и информационные отношения в праве // НТИ. Сер. 1. 1999. N 8; Копылов В.А. Информация как объект гражданского права; проблемы дополнения Гражданского кодекса РФ // Информационные ресурсы России. 1998. N 5. [↑](#footnote-ref-20)
21. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.23 [↑](#footnote-ref-21)
22. См., например: Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М.: Издат. группа "Юрист", 2001, с. 12-20; Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник/Под ред. Б.Н. Топорнина. СПб.: Изд-во "Юридический центр Пресс", 2001, с. 143-146. [↑](#footnote-ref-22)
23. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.26 [↑](#footnote-ref-23)
24. См: Бачило И.Л. Информация как объект правоотношений // НТИ. Сер. 1. М., 1997; Информационные ресурсы как объект права и отношений, регулируемых ГК РФ // Информационные ресурсы России. 1999. N 1; Информация и информационные отношения в праве // НТИ. Сер. 1. 1999. N 8; Копылов В.А. Информация как объект гражданского права; проблемы дополнения Гражданского кодекса РФ // Информационные ресурсы России. 1998. N 5. [↑](#footnote-ref-24)
25. Народная газета Московского региона", N 12, 28.10.2001., [↑](#footnote-ref-25)
26. Батурин Ю. М. Проблемы компьютерного права. М., 1999.С.32 [↑](#footnote-ref-26)
27. Вехов В. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательства стран СНГ//Уголовное право. № 3 2004. С. 17 [↑](#footnote-ref-27)
28. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.30. [↑](#footnote-ref-28)
29. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.30. [↑](#footnote-ref-29)
30. Вехов В. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательства стран СНГ//Уголовное право. № 3 2004. С. 18 [↑](#footnote-ref-30)
31. См.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право: Учебник/Под ред. Б.Н. Топорнина. СПб.: Изд-во "Юридический центр Пресс", 2001, с. 139. [↑](#footnote-ref-31)
32. См.: Фатьянов А.А. Правовое обеспечение безопасности информации в Российской Федерации. М.: Издат. группа "Юрист", 2001, с. 38-44. [↑](#footnote-ref-32)
33. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.31 [↑](#footnote-ref-33)
34. Соколова О.С. Персональные данные как информация ограниченного доступа: проблемы правового регулирования// Современное право. № 2. 2004.С.29. [↑](#footnote-ref-34)
35. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.31 [↑](#footnote-ref-35)
36. Вехов В. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательства стран СНГ//Уголовное право. № 3 2004. С. 19 [↑](#footnote-ref-36)
37. Зверева Е.А. Информация как объект имущественных гражданских прав// Право и экономика, 2003, № 9.С.26 [↑](#footnote-ref-37)
38. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М.: Право и закон, 1996. С. 24. [↑](#footnote-ref-38)
39. Селиванов Н. Проблемы борьбы с компьютерной преступностью//Законность. 1993. N 8. С. 36 [↑](#footnote-ref-39)
40. Вус М.А., Войтович Н.А., Гусев В.С. Россия на пороге информационного общества//Россия на пороге информационного общества. Материалы семинара 22 апреля 1997 г. СПб., 1997. [↑](#footnote-ref-40)
41. Селиванов Н. Проблемы борьбы с компьютерной преступностью//Законность. 1993. N 8. С. 38 [↑](#footnote-ref-41)
42. См.: Зумакулов Д., Прохоров Л. Квалификация компьютерных преступлений//Российская юстиция. 2000. N 8. С. 36-37. [↑](#footnote-ref-42)
