# ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Глава 1 Преступления в сфере компьютерной информации в системе преступлений против общественной безопасности и общественного порядка

1.1 История развития законодательства об уголовной ответственности за преступления в сфере компьютерной информации

1.2 Уголовная ответственность за преступления в сфере компьютерной информации по законодательству зарубежных стран

Глава 2 Характеристика составов преступлений в сфере компьютерной информации

2.1 Характеристика общих объективных и субъективных признаков преступлений в сфере компьютерной информации

2.2 Особенности характеристики неправомерного доступа к компьютерной информации

2.3 Особенности характеристики создания, использования и распространения вредоносных программ для ЭВМ

2.4 Особенности характеристики нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети

ЗАКЛЮЧЕНИЕ

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

# ВВЕДЕНИЕ

В последние годы проблема преступности в сфере компьютерной информации приобрела особую остроту и актуальность. Эта проблема, заявившая о себе в развитых странах Запада во второй половине 60-х годов, а в нашей стране – на рубеже 70 – 80-х годов, в настоящее время все больше проявляет тенденцию к росту, распространенности и повышенной опасности. К причинам возникновения компьютерной преступности можно отнести: информационно-технологическое переоборудование предприятий, учреждений и организаций, насыщение их компьютерной техникой, программным обеспечением, базами данных; а также реальную возможность получения значительной экономической выгоды от противоправных деяний с использованием ЭВМ.

С момента зарождения человеческого общества люди испытывают потребность в общении друг с другом. Первоначально общение (обмен сведениями) осуществлялось жестами, знаками, мимикой и нечленораздельными звуками, затем появились человеческая речь, письменность, книгопечатание. В ХХ столетии получили развитие такие средства коммуникации, как телеграф, телефон, радио, кино, телевидение, компьютер. Параллельно проходил и иной процесс: по мере появления различных достижений науки и техники многие из них принимались на вооружение преступного мира. Однако внедрение во все сферы деятельности компьютерной техники сыграло наиболее существенную роль в деле технического вооружения преступности. «Невидимость» компьютерного преступника и одновременно «удлинение его рук» путем доступа к любым охраняемым секретам – военным, финансовым, иным – делают компьютерную технику весьма привлекательной для представителей преступного мира.

Опасность подобного рода деяний определяется еще и тем, что компьютер постепенно во всем мире заполняет все сферы жизнедеятельности человека, что позволяет преступникам значительно расширить свою экспансию. «Спектр преступного использования компьютеров практически равен спектру его применения по прямому назначению, а это означает, что преступное вторжение через ЭВТ может быть произведено в сферу космической и оборонной индустрии, политики и международных отношений и т.п.».

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.

Статистика свидетельствует о тенденции устойчивого роста числа преступлений в сфере компьютерной информации на протяжении 2002 – 2007 гг.: в 2002 году – 4050, в 2003 году – 7541, в 2004 году – 8739, в 2005 году – 10216, в 2006 году – 12131, в 2007 году – 12338[[1]](#footnote-1).

Количество зарегистрированных преступлений в сфере компьютерной информации за 2007 отчетный год в 3,1 раза превышает аналогичные показатели за 2002 год при среднегодовом показателе роста в 155,34%. При этом число осужденных за тот же период возросло значительно меньше – со 109 до 260 человек, то есть в 2,4 раза.

Исключение – преступления, связанные с нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК РФ[[2]](#footnote-2)). Так, за период 2001 – 2007 гг. их было зарегистрировано 160, а осужден только 2 человека.

Как показывает практика, квалификация преступлений, совершаемых в сфере компьютерной информации, представляет определенные трудности. Особенно при оценке неправомерного доступа к компьютерной информации как самого распространенного общественно опасного деяния в рассматриваемой сфере. Указанные обстоятельства и обусловливают актуальность выбранной темы дипломного исследования.

Объектом данного исследования является совокупность общественных отношений, связанных с привлечением виновного лица к уголовной ответственности за совершение компьютерных преступлений. Предметом же выступают нормы уголовного законодательства как России, так и зарубежных стран, статистические и справочные материалы, материалы судебной практики, учебная и научная литература.

Целью данного исследования является комплексный анализ системы компьютерных преступлений по Уголовному кодексу Российской Федерации.

К задачам данного исследования можно отнести:

* рассмотрение истории развития законодательства России об уголовной ответственности за совершение компьютерных преступлений;
* анализ норм уголовного законодательства зарубежных стран об уголовной ответственности за совершение компьютерных преступлений;
* общая характеристика компьютерных преступлений, предусмотренных УК РФ (ст. 272-274), а также анализ отдельных признаков составов данных преступлений.

Задачи исследования определяют его структуру. Работа состоит из введения, двух глав, заключения, списка использованных источников и литературы.

Методологическую основу данного исследования составляют как общенаучные (анализ, синтез, индукция, дедукция, классификация и т.д.), так и частнонаучные (формально-юридический, исторический, системный и т.д.) методы юридического исследования. Особое внимание уделено использованию метода сравнительного правоведения, который предполагает сопоставление норм недействующего законодательства с нормами действующего законодательства или сравнение норм законодательства разных стран с целью выявления недостатков и достоинств тех или иных правовых норм.

Компьютерные преступления представляют собой проблему, которая в науке отечественного уголовного права представляется довольно плохо изученной. Причиной этого, несомненно, является относительно небольшая доля компьютерных преступлений в структуре преступности, а также слабое внимание законодателя к нормам об уголовной ответственности за совершение компьютерных преступлений (так, с момента принятия УК РФ в 1996 году, в статьи 272-274 не было внесено ни одной поправки).

Среди ученых, посвятивших свои труды проблеме компьютерных преступлений, можно выделить таких специалистов как Б. В. Волженкин, О. В. Мосин, Л. А. Осипенко, Л. Н. Соловьев, И. А. Юрченко и ряд других.

# Глава 1 Преступления в сфере компьютерной информации в системе преступлений против общественной безопасности и общественного порядка

# 1.1 История развития законодательства об уголовной ответственности за преступления в сфере компьютерной информации

Человечеству потребовалось немало времени, чтобы от первых, примитивных счетных устройств XVII века перейти к использованию сверхбыстродействующих, с огромным объемом памяти (по нынешним меркам) электронно-вычислительных машин (ЭВМ), способных собирать, хранить, перерабатывать, передавать и выдавать любую информацию. Появление на рынке в 1974 году компактных и сравнительно недорогих персональных компьютеров, по мере совершенствования которых стали размываться границы между мини- и большими ЭВМ, дали возможность подключаться к мощным информационным потокам неограниченному кругу лиц. Встал вопрос о контролируемости доступа к информации, ее сохранности и доброкачественности. Организационные меры, а также программные и технические средства защиты оказались недостаточно эффективными. Особенно остро проблема несанкционированного вмешательства дала о себе знать в странах с высокоразвитыми технологиями и информационными сетями. Вынужденные прибегать к дополнительным мерам безопасности, они стали активно использовать правовые, в том числе уголовно-правовые средства защиты[[3]](#footnote-3).

В 1992 году был принят Закон России о правовой охране программ для электронно-вычислительных машин и баз данных[[4]](#footnote-4), в 1994 году – Гражданский кодекс, который содержит ряд норм, связанных с компьютерной информацией, в 1995 году – Федеральный закон об информации, информатизации и защите информации[[5]](#footnote-5). Логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за так называемые компьютерные преступления.

Основным средством борьбы с преступными нарушениями нормального функционирования компьютерной техники должно было стать уголовное законодательство. Российские правоведы уже давно ставили вопрос о необходимости законодательного закрепления правоотношений, вытекающих из различных сфер применения средств автоматической обработки информации. Однако сформулированные в 1996 году уголовно-правовые нормы, направленные на борьбу с компьютерными преступлениями, были результатом множества реформ законодательства в этой сфере.

Первой попыткой решить вопрос о необходимости борьбы с компьютерными преступлениями стала разработка в 1991 году проекта Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который предусматривал основания для дисциплинарной, гражданско-правовой, административной, уголовной ответственности за подобные деяния. Однако он так и не был принят, главным образом из-за общей неразработанности законодательного поля в данной области права[[6]](#footnote-6).

Прорывом в этом направлении правотворчества явилось принятие Верховным Советом России 23 сентября 1992 года упомянутого выше Закона «О правовой охране программ для электронных вычислительных машин и баз данных», который содержал положение о том, что выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких продуктов влечет за собой уголовную ответственность.

В последующие годы высшие органы власти уделяли уже повышенное внимание вопросам упорядочения отношений в сфере информации. В 1992 году принимается в общей сложности около 60 актов Верховного Совета России, Президента и Правительства в данной области, а в 1993 году – уже более 100[[7]](#footnote-7).

В 1994 году был разработан проект закона о внесении дополнений в УК РСФСР, которым устанавливалась ответственность за: незаконное овладение программами для ЭВМ, файлами и базами данных; фальсификацию или уничтожение информации в автоматизированной системе; незаконное проникновение в автоматизированную информационную систему, совершенное путем незаконного завладения парольно-ключевой информацией, нарушение порядка доступа или обход механизмов программной защиты информации с целью ее несанкционированного копирования, изменения или уничтожения; внесение и распространение «компьютерного вируса»; нарушение правил, обеспечивающих безопасность АИС. Но проект не был реализован ввиду постановки новой задачи в виде формирования уже в рамках нового Уголовного кодекса России преступлений в области компьютерной информации.

В январе – феврале 1995 года был разработан и опубликован проект УК РФ, в который была включена гл. 28 «Компьютерные преступления», устанавливающая ответственность за: самовольное проникновение в автоматизированную компьютерную систему (ст. 271); неправомерное завладение программами для ЭВМ, файлами и базами данных (ст. 272); самовольную модификацию, повреждение, уничтожение баз данных или программ для ЭВМ (ст. 273); внесение или распространение вирусных программ для ЭВМ (ст. 274); нарушение правил, обеспечивающих безопасность информационной системы (ст. 275). Юристами и специалистами в области информационных технологий было указано на существенные недостатки, в частности на отсутствие единой правовой концепции в главе, недостаточную связь с отраслевыми законами, слабую проработку терминологии и стилистику[[8]](#footnote-8).

Важное место в ряду нормативных правовых актов в области информационного права занял Федеральный закон от 20 февраля 1995 года «Об информации, информатизации и защите информации», давший определение многих терминов данной сферы деятельности. Этот Закон подготовил правовое поле для принятия нового уголовного законодательства, а в более отдаленной перспективе – и формирования целостного компьютерного права как самостоятельной отрасли. По отдельным подсчетам, за период с 1992 по июль 1995 года было издано таким образом около 500 нормативных правовых актов по вопросам информационного законодательства, в том числе 75 – полностью посвященных им[[9]](#footnote-9).

В 1996 году был принят Модельный уголовный кодекс государств – участников СНГ, содержавший нормы об ответственности за компьютерные преступления[[10]](#footnote-10).

С 1 января 1997 года был введен в действие Уголовный кодекс Российской Федерации, который содержит гл. 28 «Преступления в сфере компьютерной информации», включившую в себя ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Разработчики проекта УК РФ, ориентируясь на сходные представления об объекте уголовно-правовой охраны, предлагали объединить компьютерные посягательства в одну из глав раздела «Преступления против общественной безопасности», где нашли место почти все деяния, относимые указанными авторами вмешательству в работу компьютера.

УК РФ не воспринял формулировки, предложенные разработчиками проекта, хотя суть задуманного в принципе была сохранена; однако некоторые законодательные недоработки могут вызвать трудности в правоприменительной практике. В первую очередь это касается ст. 272 УК, предусматривающей ответственность за неправомерный доступ к компьютерной информации, «... если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети». Термин «повлекло» дает основание полагать, что объективная сторона данного состава преступления складывается из деяния (неправомерного доступа), последствий (уничтожение информации и т. д.) и причинной связи между ними. Этот состав преступления образовался путем объединения трех названных в проекте самостоятельных составов: а) самовольное проникновение в автоматизированную компьютерную систему, если это повлекло ознакомление ненадлежащих пользователей с конфиденциальной информацией», б) «неправомерное копирование программ для ЭВМ, файлов или баз данных, занесенных в память ЭВМ, если это повлекло причинение существенного вреда», и в) «самовольная модификация, повреждение, уничтожение баз данных или программ для ЭВМ»[[11]](#footnote-11).

Однако нельзя не признать, что уничтожение, блокирование, модификация и копирование информации не исключают совершения самостоятельных действий. Представляется, было бы правильнее рассматривать основанием уголовной ответственности за неправомерный доступ к компьютерной информации случаи, когда неправомерный доступ сопряжен с уничтожением, блокированием и т. д. (то есть такому доступу следовало бы придать значение не только причины, но и необходимого условия).

Есть и другие соображения, которые позволяют констатировать, что в статьях, посвященных преступлениям в сфере компьютерной информации, решение вопроса о последствиях содеянного оказывается наиболее слабо проработанным. Сам факт уничтожения, блокирования, модификации, копирования охраняемой законом информации причиняет ущерб владельцу информации, которую законодатель не без оснований ставит под защиту. Но серьезные препятствия в пользовании владельцем своей информацией могут возникать и в результате нарушения работы ЭВМ, системы ЭВМ, их сети, а стало быть, и такие последствия незаконных деяний должны влечь уголовную ответственность, причем в одних случаях как за посягательство на собственность, в других – за совершение компьютерных преступлений (вирусные программы способны выводить из строя, скажем, электронную начинку ЭВМ), а в третьих – по совокупности преступлений. Вместе с тем применительно к наказуемости нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети упоминается о последствиях в виде уничтожения, блокирования или модификации информации, но ничего не говорится о нарушении работы ЭВМ, системы ЭВМ, их сети. Не совсем понятно, почему при нарушении данных правил, если оно повлекло уничтожение информации, виновный может быть привлечен к уголовной ответственности, а при последствиях в виде нарушения работы ЭВМ – не может[[12]](#footnote-12).

Единый подход к решению данного вопроса диктуется не столько формальными соображениями, сколько тем, что при совершении любого компьютерного преступления возможны последствия второго уровня. Из периодической и научной печати многим стали известны случаи использования ЭВМ для взлома электронной банковской системы безопасности с целью похищения огромных денежных сумм или умышленной либо неосторожной дезорганизации работы систем национальной безопасности, крупнейших предприятий, диспетчерских служб и т. д.

В конечном счете, не так уж важно, почему именно (в результате «взлома», «шалости», появления компьютерного вируса, небрежности программиста) произошел сбой в работе компьютерной сети какого-либо технологического процесса: в любом случае последствия могут быть катастрофическими. Это, собственно, и есть одна из причин, по которой компьютерные преступления следует считать посягательствами не столько на интеллектуальную собственность, сколько на безопасность общества.

Вряд ли последовательным нужно признать такой подход, при котором неосторожное причинение тяжких последствий в результате, например, нарушения правил эксплуатации ЭВМ должно признаваться квалифицирующим обстоятельством, в то время как наступление такого рода последствий, вызванных неправомерным доступом к охраняемой законом компьютерной информации – не может[[13]](#footnote-13).

К сожалению, в отечественной специальной литературе до сих пор не нашли достаточного отражения проблемы правового регулирования международного сотрудничества в сфере борьбы с компьютерной преступностью, а также полученный в мировой практике опыт их решения, выработанные принципы, рекомендации, правовые нормы.

Нельзя считать до конца решенными вопросы правовой регламентации государственного контроля за развитием глобальных компьютерных сетей, что является одним из факторов, приводящим к отставанию России от промышленно развитых стран по уровню информатизации экономики и общества. Несовершенство этой нормативной правовой базы приводит к отсутствию четкости при проведении государственной политики в области формирования российского информационного пространства, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство. Кроме того, отдельные нормативные правовые акты вполне очевидно создавались без необходимых консультаций с техническими специалистами, в связи с чем закрепленные в них правовые положения не работоспособны на практике[[14]](#footnote-14).

Развитие информационных технологий заставляет интенсивно совершенствовать законодательную базу, вводит в юридическую сферу понятия, ранее применявшиеся в кибернетике и информатике.

В 2006 году был принят Федеральный закон «Об информации, информационных технологиях и защите информации»[[15]](#footnote-15), в котором даны новые определения информации, защиты информации и пр., сформулирован ряд новых подходов к охране информации, что не может не повлиять на содержание уголовно-правовых норм о компьютерных преступлениях.

Подводя итог, можно отметить, что интенсивное развитие технологий опережает реакцию законодателя, которому требуется время для адекватной регламентации в законах и иных нормативно-правовых актах отношений, возникающих в рассматриваемой сфере. Кроме того, очень важно разумно учитывать опыт других государств, которые, значительно раньше приступив к борьбе с преступлениями в сфере высоких технологий, выработали систему эффективных правовых средств этой борьбы.

# 1.2 Уголовная ответственность за преступления в сфере компьютерной информации по законодательству зарубежных стран

Принятие УК РФ поставило ряд проблем перед теоретиками уголовно-правовой науки: определить объект преступлений в сфере компьютерной информации, сформулировать их понятие и систему; установить критерии выделения близких по содержанию видов преступных посягательств, отграничение от других составов преступлений; решить вопрос квалификации, а также ответственности и наказания за них. Бланкетный характер диспозиций соответствующих уголовно-правовых норм требует обращения к различным правовым актам, регулирующим возникающие правоотношения, и знания терминологии.

Анализ специальной литературы показывает, что вопросам терминологии, используемой законодателем для формулирования норм о преступлениях в сфере компьютерной информации, не было уделено надлежащего внимания, что диктует исследование зарубежного опыта борьбы с этими преступлениями[[16]](#footnote-16).

В параметрах построения миропорядка на основе верховенства права важное место занимает борьба с международной преступностью. В рамках общепризнанного понимания в российской и зарубежной науке международного уголовного права установлено деление международных преступных деяний на международные преступления и преступления международного характера[[17]](#footnote-17).

В то время как международные преступления затрагивают интересы всего мирового сообщества и подлежат юрисдикции Международного уголовного суда, преступления международного характера касаются ряда отдельных государств и в рамках принципа двойной подсудности подпадают под регулятивное действие института выдачи (экстрадиции).

Характер новации в системе международного уголовного права в настоящее время приобрели преступления в сфере компьютерной информации, которые по всем меркам объективного анализа подпадают под понятие «преступления международного характера». Через консолидированные усилия государств предпринимаются меры по противодействию на международно-правовом и внутригосударственном уровнях преступлениям международного характера в сфере высоких технологий.

Для эффективной борьбы с преступлениями в сфере компьютерной информации необходимо учитывать опыт борьбы других стран[[18]](#footnote-18).

По мнению многих исследователей, проблема обеспечения безопасности компьютерных информации и технологий, в том числе и уголовно-правовыми средствами, является на сегодня одной из самых актуальных в большинстве развитых стран мира[[19]](#footnote-19).

Уголовно-правовое регулирование зарубежным законодательством вопросов уголовной ответственности за так называемые компьютерные преступления существенно отличается друг от друга. Не во всех государствах законодательство в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием компьютерных технологий и информации.

Определенный опыт законодательного регулирования в уголовном праве вопросов ответственности за совершение преступлений в сфере компьютерной информации накоплен государствами, входившими ранее в состав СССР и вошедших в состав Содружества Независимых Государств.

В Уголовном кодексе Республики Беларусь[[20]](#footnote-20) имеется семь статей, устанавливающих ответственность за следующие деяния: несанкционированный доступ к компьютерной информации (ст. 349), модификацию компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработку, использование либо распространение вредоносных программ (ст. 354), нарушение правил эксплуатации компьютерной системы или сети (ст. 355)[[21]](#footnote-21).

Таким же образом урегулированы вопросы уголовной ответственности за преступления против информационной безопасности в Уголовном кодексе Республики Таджикистан[[22]](#footnote-22) (ст. ст. 298–304).