43. Голованов В.А. Модельный уголовный кодекс СНГ// Уголовное право. № 5 2003.С.14. [↑](#footnote-ref-43)
44. См.: Боер В.М. Информационно-правовая политика России. СПб., 1998. С. 187. [↑](#footnote-ref-44)
45. Собрание законодательства Российской Федерации. 1996. N 28. Ст. 3347. [↑](#footnote-ref-45)
46. Доктрина информационной безопасности Российской Федерации. Утв. Президентом РФ 9 сентября 2000 г. N Пр-1895. Ст. 1//Российская газета. N 187. 2000. 28 сент. [↑](#footnote-ref-46)
47. Вус М.А., Войтович Н.А., Гусев В.С. Указ. соч. 1997. С. 6. [↑](#footnote-ref-47)
48. См.: Собрание законодательства Российской Федерации. 1995. N 8. Ст. 609. [↑](#footnote-ref-48)
49. См. там же. 1994. N 35. Ст. 3648. [↑](#footnote-ref-49)
50. См., например: Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления//Законность. 1997. N 1. [↑](#footnote-ref-50)
51. См. подробнее раздел "Международные преступления" курса уголовного права. Том 4. Особенная часть (под ред. доктора юридических наук, профессора Г.Н.Борзенкова и доктора юридических наук, профессора В.С.Комиссарова) - М.: ИКД "Зерцало-М", 2002 [↑](#footnote-ref-51)
52. Селиванов Н. Проблемы борьбы с компьютерной преступностью//Законность. 1993. N 8. С. 44 [↑](#footnote-ref-52)
53. Вус М.А., Войтович Н.А., Гусев В.С. Указ. соч. 1997. С. 6. [↑](#footnote-ref-53)
54. Постановление Пленума Верховного Суда РФ от 25 апреля 1995 г. N 5 "О некоторых вопросах применения судами законодательства об ответственности за преступления против собственности"// Бюллетень Верховного Суда Российской Федерации, 1995, N 7, стр. 2, [↑](#footnote-ref-54)
55. Голубев В.В. Новое уголовное право России: Особенная часть: Учебное пособие. М., 1996. С.273. [↑](#footnote-ref-55)
56. Симкин Л.С. Программы для ЭВМ: правовая охрана (правовые аспекты против компьютерного пиратства). М., 1998. С. 91. [↑](#footnote-ref-56)
57. Федеральный закон от 27 июля 2006 г. N 149-ФЗ "Об информации, информационных технологиях и о защите информации"// Собрании законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448 [↑](#footnote-ref-57)
58. См.: Симкин Л.С. Как остановить компьютерное пиратство?//Российская юстиция. 1996. N 10. [↑](#footnote-ref-58)
59. Кузнецова Н.Ф. Квалификация сложных составов преступлений//Уголовное право. 2000. N 1. С. 26. [↑](#footnote-ref-59)
60. См., например: Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления//Законность. 1997. N 1. [↑](#footnote-ref-60)
61. Закон РФ от 21 июля 1993 г. N 5485-1 "О государственной тайне" в ред. Федерального закона от 6 октября 1997 г. N 131-ФЗ (Собрание законодательства Российской Федерации. 1997. N 41. Ст. 8220, 4673). Перечень сведений, отнесенных к государственной тайне, утвержден Указом Президента РФ от 24 января 1998 г. N 61 "О перечне сведений, отнесенных к государственной тайне" (Собрание законодательства Российской Федерации. 1998. N 5. Ст. 561). Подробнее о государственной тайне см. гл. 1 т. 5 настоящего курса. [↑](#footnote-ref-61)
62. См.: Собрание законодательства Российской Федерации. 1997. N 10. Ст. 1127. [↑](#footnote-ref-62)
63. См. там же. 1997. N 47. Ст. 5340. [↑](#footnote-ref-63)
64. См. ст. 5 Федерального закона от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности" с последующими изменениями и дополнениями//Собрание законодательства Российской Федерации. 1995. N 33. Ст. 3349; Российской газете" - 06.12.2005 [↑](#footnote-ref-64)
65. См. ст. 61 Основ законодательства Российской Федерации "Об охране здоровья граждан", принятых 22 июля 1993 г. N 5487-1 с последующими изменениями и дополнениями//Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. N 33. Ст. 1318; Собрание актов Президента и Правительства Российской Федерации. 1993. N 52. Ст. 5086; Собрание законодательства Российской Федерации. 1998. N 10. Ст. 1143; 1999. N 37. Ст. 4506; N 51. Ст. 6289; 2000. N 49. Ст. 4740. [↑](#footnote-ref-65)
66. См. ст. 5, 17 Основ законодательства Российской Федерации "О нотариате" от 11 февраля 1993 г. N 4462-1//Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1993. N 10. Ст. 357. [↑](#footnote-ref-66)
67. Федеральный закон от 31 мая 2002 г. N 63-Ф3 "Об адвокатской деятельности и адвокатуре в Российской Федерации"// "Собрание законодательства РФ", 10.06.2002, N 23, ст. 2102; "Российской газете" - 23.12.2004 [↑](#footnote-ref-67)
68. См. ст. 3 Федерального закона от 26 сентября 1997 г. N 125-ФЗ "О свободе совести и о религиозных объединениях" в ред. Федерального закона от 26 марта 2000 г. N 45-ФЗ//Собрание законодательства Российской Федерации. 1997. N 39. Ст. 4465; 2000. N 14. Ст. 1430. [↑](#footnote-ref-68)
69. См. ст. 12 Федерального закона от 12 августа 1995 г. N 144-ФЗ "Об оперативно-розыскной деятельности". [↑](#footnote-ref-69)
70. СП РФ. 1992. N 1-2. Ст. 7. [↑](#footnote-ref-70)
71. См.: Собрание законодательства Российской Федерации. 1996. N 6. Ст. 492; 1998. N 31. Ст. 3829; 1999. N 28. Ст. 3469, 3470. [↑](#footnote-ref-71)
72. См.: Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. N 42. Ст. 2319. [↑](#footnote-ref-72)
73. См.: Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М., 1999; Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М., 1996. [↑](#footnote-ref-73)
74. Крылов В.В. Информационные компьютерные преступления. М., 1997. С. 32, 34. [↑](#footnote-ref-74)
75. Зумакулов Д., Прохоров Л. Квалификация компьютерных преступлений//Российская юстиция. 2000. N 8. С. 36. [↑](#footnote-ref-75)
76. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления//Законность. 1999. N 1.С.54. [↑](#footnote-ref-76)
77. См.: Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. N 42. Ст. 2325. [↑](#footnote-ref-77)
78. Крылов В.В. Информационные компьютерные преступления. М., 1997. С. 32, 34. [↑](#footnote-ref-78)
79. Уголовное право. Особенная часть/под ред. Н.И.Ветрова и Ю.И.Ляпунова. М.: Новый юрист, 1998. С. 555. [↑](#footnote-ref-79)
80. Черных А.В. Некоторые вопросы квалификации компьютерного саботажа за рубежом//СГП. 1999. N 8. С. 72-73. [↑](#footnote-ref-80)
81. Уголовное право. Особенная часть/под ред. Н.И.Ветрова и Ю.И.Ляпунова. М.: Новый юрист, 1998. С. 555. [↑](#footnote-ref-81)
82. Уголовное право. Особенная часть/под ред. Н.И.Ветрова и Ю.И.Ляпунова. М.: Новый юрист, 1998. С. 555. [↑](#footnote-ref-82)
83. Уголовное право РФ. Часть Общая. Часть Особенная./ Под ред. Л.Д. Гаухмона. –М., 1999.С.580 [↑](#footnote-ref-83)
84. Таганцев Н. С. Русское уголовное право, Общая часть. Т. 1. –Тула., 2001.С.362. [↑](#footnote-ref-84)
85. Уголовное право/ Под ред. Н.И. Ветрова. –М., 1997.С.206 [↑](#footnote-ref-85)
86. Уголовное право России. Части Общая и Особенная/ М.П. Журавлев, А.В Наумов и др. –М., 2004.С.431. [↑](#footnote-ref-86)
87. Наумов А.В. Российское уголовное право. Общая часть. –М., 1998.С.213. [↑](#footnote-ref-87)