С 1 сентября 2001 года вступил в действие Уголовный кодекс Украины[[23]](#footnote-23), которым установлена ответственность за ряд преступлений, родовым объектом посягательств которых согласно заглавию раздела XVI обозначена сфера использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей. В данный раздел включены: ст. 361 «Незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей»[[24]](#footnote-24); ст. 362 «Хищение, присвоение, вымогательство компьютерной информации либо завладение ею путем мошенничества или злоупотребления служебным положением»; ст. 363 «Нарушение правил эксплуатации автоматических электронно-вычислительных систем».

Кроме того, в ст. 301 УК Украины, устанавливающей ответственность за ввоз, изготовление, сбыт и распространение порнографических предметов, включен квалифицирующий признак совершения данных преступлений (ч. ч. 2 и 3): изготовление или использование компьютерных программ, что влечет за собой усиление наказания.

В конце 2004 года Верховная Рада Украины внесла изменения в Уголовный кодекс Украины относительно ответственности за преступления в сфере использования компьютеров. В частности, в новой редакции представлена ст. 361 УК Украины, в соответствии с которой уголовная ответственность будет наступать за несанкционированное вмешательство в работу ЭВМ (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, что привело к утечке; потере; подделке; блокированию информации; искажению процесса обработки информации; нарушению установленного порядка ее маршрутизации.

В то же время УК Украины дополняется новыми статьями, которые устанавливают уголовную ответственность за: создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт (ст. 361-1 УК Украины); несанкционированный сбыт или распространение информации с ограниченным доступом, которая хранится в ЭВМ (компьютерах), автоматизированных системах, компьютерных сетях или на носителях такой информации (ст. 361-2 УК Украины); препятствование работе электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи путем массового распространения сообщений электросвязи (ст. 363-3 УК Украины).

В новой редакции излагаются ст. ст. 362 и 363 УК Украины, которые устанавливают ответственность за: несанкционированные действия с информацией, которая обрабатывается в электронно-вычислительных машинах (компьютерах), автоматизированных системах, компьютерных сетях или хранится на носителях такой информации, содеянные лицом, которое имеет право доступа к ней (ст. 362 УК Украины); нарушение правил эксплуатации электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи или порядка или правил защиты информации, которая в них обрабатывается (ст. 363 УК Украины).

Уголовный кодекс Республики Узбекистан[[25]](#footnote-25) предусматривает такие составы преступлений, как: хищение путем присвоения и растраты с использованием средств компьютерной техники (п. «г» ч. 3 ст. 167); мошенничество с использованием средств компьютерной техники (п. «в» ч. 3 ст. 168); кража, совершенная с несанкционированным проникновением в компьютерную систему (п. «в» ч. 3 ст. 169); нарушение правил информатизации (ст. 174); незаконное собирание, разглашение или использование информации (ст. 191); дискредитация конкурента (ст. 192).

Уголовная ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ предусмотрены ст. 227 Уголовного кодекса Республики Казахстан[[26]](#footnote-26), которая расположена в разделе «Преступления в сфере экономической деятельности».

Аналогичным образом подходит к регулированию борьбы с преступлениями в сфере компьютерной информации Уголовный кодекс Республики Кыргызстан[[27]](#footnote-27). Кроме того, законодатель отразил особенности их совершения с использованием компьютерных информации и технологий, предусмотрев ответственность за: нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ч. 1 ст. 136); аналогичное деяние, совершенное с использованием специальных технических средств, предназначенных для негласного получения информации (ч. 2 ст. 136); незаконное производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации (ч. 3 ст. 136); нарушение авторских, смежных прав и прав патентообладателей путем выпуска под своим именем чужой программы для ЭВМ либо базы данных, либо иное присвоение авторства на такое произведение, а равно принуждение к соавторству (ч. 1 ст. 150); незаконное использование программы для ЭВМ или базы данных (ч. 2 ст. 150); незаконное получение сведений, составляющих коммерческую или банковскую тайну, путем перехвата информации в средствах связи, незаконного проникновения в компьютерную систему или сеть (ст. 193).

Уголовный кодекс Республики Туркменистан[[28]](#footnote-28) содержит гл. 33 «Преступления в сфере компьютерной информации», в которую включены: ст. 333 «Нарушение законодательства о правовой охране алгоритмов, программ для электронных вычислительных машин (ЭВМ), баз данных и топологий интегральных микросхем»; ст. 334 «Неправомерный доступ к компьютерной информации» и ст. 335 «Создание, использование и распространение вредоносных программ для ЭВМ», положения которых аналогичны ст. 272 и ст. 273 УК РФ.

Фактически соответствуют положениям ст. ст. 272 – 274 УК РФ нормы об уголовной ответственности за преступления в сфере компьютерной информации, содержащиеся в УК Азербайджанской Республики (ст. ст. 271 – 273)[[29]](#footnote-29) и УК Грузии[[30]](#footnote-30) (ст. ст. 284 – 286).

Уголовным кодексом Республики Молдова[[31]](#footnote-31), принятым 18 апреля 2002 года, преступления рассматриваемого вида сгруппированы в гл. XI «Преступления в сфере информатики», например ст. 259 «Несанкционированный доступ к компьютерной информации», то есть к информации, хранящейся в компьютерах, на машинных носителях, в компьютерной системе или сети, сопряженный с уничтожением, повреждением, модификацией, блокированием или копированием информации, нарушением работы компьютеров, компьютерных систем или сетей[[32]](#footnote-32).

Кроме того, в соответствии со ст. 260 УК Республики Молдова предусмотрена уголовная ответственность за: «внесение или распространение вредоносных компьютерных программ», которое законодатель определил как заведомое внесение в компьютерные программы вирусных модификаций либо распространение компьютерных программ или информации, выводящих из строя машинные носители информации, технические средства обработки данных или нарушающих систему защиты. А ст. 261 УК Республики Молдова предусмотрена уголовная ответственность за нарушение ответственным лицом правил сбора, обработки, хранения, распространения, распределения информации или правил защиты информационных систем, предусмотренных в соответствии с видом информации или степенью ее защиты, если это действие способствовало хищению, искажению, уничтожению информации или повлекло иные тяжкие последствия.

В соответствии с Уголовным кодексом Республики Армения[[33]](#footnote-33) (УК РА), принятом в апреле 2003 года, в гл. 24 «Преступление против безопасности компьютерной информации», размещенной в разделе 9 «Преступления против общественной безопасности, безопасности компьютерной информации, общественного порядка, общественной нравственности и здоровья населения», предусмотрено семь составов.

Так, в ст. 251 УК РА предусмотрена уголовная ответственность за несанкционированный доступ (проникновение) к системе компьютерной информации.

Кроме того, установлена уголовная ответственность за: изменение информации, хранящейся в компьютере, компьютерной системе, сети или на машинных носителях, либо внесение в них ложной информации при отсутствии признаков хищения чужого имущества, либо причинение имущественного ущерба путем обмана или злоупотребления доверием, повлекшие значительный ущерб; компьютерный саботаж – уничтожение, блокирование либо приведение в негодность компьютерной информации или программы, выведение из строя компьютерного оборудования либо повреждение компьютера, компьютерной системы, сети или машинных носителей; неправомерное завладение компьютерной информацией; за изготовление в целях сбыта или сбыт специальных программных или аппаратных средств для неправомерного доступа (проникновения) к защищенной информации; за разработку, использование и распространение вредоносных программ; за нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ (право на проникновение) к компьютеру, компьютерной системе или сети, если это деяние повлекло по неосторожности уничтожение, блокирование, изменение охраняемой законом компьютерной информации, нарушение работы компьютерного оборудования либо повлекло иной значительный ущерб.

Кроме того, в разделе 8 УК РА «Преступления против собственности, экономики и экономической деятельности» предусмотрено два состава, имеющих отношение к рассматриваемой проблеме. Так, в гл. 21 УК РА «Преступления против собственности», в соответствии со ст. 181 уголовно наказуемым является: хищение чужого имущества в значительных размерах, совершенное с использованием компьютерной техники.

В гл. 22 УК РА «Преступления против экономической деятельности» предусмотрена уголовная ответственность за собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа или угроз в отношении лиц, владеющих коммерческой или банковской тайной, их близких, прослушивания средств связи, незаконного проникновения в компьютерную или программную систему или сеть, использования специальных технических средств, а также иными незаконными способами в целях разглашения или использования этих сведений (ст. 199 УК РА).

В ст. 307 гл. 28 УК РА «Преступления против основ конституционного строя и безопасности государства» раздела 11 «Преступления против государственной власти» установлена уголовная ответственность за нарушение правил обращения с документами или компьютерной информацией, содержащими государственную тайну, а также с иными предметами, содержащими сведения о государственной тайне, лицом, обязанным соблюдать эти правила, если это повлекло по неосторожности утрату этих документов, или предметов, или компьютерной информации.

Как видно, родовой объект «компьютерных преступлений» в уголовном законодательстве стран СНГ различен[[34]](#footnote-34). Более того, уголовное законодательство стран СНГ по-разному оценивает степень общественной опасности преступлений в сфере компьютерной информации.

В Республике Беларусь и Таджикистане, где общественно опасные деяния объединены в главу «Преступления против информационной безопасности», законодатель установил в качестве родового объекта информационную безопасность, хотя преступления, посягающие на состояние защищенности жизненно важных интересов физических и юридических лиц в информационной сфере, содержатся и в других разделах и главах УК. В УК Украины родовой объект определен как отношения в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей и соответствующая глава называется «Преступления в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей».

В УК Грузии (глава «Компьютерные преступления») и Молдовы (глава «Преступления в сфере информатики») законодатель четко не определил родовой объект группы общественных отношений, подлежащих уголовно-правовой охране.

В УК Узбекистана (глава «Хищение чужого имущества») состав преступления «Нарушение правил информатизации» отнесен к преступлениям против собственности, а в УК Казахстана преступление в соответствии со ст. 227 относится к преступлениям в сфере экономической деятельности.

Проблема борьбы с компьютерными (информационными) преступлениями в настоящее время стоит перед многими государствами.

Многие европейские государства повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества.

Так, в 1993 году в Нидерландах был принят Закон о компьютерных преступлениях, дополняющий Уголовный кодекс[[35]](#footnote-35) новыми составами: несанкционированный доступ в компьютерные сети (ст. 138а (1)); несанкционированное копирование данных (ст. 138 (2)); компьютерный саботаж (ст. 350а (1), 350b (1)); распространение вирусов (ст. 350а (3), 350b); компьютерный шпионаж (ст. 273 (2)).

В ряд статей, предусматривающих ответственность за совершение традиционных преступлений (вымогательство (ст.ст. 317, 318); запись (прослушивание, копирование) информационных коммуникаций; кража путем обмана служб (ст. 362с)), были внесены дополнения, в редакции других (саботаж (ст.ст. 161, 351); подлог банковских карточек (ст. 232)) даны специальные разъяснения. Были значительно изменены такие составы, как шпионаж (ст.ст. 98, 98а); вмешательство в коммуникации (ст. 139а, 139b); порнография (ст. 240b).

Таким образом, уголовное законодательство Нидерландов предоставляет широкие возможности для борьбы с различными видами компьютерных преступлений.

В ФРГ с 1 января 1975 года действует новая редакция Уголовного кодекса 1871 года. С этого же времени началась дискуссия о целесообразности разработки уголовного законодательства, предусматривающего ответственность за действия, связанные с компьютерами.

В 1986 году в Уголовный кодекс было введено несколько новых поправок, содержащих описание компьютерных преступлений. В настоящее время УК ФРГ имеет 7 составов компьютерных преступлений. Предусмотрена уголовная ответственность для лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (ст. 202а).

Ответственности за компьютерное мошенничество (ст. 263а) подлежит лицо, оказавшее влияние на результаты процесса обработки информации путем неправильного оформления программ (манипуляцией с программным обеспечением), использования неправильных или неполных данных, а также посредством незаконного использования данных или воздействия на процесс обработки информации. Уголовно наказуемо изменение данных, имеющих доказательственное значение (ст. 269), а также фальсифицированное использование результатов переработки данных в правоприменительной деятельности (ст. 270).

УК ФРГ предусматривает наказание за уничтожение, повреждение технических записей, не принадлежащих виновному вообще или исключительно (ст. 274). Подлежит ответственности тот, кто неправомерно аннулирует, уничтожает, делает непригодными или изменяет данные (ст. 303а). Установлена уголовная ответственность за компьютерный саботаж (ст. 303b).

Среди уголовных кодексов европейских зарубежных государств особое внимание привлекают кодексы Испании[[36]](#footnote-36) и Франции[[37]](#footnote-37), недавно вступившие в силу. Кодекс Франции вступил в действие с весны 1994 года, а Испании в 1996 года.

Кодекс Франции включает составы большого числа компьютерных преступлений. Среди них посягательства на деятельность ЭВМ. Так, в главе 3 устанавливается ответственность за преступления, посягающие на системы автоматизированной обработки данных, такие как незаконный доступ к автоматизированной системе обработки данных или незаконное пребывание в ней (ст. 323-1); воспрепятствование работе или нарушение работы системы (ст. 323-2); ввод обманным путем в систему информации, а также изменение или уничтожение содержащихся в автоматизированной системе данных (ст. 323-3).

В УК Франции предусмотрена ответственность за посягательства, связанные с использованием картотек и обработкой данных на ЭВМ: осуществление или отдача указания об осуществлении автоматизированной обработки поименных данных без осуществления предусмотренных в законе формальностей (ст. 226-16); осуществление или отдача указания об осуществлении обработки этих данных без принятия всех мер предосторожностей, необходимых для того, чтобы обеспечить безопасность данных (ст. 226-17); сбор и обработка данных незаконным способом (ст. 226-18); ввод или хранение в памяти ЭВМ запрещенных законом данных (ст. 226-19); хранение определенных данных сверх установленного законом срока (ст. 226-20); использование данных с иной целью, чем это было предусмотрено (ст. 226-21); разглашение данных, могущее привести к указанным в законе последствиям (ст. 226-22).

Кроме того, Кодекс Франции предусматривает ответственность за действия, совершаемые с компьютерной информацией в ущерб интересам государства. Перечень данных составов преступлений также достаточно велик: сбор или передача содержащейся в памяти ЭВМ или картотеке информации иностранному государству, уничтожение, хищение, изъятие или копирование данных, носящих характер секретов национальной обороны, содержащихся в памяти ЭВМ или в картотеках, а также ознакомление с этими данными посторонних (ст.ст. 411-7, 411-8, 413-9, 413-10, 413-11).

В УК Испании, в отличие от УК Франции, нет специальных норм, предусматривающих ответственность за посягательство на компьютерную информацию, но она установлена за преступления, совершаемые с использованием информационных технологий: раскрытие и распространение тайных сведений (ст. 197); посягательство на интеллектуальную собственность (ст. 270) и коммерческую тайну (ст.278); подделка документов (ст. 394); изготовление и владение средствами (инструмент, материал, орудие, вещество, машина, компьютерная программа, аппарат), специально предназначенными для совершения преступлений, предусмотренных в предыдущих статьях (ст. 400); раскрытие и выдача тайны и информации, связанных с национальной обороной (ст.ст. 598, 599).

В Соединенных Штатах Америки компьютерная преступность появилась на рубеже 70-х годов. Именно с этого времени возник вопрос о том, в какой мере действующее уголовное законодательство обеспечивает потребности борьбы с компьютерными преступлениями. Американские исследователи пришли к выводу, что законодательство нуждается в новых законах, ориентированных на противодействие не известным ранее явлениям[[38]](#footnote-38).

В частности, в США возникла проблема уголовно-правовой оценки действий человека, который делает копию записи информации, а затем продает ее заинтересованным лицам. За что привлекать к ответственности в данном случае? Ведь кражи имущества в традиционном значении этого слова не происходило. Можно ли компьютерную программу считать «имуществом»? Как оценивать действия человека, который продает машинное время, стоимость которого представляется достаточно высокой? Поэтому не случайно в 1977 года в США появился законопроект о защите федеральных компьютерных систем.

Он предусматривал уголовную ответственность за следующие категории компьютерных преступлений: введение ложных данных в компьютерную систему; незаконное использование компьютерных устройств; внесение изменений в процессы обработки информации или нарушение этих процессов; кража денег, ценных бумаг, имущества, услуг, ценной информации, совершенная электронными или иными средствами. На основе данного законопроекта в 1984 году был принят соответствующий федеральный закон, который затем был дополнен в 1986 году.

В настоящее время в Соединенных Штатах преступления с использованием компьютера становятся все более обычным явлением вследствие всеобщей компьютеризации страны, хотя никто в точности не знает, сколько их совершается в действительности.

По приблизительным оценкам американских исследователей, ущерб от такого рода преступлений составляет миллиарды долларов ежегодно.

Общепринятого определения того, что надо понимать под компьютерным преступлением, в США нет. Каждый штат имеет свой закон, специально рассматривающий преступления, связанные с использованием компьютера. Причем некоторые штаты ограничиваются модификацией традиционных законов, например, предусматривая ответственность за хищения компьютерного времени или данных.

Американские исследователи, основываясь на анализе действующего законодательства, выделяют пять основных форм неправомерного поведения, связанного с использованием компьютеров, которые в той или иной формулировке представлены в законах штатов: неразрешенный доступ; неразрешенное использование; нечестная манипуляция или изменение данных; компьютерный саботаж; хищение информации[[39]](#footnote-39).

Данная классификация не лишена недостатков, которые отмечают и сами американские ученые. В частности, она не включает хищение элементов компьютерного оборудования, не предусматривает ситуации, когда компьютеры используются при совершении других преступлений и т.д.

Анализируя все изложенное в первой главе, можно сделать ряд выводов.

В конце восьмидесятых и начале девяностых годов прошлого столетия ответственность за компьютерные преступления была предусмотрена во многих государствах мира.

«Информационная революция» застала Россию в сложный экономический и политический период. Необходимость досрочной разработки правовых основ охраны информационных отношений, еще слабая развитость электронно-вычислительных систем, незначительное количество выявленных общественно опасных посягательств на эти отношения, отсутствие необходимого опыта привело к тому, что во вновь принятом в 1996 года Уголовном кодексе РФ в гл. 28 «Преступления в сфере компьютерной информации» содержалось три статьи, предусматривающие ответственность за «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). Названные в ст. 272 и 274 УК РФ деяния относятся к преступлениям небольшой тяжести, а эти же преступления, совершенные при отягчающих обстоятельствах, – к преступлениям средней тяжести.

В тот период времени эти нормы в минимальной степени удовлетворяли потребности правоприменительной практики. В настоящее время с компьютеризацией общества, переходом на расчеты финансовых и банковских структур с использованием электронно-вычислительных машин и в связи с транснациональным характером компьютерной преступности упомянутые нормы не могут обеспечить борьбу с компьютерными преступлениями. В них не учтено многообразие общественных отношений, на которые посягают названные преступления (это не только экономические интересы, но и государственная безопасность, конституционные права человека, его честь и достоинство т.д.).

Несмотря на новизну компьютерных преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает.

Проведенный анализ показал, что законодательство об уголовной ответственности за преступления в сфере компьютерной информации отличается определенным своеобразием; не во всех государствах бывшего Союза ССР законодательство в должной мере адаптировано к постоянно возрастающим потребностям усиления уголовно-правовой охраны правоотношений, связанных с использованием компьютерных информации и технологий. Многие европейские государства и США повели решительную борьбу с компьютерными преступлениями с момента их появления в жизни общества, следовательно, правовая регламентация уголовной ответственности за совершение компьютерных преступлений отличается очень высокой степенью детализации и высоким уровнем юридической техники.

Очевидно, что российскому законодателю следует оценить опыт зарубежных государств и выяснить пригодность вышеупомянутых правовых инструментов для защиты компьютерной информации.

# Глава 2 Характеристика составов преступлений в сфере компьютерной информации

# 2.1 Характеристика общих объективных и субъективных признаков преступлений в сфере компьютерной информации

Опасность компьютерных преступлений помимо того, что преступник, оставаясь «невидимым», может принести значительный ущерб, определяется еще и тем, что компьютер постепенно во всем мире заполняет все сферы жизнедеятельности человека, что позволяет преступникам значительно расширить свою экспансию. «Спектр преступного использования компьютеров практически равен спектру его применения по прямому назначению, а это означает, что преступное вторжение через ЭВТ может быть произведено в сферу космической и оборонной индустрии, политики и международных отношений и т.п.»[[40]](#footnote-40).

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 году компьютерные преступления определялись как «предусмотренные уголовным законом общественно опасные действия, в которых машинная информация является либо средством, либо объектом преступного посягательства»[[41]](#footnote-41). 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%[[42]](#footnote-42). 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.

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.[[43]](#footnote-43) Начиная с 80-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[[44]](#footnote-44). 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»)[[45]](#footnote-45).

Родовым объектом компьютерных преступлений является общественная безопасность.

Нормы раздела IX УК РФ предусматривают ответственность за посягательства на общественную безопасность.

В ст. 1 Закона РФ от 5 марта 1992 года № 2446-1 «О безопасности»[[46]](#footnote-46) дается понятие безопасности – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Жизненно важные интересы – совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства.

К основным объектам безопасности Закон относит: личность – ее права и свободы; общество – его материальные и духовные ценности; государство – его конституционный строй, суверенитет и территориальную целостность. В круг этих объектов Закон включает, кроме того, интересы в информационной, экологической сферах.

Выделяют различные виды безопасности: безопасность человечества, национальную, государственную, общественную, личную, экологическую, информационную безопасность, безопасность функционирования транспорта и иные виды (например, пожарную, радиационную, санитарную).

Уголовно-правовая охрана таких объектов общественной безопасности, как основы конституционного строя и безопасность государства, а также мир и безопасность человечества, от внешних и внутренних угроз, относится к иным разделам УК. В рассматриваемом же разделе УК берет под охрану личность (жизнь, здоровье, собственность, иные права и свободы); общество (его материальные и духовные ценности) от внешних угроз.

Безопасность как условие функционирования и развития общества имеет две составляющие, которые оцениваются по объективным и субъективным критериям. Объективный критерий – это уровень реальной защищенности системой законодательного регулирования, организационными мерами по использованию материальных средств, реализацией этих мер правоохранительными и другими органами. Субъективный критерий общественной безопасности как объекта уголовно-правовой охраны – часть общественной психологии, то есть общественное спокойствие, ощущение состояния защищенности, своей безопасности и безопасности других, неприкосновенности собственности, уверенность в нормальной работе государственных и общественных институтов.

В юридической литературе спорным является вопрос об объеме понятия общественной безопасности. Преступления против общественной безопасности причиняют физический, психический (моральный), материальный, организационный, социальный, политический, экологический вред гражданам, обществу, государству. Это не означает, что каждое преступление обязательно влечет все эти последствия одновременно. Для преступлений против общественной безопасности свойственна многообъектность посягательства (наличие основного и дополнительного непосредственных объектов посягательства). Одни ученые полагают, что основным объектом этих преступлений является общественная безопасность, а в качестве дополнительных могут быть жизнь, здоровье, собственность[[47]](#footnote-47), другие полагают, что единственным объектом здесь выступает общественная безопасность, поскольку без причинения вреда таким благам, как жизнь, здоровье людей, собственность и т.д., не может быть посягательства на общественную безопасность[[48]](#footnote-48).

Более убедительной представляется все-таки первая позиция.

Вся совокупность общественных отношений (предусмотренных нормами раздела IX УК), на которые посягает лицо, представляет понятие «общественная безопасность и общественный порядок» в широком смысле слова; нормы о преступлениях против общественной (общей) безопасности (предусмотренные гл. 24), о преступлениях против здоровья населения и общественной нравственности (гл. 25), экологических преступлениях (гл. 26), о преступлениях против безопасности движения и эксплуатации транспорта (гл. 27), о преступлениях в сфере компьютерной информации (гл. 28) – в узком смысле слова.

Общественная безопасность – это совокупность общественных отношений, регулирующих и обеспечивающих условия жизни общества, его материальные и духовные ценности.

Общественная опасность этой группы преступлений заключается в том, что они посягают на широкий круг общественных отношений, причиняют или могут причинить вред неопределенному кругу лиц, посягают на основы безопасности личности, общества и государства.

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. «На наш взгляд представляется, что относительно объекта преступного посягательства двух мнений быть не может – им, естественно, является информация, а действия преступника следует рассматривать как покушение на информационные отношения общества»[[49]](#footnote-49). Однако 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).

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[[50]](#footnote-50).

В доктрине информационной безопасности Российской Федерации, утвержденной Президентом РФ 9 сентября 2000 года[[51]](#footnote-51), это понятие определено уже как состояние защищенности национальных интересов Российской Федерации, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

«Современное общество использует четыре основных ресурса: природные богатства, труд, капитал и информацию»[[52]](#footnote-52).

Информация признается одним из прав граждан. Всеобщая декларация прав человека и гражданина, принятая Генеральной Ассамблеей ООН 10 декабря 1948 года[[53]](#footnote-53), 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.

На сегодняшний день новейшие информационные технологии, СМИ, многократно усилили возможности информационного воздействия на человека, население государства в целом. В результате информация превратилась в важнейший ресурс государства наряду с его другими основными ресурсами (природными, экономическими, трудовыми, материальными и т.д.).

Некоторые психологи утверждают, что человек разумный постепенно превращается в человека информационного. Наряду с традиционными методами управления обществом (административно-организационными, экономическими, социально-психологическими, правовыми) и отдельными личностями все большее распространение получает специальный метод централизованного воздействия на широкие слои населения – метод информационного управления.

В основе метода информационного управления лежит теория Антонио Грамши о том, что для достижения стратегических целей изменения общественного строя надо действовать меняя не базис общества, а через надстройку – силами интеллигенции, совершая молекулярную агрессию в сознание общества и разрушая его культурное ядро. Так, один из постулатов теории управления гласит, что эволюции в человеческом сознании достичь проще, чем совершить в нем революционные изменения[[54]](#footnote-54).

Информация в переводе с латинского information означает «ознакомление, разъяснение, изложение».

В философской литературе сложилась устойчивая традиция рассмотрения информации на основе философских категорий отражения и различия (разнообразия). Информация не существует без отражения, как и отражение без информации. Свойство отражения заключается в способности любого объекта воспроизводить некоторые особенности воздействующих на него объектов. Однако для определения понятия информации одной категории отражения недостаточно. Информация имеет место только там, где среди некоторого тождества существует определенное различие. Единицей измерения информации может считаться элементарное различие, то есть различие между двумя объектами в каком-либо одном фиксированном свойстве. Чем больше в совокупности отличных друг от друга элементов, тем больше эта совокупность содержит информации. Таким образом, информация в философии определяется как отраженное разнообразие, а именно разнообразие, которое отражающий объект содержит об отражаемом[[55]](#footnote-55).

Как отмечает Юрченко И. А., особенностью информации является то, что ее невозможно представить без какой-либо материальной основы, она является атрибутом (свойством) материи и неотделима от нее. Даже тогда, когда информация отражается сознанием человека, она существует лишь в единстве с определенными нейрофизиологическими процессами, то есть имеет свой материальный носитель[[56]](#footnote-56).

В конце 50-х годов один из основоположников кибернетики, Н. Виннер определил информацию как: «обозначение содержания, полученного из внешнего мира в процессе нашего приспособления к нему и приспособления к нему наших чувств. Процесс получения и использования информации является процессом нашего приспособления к случайностям внешней среды и нашей жизнедеятельности в этой среде»[[57]](#footnote-57). В данном определении ученый впервые затрагивает проблему неполноты получаемой индивидом информации, с одной стороны, а с другой, необходимость защиты сведений от «случайностей внешней среды».

Развитие информационных технологий заставляет интенсивно совершенствовать законодательную базу, вводит в юридическую сферу понятия, ранее применявшиеся в кибернетике и информатике.

Правовое понятие информации несколько уже, чем философское. В контексте Федерального закона «Об информации, информационных технологиях и защите информации»[[58]](#footnote-58) термин «информация» становится универсальным, он обозначает любые сведения о ком-либо или о чем-либо, получаемые из любого источника в любой форме: письменной, устной, визуальной и т.п. В данном определении сведения понимаются как реальные объекты социальной жизни: лица, предметы, факты, события, явления, процессы. Эти сведения могут служить и объектом познания, и ресурсом пополнения информационной базы: с одной стороны, сведения могут быть получены в результате исследования окружающей действительности и приобщены к уже существующей объективной системе знаний о мире, а с другой, быть объектом поиска, производимого конкретным потребителем для достижения его целей.

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. 5 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. 2 ст. 8 Федерального закона «Об информации, информационных технологиях 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.

Компьютерная информация – это информация в оперативной памяти ЭВМ, информация на иных машинных носителях как подключенных к ЭВМ, так и на съемных устройствах, включая дискеты, лазерные и иные диски. Цена дискеты не имеет никакого отношения к ценности информации, на ней записанной. Хищение дискеты (кроме грабежа и разбоя) влечет административную ответственность за мелкое хищение, что не исключает ответственности за неправомерный доступ к информации, на ней записанной, если виновный при этом умышленно приобретает доступ к информации на дискете.

Компьютерная информация в системе или сети ЭВМ не может существовать иначе как на конкретных ЭВМ, в эту систему или сеть объединенных. Поэтому, например, перехват информации при ее передаче по каналам связи будет неправомерным доступом к информации в ЭВМ, с которой она передается. Компьютерная информация в ЭВМ, в свою очередь, существует только в виде записей на машинных носителях.

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

Определяя слово «компьютер» следует исходить из употребления слов «ЭВМ», «компьютер» в естественном русском языке. Так, очевидно, не может рассматриваться в качестве компьютера калькулятор, и использование чужого калькулятора без разрешения его хозяина не является преступлением. Не будет компьютером и кассовый аппарат, в том числе и оборудованный электронным запоминающим устройством. В русском языке слова «ЭВМ», «компьютер» употребляются для обозначения «карманных компьютеров» (например, компьютеров для Windows CE, «ньютонов»), персональных компьютеров и компьютеров более высокого уровня. Компьютерами будут и электронные машины, являющиеся неотъемлемой частью какой-либо технической системы (бортовые компьютеры, компьютеры в автоматизированных производствах и т.п.).

Специалисты прибегают к разным критериям отграничения «компьютеров» от иных вычислительных устройств. Так, например, одни используют идеальную модель «машины Тьюринга» (минимальный набор функций – по этому критерию к компьютерам можно отнести и программируемый калькулятор), другие большее внимание уделяют интерфейсу и операционной системе, третьи вовсе отрицают принципиальное отличие компьютера от иных вычислительных устройств. В уголовном праве приемлем лишь лингвистический критерий[[59]](#footnote-59).

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.

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[[60]](#footnote-60). 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.

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 года 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. 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.

О важности определения места совершения преступления красноречиво говорит следующий пример. С июня по сентябрь 1994 года 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 года 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[[61]](#footnote-61).

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.

Среди основных мотивов компьютерных преступлений выделяют обычно два: корыстный и желание продемонстрировать собственный профессионализм – так называемый «интеллектуальный вызов»[[62]](#footnote-62).

# 2.2 Особенности характеристики неправомерного доступа к компьютерной информации

Неправомерный доступ к компьютерной информации (ст. 272 УК РФ). Данная статья предусматривает уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, то есть 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, а предметом – охраняемая законом компьютерная информация.

Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон «Об информации») определяет конфиденциальность информации как обязанность лица, получившего доступ к определенной информации, не передавать ее третьим лицам без согласия обладателя. В целом свойство конфиденциальности присуще информации, доступ к которой может получать строго определенный круг лиц, установленный ее владельцем. Если такая информация становится известна иным лицам, конфиденциальность утрачивается. Для определенных типов информации конфиденциальность является одним из наиболее важных атрибутов. Например, это относится к данным стратегических исследований, спецификации новых изделий и т.п. Особое значение выполнение требования о конфиденциальности приобретает при обработке в компьютерных системах информации, содержащей один из видов тайн (государственной, коммерческой, банковской, личной и других).

В соответствии со ст. 9 Закона «Об информации» ограничение доступа к ней устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства. Условия отнесения информации к сведениям, составляющим государственную, коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение устанавливаются соответствующими федеральными законами.

Очевидно, что высшую степень защиты от утечки из информационных компьютерных систем должны иметь сведения, отнесенные к государственной тайне[[63]](#footnote-63).

Иные виды защищаемой законом конфиденциальной информации, присутствие которой в подключенных к сети Интернет информационных системах вполне возможно, определяются Перечнем сведений конфиденциального характера, утвержденным Указом Президента РФ[[64]](#footnote-64). Сюда отнесены: сведения о фактах, событиях и обстоятельствах частной жизни гражданина (персональные данные); сведения, составляющие тайну следствия и судопроизводства; служебные сведения, доступ к которым ограничен органами государственной власти (служебная тайна); сведения, связанные с определенными видами профессиональной деятельности (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.); сведения, связанные с коммерческой деятельностью (коммерческая тайна); сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

В Уголовном кодексе РФ деяния, связанные с нарушением права собственника вычислительной системы на неприкосновенность информации в ней (в том числе на сохранение конфиденциальности), нашли отражение в ст. 272 «Неправомерный доступ к компьютерной информации». Понятие доступа к информации в Законе «Об информации» определено как возможность получения информации и ее использования. В сложившемся к настоящему моменту понимании контекста ст. 272 УК «неправомерный доступ» охватывает незаконное (самовольное, с нарушением установленных законом и обладателем информации требований) подключение к компьютерной системе (ее части) с последующим неуполномоченным воздействием на ее аппаратные средства, компоненты, сохраненные данные, проходящий через систему трафик[[65]](#footnote-65).

Последствия такого воздействия могут относиться не только к информации (уничтожение, блокирование, модификация, копирование), но и к программно-аппаратной части информационной системы (нарушение работы ЭВМ, системы ЭВМ или их сети). В этом отношении нельзя признать вполне удачным название ст. 272 УК. Исходя из ее диспозиции, правильнее было бы говорить о неправомерном воздействии на информационную систему. Это вполне согласуется и с введенным ст. 2 Закона «Об информации» понятием информационной системы, определяемой как «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

Что же касается неправомерного доступа к информации, то здесь стоит отметить следующее.

К охраняемой законом относится не вся информация в компьютерной системе, а лишь та, для которой законодателем установлен специальный режим правовой защиты, а обладателем приняты специальные меры защиты. Стоит уточнить, что в соответствии с Законом «Об информации» обладателем последней признается лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект РФ, муниципальное образование. Закон устанавливает, что обладатель информации, в частности, вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа, защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами. Одновременно Закон обязывает обладателя информации принимать меры по ее защите.

Выше уже упоминалось, что ст. 272 УК РФ устанавливает наказание за неправомерный доступ к охраняемой законом компьютерной информации при условии, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети. Такой перечень обязательных последствий вполне обоснован. На практике ему соответствует достаточно широкий круг противоправных деяний, направленных на нарушение целостности, доступности и конфиденциальности компьютерной информации. В то же время защиту конфиденциальной компьютерной информации ст. 272 УК, на наш взгляд, обеспечивает не в полной мере. С чем это связано?

Прежде всего, среди специалистов распространено мнение, что «сам по себе факт вызова или просмотра компьютерной информации, хранящейся на машинном носителе, состава анализируемого преступления не образует. Необходимо по крайней мере установить факт переноса указанной информации на другой машинный носитель»[[66]](#footnote-66). Действительно, если полученные следствием материалы не подтверждают факта уничтожения, блокирования, модификации или копирования компьютерной информации, то несанкционированное обладателем ознакомление с ней не может служить достаточным основанием к применению ст. 272 УК. Однако совершенно понятно, что на практике в большинстве случаев существенный ущерб обладателю конфиденциальной информации наносит уже само ознакомление с ней постороннего лица.

В рассматриваемом аспекте проблема юридической оценки мысленного восприятия информации лицом, осуществляющим неправомерный доступ к ней без ее копирования на машинные носители, является достаточно сложной. По замечанию В. В. Крылова, «если придерживаться понимания термина копирования только как процесса изготовления копии документированной информации в виде физически осязаемого объекта, то все случаи, не связанные с копированием, но приводящие к ознакомлению с информацией независимо от того, какой режим использования информации установил ее собственник, не являются противоправными»[[67]](#footnote-67). С другой стороны, с учетом технологических особенностей передачи информации в компьютерных сетях (в том числе в Интернете) уже с момента несанкционированного подключения к удаленной системе из нее, строго говоря, происходит копирование информации, так как передаче данных по сети сопутствует перенос их в оперативную память принимающего информацию компьютера. Это обстоятельство учитывалось в отечественной судебной практике. Однако распространение получил подход, при котором лицу, получившему доступ к компьютерной информации, не может быть поставлено в вину ее копирование, обусловленное не зависящим от его воли («автоматическим») действием программных средств.

В данном случае мы наблюдаем явное противоречие между содержанием и результатом действий по получению доступа к информации и содержанием нормы закона, по которой эти действия оцениваются. Субъект осуществил неправомерный доступ к конфиденциальной информации, ознакомился с ней (тем самым уже нанес ущерб потерпевшему), в его компьютере обнаружены копии с просмотренных данных. Однако предъявление ему обвинения в преступлении, предусмотренном ст. 272 УК, не представляется возможным, поскольку копии сохранялись системой автоматически без участия подозреваемого. При этом не учитывается позиция некоторых исследователей о «существовании исключительного специфического носителя охраняемых информационных ресурсов – человека, его памяти»[[68]](#footnote-68) и то обстоятельство, что в ряде случаев с запечатленной в памяти информации может быть впоследствии изготовлена копия, в том числе и на машинном носителе.

Указанную неоднозначность, на наш взгляд, все же следует устранить путем уточнения диспозиции ст. 272 УК, включив в состав данного преступления необходимых альтернативных последствий неправомерного доступа к компьютерной информации и «несанкционированное обладателем ознакомление лица с информацией ограниченного доступа».

Согласно судебной практике, наиболее распространена ситуация, когда неправомерный доступ к информации осуществляется неуполномоченным субъектом с использованием реквизитов доступа (имя, пароль), принадлежащих законным пользователям информационной системы. В этом случае при решении вопроса о квалификации преступления по ст. 272 УК РФ требуется установить обстоятельства получения таких реквизитов. Нередко эти сведения становятся практически общедоступными в результате беспечности их владельца, который добровольно сообщает их третьим лицам.

Получение не только реквизитов доступа, но и значительных объемов конфиденциальной информации часто связано с применением «шпионских программ» (например, программы типа «троянский конь»). Действия по установке на компьютерах системы вредоносных программ дают основания для дополнительной их квалификации по ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ».

Объективная сторона этого преступления, наряду с иными альтернативными действиями (создание вредоносных программ, их распространение, внесение изменений в существующие программы), характеризуется использованием вредоносных программ, которое в рассматриваемой ситуации выражается в несанкционированном размещении программы в компьютерной системе. Кроме того, состав ст. 273 УК РФ сконструирован как формальный и преступление признается оконченным с момента совершения указанных действий (внедрения программы в систему) независимо от наступивших последствий. В то же время последствия могут наступить в виде передачи скопированной конфиденциальной информации по каналам сети Интернет на заданный адрес электронной почты. Поскольку неправомерное копирование информации при этом осуществляется в автоматическом режиме, здесь опять возникает вопрос о допустимости вменения ст. 272 УК.

Представляется, что в данном случае ответ на него должен быть положительным, если будет установлено, что внедрение вредоносной программы преследовало цель неправомерного получения информации.

К этому стоит добавить, что вредоносные программы указанного типа имеются в свободном доступе в Интернете и часть из них может попасть в компьютер потерпевшего опять-таки в результате его самостоятельных и беспечных с точки зрения компьютерной безопасности действий (например, при копировании программ из сети Интернет, просмотре подозрительных вложений в сообщения электронной почты, использовании систем обмена файлами, посещении сайтов сомнительного содержания и т.п.). Установление источника появления программ в компьютерной системе потерпевшего чаще всего представляет серьезную проблему для следствия.

Достаточно часто неправомерный доступ к конфиденциальной компьютерной информации с использованием сети Интернет предпринимается при подготовке к совершению иного преступления. Например, взлом информационной системы интернет-магазина может выполняться для размещения в системе магазина фальсифицированного заказа с целью мошенничества (ст. 159 УК). Нередко получение несанкционированного доступа к компьютерным системам крупных компаний сопровождается попытками вымогательства у них крупных денежных средств под угрозой разглашения незаконно полученных конфиденциальных сведений (ст. 163 УК).

В качестве примера можно упомянуть деятельность российских граждан А. Иванова и В. Горшкова, осуществивших в 2001 году взлом компьютерных систем нескольких международных компаний (в частности Western Union и PayPal). Преступники похитили номера около 16 тыс. кредитных карт и пытались вымогать значительные денежные средства, однако были задержаны ФБР США[[69]](#footnote-69).

При рассмотрении неправомерного доступа к информации в сети Интернет нельзя не учитывать статьи УК, направленные в основном на защиту конкретных видов конфиденциальной информации. Проникновение в компьютерные системы и перехват электронной корреспонденции могут выступать в качестве одной из стадий совершения таких преступлений, как нарушение неприкосновенности частной жизни (ст. 137 УК), нарушение тайны переписки (ст. 138 УК), незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК). Такие преступления, совершаемые с использованием сети Интернет, в последнее время часто называют «компьютерным шпионажем».

За незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, предусмотрена уголовная ответственность (ст. 137 УК). При этом собирание предусматривает любые действия, направленные на приобретение указанных сведений, в том числе и доступ к компьютерной информации потерпевшего лица, содержащей конфиденциальные данные о его личных связях, состоянии здоровья, фактах из жизни, привычках, наклонностях, интересах, интимных отношениях и т.п.[[70]](#footnote-70)

Часть таких сведений может быть отнесена и к иным видам тайн (врачебная, нотариальная, адвокатская и др.). Незаконность собирания сведений о частной жизни связывается с отсутствием согласия потерпевшего и использованием запрещенных законом методов и средств (в рассматриваемом случае – неправомерного доступа к компьютерной информации). Стоит учитывать, что потерпевшими по указанному в них составу преступления могут быть только физические лица. Защита прав на неприкосновенность частной жизни, личную и семейную тайну также определена в качестве цели нового Федерального закона «О персональных данных», регламентирующего принципы и условия сбора и обработки персональных данных, в том числе с использованием информационных систем[[71]](#footnote-71). Не все из положений данного Закона представляются абсолютно бесспорными, и время покажет, насколько же они соответствуют потребностям практики.

Уголовная ответственность предусмотрена и за действия, в результате которых нарушается тайна сообщений, передаваемых с использованием каналов сети Интернет (ст. 138 УК). Неправомерность таких действий возникает в случае, если они производятся без согласия владельца информации, без решения суда или наличия иных правовых оснований. Сюда, в частности, может быть отнесен неправомерный доступ к содержимому электронной почты, в результате которого содержание посланий становится известным виновному лицу. В определенных ситуациях нарушение тайны электронной корреспонденции может сочетаться с собиранием сведений о частной жизни граждан, что вызывает необходимость квалификации содеянного по совокупности составов преступлений, предусмотренных ст. 137, 138, 272 УК РФ.

Неправомерный доступ к компьютерной информации может осуществляться с целью получения сведений, составляющих коммерческую, налоговую или банковскую тайну, и тем самым подпадать под действие ст. 183 УК РФ. Данная статья, в частности, устанавливает уголовную ответственность за собирание указанных сведений незаконным способом. Здесь важно установить, осуществлялось ли получение информации с умышленным преодолением принятых обладателем мер по охране ее конфиденциальности и знало ли получающее эту информацию лицо (или имело достаточные основания полагать), что эта информация составляет указанные виды тайн. Понятие коммерческой тайны дано в Федеральном законе «О коммерческой тайне»[[72]](#footnote-72) и ст. 139 Гражданского кодекса РФ.

Закон «О коммерческой тайне» (ст. 3) связывает коммерческую тайну с конфиденциальностью информации, позволяющей ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду. При этом к информации, составляющей коммерческую тайну, отнесена научно-техническая, технологическая, производственная, финансово-экономическая или иная информация, которая имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к которой нет свободного доступа на законном основании и в отношении которой обладателем такой информации введен режим коммерческой тайны. В части 1 ст. 4 Закона «О коммерческой тайне» устанавливается право обладателя информации на отнесение ее к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации.

В рассматриваемой ситуации важно учитывать, что информация, составляющая коммерческую тайну, считается полученной незаконно, если доступ к ней осуществлялся с умышленным преодолением принятых ее обладателем мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо. Права на коммерческую тайну действуют, пока соблюдаются условия ее защиты.

По общему правилу степень защиты конфиденциальной информации должна соответствовать уровню ее ценности для обладателя. Перечень обязательных мер по охране конфиденциальности информации, принимаемых ее обладателем (ст. 10 Закона «О коммерческой тайне»), в частности, включает: ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за его соблюдением. При этом меры по охране конфиденциальности коммерческой тайны признаются разумно достаточными, если исключается доступ к коммерческой тайне любых лиц без согласия ее обладателя. Необходимо подчеркнуть, что обладатель компьютерной информации должен принимать не только организационные и юридические меры к охране конфиденциальности информации, но и специальные технические, затрудняющие доступ третьих лиц к ней в компьютерной системе.

Как видно из анализа данного преступления, часто осуществление неправомерного доступа к компьютерной информации выступает лишь способом совершения других преступлений, что, несомненно, приводит к выводу о возможном включении в качестве квалифицирующего признака «при помощи компьютерных средств» в диспозиции ряда статей УК РФ – например, ст. 137, 138, 183.

# 2.3 Особенности характеристики создания, использования и распространения вредоносных программ для ЭВМ

Ст. 273 УК РФ предусматривает ответственность за создание, использование или распространение вредоносных программ для ЭВМ, то есть Создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

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[[73]](#footnote-73).

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.

Вопрос о том, как определить, является ли программа вредоносной, очень сложный, особенно для неспециалиста. Вредоносных для ЭВМ программ существует очень много.

Так, к вредоносному программному обеспечению относятся сетевые черви, классические файловые вирусы, троянские программы, хакерские утилиты и прочие программы, наносящие заведомый вред компьютеру, на котором они запускаются на выполнение, или другим компьютерам в сети.

«Сетевые черви»

К данной категории относятся программы, распространяющие свои копии по локальным и/или глобальным сетям с целью:

* проникновения на удаленные компьютеры;
* запуска своей копии на удаленном компьютере;
* дальнейшего распространения на другие компьютеры в сети.

Для своего распространения сетевые черви используют разнообразные компьютерные и мобильные сети: электронную почту, системы обмена мгновенными сообщениями, файлообменные (P2P) и IRC-сети, LAN, сети обмена данными между мобильными устройствами (телефонами, карманными компьютерами) и т. д.

Большинство известных червей распространяется в виде файлов: вложение в электронное письмо, ссылка на зараженный файл на каком-либо веб- или FTP-ресурсе в ICQ– и IRC-сообщениях, файл в каталоге обмена P2P и т. д.

Некоторые черви (так называемые «бесфайловые» или «пакетные» черви) распространяются в виде сетевых пакетов, проникают непосредственно в память компьютера и активизируют свой код.

Для проникновения на удаленные компьютеры и запуска своей копии черви используют различные методы: социальный инжиниринг (например, текст электронного письма, призывающий открыть вложенный файл), недочеты в конфигурации сети (например, копирование на диск, открытый на полный доступ), ошибки в службах безопасности операционных систем и приложений.

Некоторые черви обладают также свойствами других разновидностей вредоносного программного обеспечения. Например, некоторые черви содержат троянские функции или способны заражать выполняемые файлы на локальном диске, то есть имеют свойство троянской программы и/или компьютерного вируса.

«Классические компьютерные вирусы»

К данной категории относятся программы, распространяющие свои копии по ресурсам локального компьютера с целью:

* последующего запуска своего кода при каких-либо действиях пользователя;
* дальнейшего внедрения в другие ресурсы компьютера.

В отличие от червей, вирусы не используют сетевых сервисов для проникновения на другие компьютеры. Копия вируса попадает на удаленные компьютеры только в том случае, если зараженный объект по каким-либо не зависящим от функционала вируса причинам оказывается активизированным на другом компьютере, например:

* при заражении доступных дисков вирус проник в файлы, расположенные на сетевом ресурсе;
* вирус скопировал себя на съемный носитель или заразил файлы на нем;
* пользователь отослал электронное письмо с зараженным вложением.

Некоторые вирусы содержат в себе свойства других разновидностей вредоносного программного обеспечения, например бэкдор-процедуру или троянскую компоненту уничтожения информации на диске.

«Троянские программы»

В данную категорию входят программы, осуществляющие различные несанкционированные пользователем действия: сбор информации и ее передачу злоумышленнику, ее разрушение или злонамеренную модификацию, нарушение работоспособности компьютера, использование ресурсов компьютера в неблаговидных целях.

Отдельные категории троянских программ наносят ущерб удаленным компьютерам и сетям, не нарушая работоспособность зараженного компьютера (например, троянские программы, разработанные для массированных DoS-атак на удалённые ресурсы сети).

«Хакерские утилиты и прочие вредоносные программы»

К данной категории относятся:

* утилиты автоматизации создания вирусов, червей и троянских программ (конструкторы);
* программные библиотеки, разработанные для создания вредоносного программного обеспечения;
* хакерские утилиты скрытия кода зараженных файлов от антивирусной проверки (шифровальщики файлов);
* «злые шутки», затрудняющие работу с компьютером;
* программы, сообщающие пользователю заведомо ложную информацию о своих действиях в системе;
* прочие программы, тем или иным способом намеренно наносящие прямой или косвенный ущерб данному или удалённым компьютерам[[74]](#footnote-74).

Цели использования компьютерных вредоносных программ

«Мелкое воровство»

С появлением и популяризацией платных Интернет-сервисов (почта, WWW, хостинг) компьютерный андеграунд начинает проявлять повышенный интерес к получению доступа в сеть за чужой счет, то есть посредством кражи чьего-либо логина и пароля (или нескольких логинов/паролей с различных пораженных компьютеров) путем применения специально разработанных троянских программ.

В начале 1997 года зафиксированы первые случаи создания и распространения троянских программ, ворующих пароли доступа к системе AOL.

В 1998 году, с распространением Интернет-услуг в Европе и России, аналогичные троянские программы появляются и для других Интернет-сервисов. До сих пор троянцы, ворующие пароли к dial-up, пароли к AOL, коды доступа к другим сервисам, составляют заметную часть ежедневных «поступлений» в лаборатории антивирусных компаний всего мира.

Троянские программы данного типа, как и вирусы, обычно создаются молодыми людьми, у которых нет средств для оплаты Интернет-услуг. Характерен тот факт, что по мере удешевления Интернет-сервисов уменьшается и удельное количество таких троянских программ.

«Мелкими воришками» также создаются троянские программы других типов: ворующие регистрационные данные и ключевые файлы различных программных продуктов (часто – сетевых игр), использующие ресурсы зараженных компьютеров в интересах своего «хозяина» и т. п.

## «Криминальный бизнес»

Наиболее опасную категорию вирусописателей составляют хакеры-одиночки или группы хакеров, которые осознанно или неосознанно создают вредоносные программы с единственной целью: получить чужие деньги (рекламируя что-либо или просто воруя их), ресурсы зараженного компьютера (опять-таки, ради денег – для обслуживания спам-бизнеса или организации DoS-атак с целью дальнейшего шантажа).

Обслуживание рекламного и спам-бизнеса – один из основных видов деятельности таких хакеров. Для рассылки спама ими создаются специализированные троянские proxy-сервера, которые затем внедряются в десятки тысяч компьютеров. Затем такая сеть «зомби-машин» поступает на черный Интернет-рынок, где приобретается спамерами. Для внедрения в операционную систему и дальнейшего обновления принудительной рекламы создаются утилиты, использующие откровенно хакерские методы: незаметную инсталляцию в систему, разнообразные маскировки (чтобы затруднить удаление рекламного софта), противодействие антивирусным программам.

Вторым видом деятельности подобных вирусописателей является создание, распространение и обслуживание троянских программ-шпионов, направленных на воровство денежных средств с персональных (а если повезет – то и с корпоративных) «электронных кошельков» или с обслуживаемых через Интернет банковских счетов.

Троянские программы данного типа собирают информацию о кодах доступа к счетам и пересылают ее своему «хозяину».

Третьим видом криминальной деятельности этой группы является Интернет-рэкет, то есть организация массированной DoS-атаки на один или несколько Интернет-ресурсов с последующим требованием денежного вознаграждения за прекращение атаки. Обычно под удар попадают Интернет-магазины, букмекерские конторы – то есть компании, бизнес которых напрямую зависит от работоспособности веб-сайта компании.

Вирусы, созданные этой категорией «писателей», становятся причиной многочисленных вирусных эпидемий, инициированных для массового распространения и установки описанных выше троянских компонент.

## «Нежелательное программное обеспечение»

Системы навязывания электронной рекламы, различные «звонилки» на платные телефонные номера, утилиты, периодически предлагающие пользователю посетить те или иные платные веб-ресурсы, прочие типы нежелательного программного обеспечения – они также требуют технической поддержки со стороны программистов-хакеров. Данная поддержка требуется для реализации механизмов скрытного внедрения в систему, периодического обновления своих компонент и противодействия антивирусным программам.

Очевидно, что для решения данных задач в большинстве случаев также используется труд хакеров, поскольку перечисленные задачи практически совпадают с функционалом троянских программ различных типов.

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 (см. соответствующие положения к ст. 272 УК). 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, то есть разработка компьютерных программ, основанных на оригинальных, новых алгоритмах, изобретенных и реализованных разработчиком;
* внесение изменений в существующие программы, то есть 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, то есть выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот;
* распространение, то есть 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»).

Использование вредоносных программ в глобальных сетях

Глобализация общественных процессов, характерная для современного этапа развития общества и тесно связанная с совершенствованием информационных технологий, привела к глобализации коммуникационных систем. Единое мировое информационное пространство стало вполне ощутимой реальностью. В последние годы происходит стремительный рост числа пользователей глобальными сетями, прежде всего Интернетом. В настоящее время также можно отметить интенсивное увеличение российского сегмента глобальной информационной сети Интернет как в количественном (число операторов и пользователей), так и в качественном (расширение круга оказываемых услуг) отношении.

В 2002 году в России была принята Федеральная целевая программа «Электронная Россия (2002 – 2010 годы)», одной из основных задач которой является развитие телекоммуникационной инфраструктуры и создание новых пунктов подключения к открытым информационным системам для расширения присутствия России в сети Интернет[[75]](#footnote-75). В связи с началом реализации Федеральной программы «Электронная Россия» в нашей стране прогнозируется восьмикратное увеличение числа пользователей сетью к концу 2005 года.

Сегодня стало совершенно очевидным, что расширение всемирной паутины и возрастание объема и качества доступных ресурсов сопровождаются соответствующим ростом различных злоупотреблений. В условиях широкого распространения интернет-технологий в экономической и иной деятельности преступность в виртуальной сфере представляет достаточно серьезную угрозу.

Интернет все более активно используется преступниками для незаконного проникновения в корпоративные и личные базы данных, а также в качестве пособий по приготовлению к террористическим акциям, рекомендаций относительно того, как уйти от уголовного преследования, для пропаганды национальной вражды и призывов к развязыванию войны.

Одним из наиболее распространенных сетевых преступлений, направленных на нарушение нормального функционирования объектов глобальных компьютерных сетей, является создание, использование и распространение вредоносных программ для ЭВМ. В статье 273 УК РФ, а также в Соглашении о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации было закреплено, что под вредоносной программой для ЭВМ понимается созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

Вредоносные программы (троянские программы, компьютерные вирусы, компьютерные черви, программные закладки) получили в глобальных компьютерных сетях очень широкое распространение. Некоторые из них, выходя из-под контроля создателей, могут неуправляемо наносить существенный вред. Здесь можно вспомнить нашумевший в свое время случай с вирусом, созданным Робертом Т. Морисом, студентом первого курса университета в Корнелле. Проверяя возможность копирования программ с компьютера на компьютер в сети ARPANET, студент вывел из строя 6200 компьютеров США, так как из-за сбоя в алгоритме скорость размножения вируса стала гигантской. При этом вирус поразил компьютеры секретной военной сети MILNET, хотя эксперимент проводился в ARPANET. Соединение этих двух сетей держалось в секрете и потому стало полной неожиданностью для американского студента[[76]](#footnote-76). А, например, вирус «Мелисса» в 1999 году независимо от воли создателя инфицировал программы более 1 млн. компьютеров, подключенных к Интернету[[77]](#footnote-77).

Особое место среди вредоносных программ занимают компьютерные вирусы, вредоносные программы для ЭВМ, способные к самораспространению путем включения своего программного кода или некоторой его части в программный код файлов, системные области или иное рабочее пространство машинных носителей информации с сохранением всех первоначальных свойств или некоторой их части[[78]](#footnote-78).

Цели, с которыми распространяются в глобальных сетях компьютерные вирусы, могут быть самыми различными – от хулиганских до политических. В последнее время довольно часто подобные действия совершаются по идеологическим мотивам. Для обозначения этого явления в западных средствах массовой информации применяется такое понятие, как «хактивизм». В качестве примера можно привести случай, когда во время Косовского конфликта коммерческие структуры, общественные организации, академические институты получали из некоторых европейских стран электронную почту с вирусами. Эти сообщения политической направленности, написанные на плохом английском, содержали обвинения НАТО в несправедливой агрессии и призывы к защите прав сербов, а также пропагандистские мультфильмы. Ущерб адресату таких писем причинялся несколькими вирусами, содержащимися во вложении (например, в антинатовском мультфильме).

Сегодня количество известных вирусов не поддается строгому учету и постоянно увеличивается. По приблизительным оценкам специалистов, ведущих борьбу с вредоносными программами, в среднем ежедневно появляется около 30 новых вирусов. Еще в 1987 году специалисты доказали невозможность разработки алгоритма, способного обнаружить все возможные вирусы. Исследования компании IBM показали, что возможно создание вирусов, выявление которых будет затруднено даже при наличии образца вируса[[79]](#footnote-79).

Еще одной проблемой являются сложности, возникающие при оценке ущерба, наносимого вирусами. Это связано с необходимостью анализа большого количества показателей, трудно поддающихся учету. Основные издержки связаны с простоями вычислительной техники, очисткой ее от зараженных файлов, восстановлением информации, внедрением нового защитного программного обеспечения, ухудшением репутации пострадавших фирм.

Один из наиболее известных производителей антивирусного программного обеспечения компания McAfee в своем отчете пришла к выводу, что ситуация с вирусами будет ухудшаться в связи с постоянным увеличением их числа, усложнением применяемых при их создании алгоритмов, изменением механизмов распространения, расширением глубины проникновения в системы и, как следствие, нарастанием масштабов причиняемого вреда[[80]](#footnote-80).

Некоторые авторы относятся к таким программам как к информационному оружию, для которого характерны универсальность, радикальность воздействия, доступность, широкие возможности места и времени применения, высокая эффективность на значительных расстояниях, скрытность использования[[81]](#footnote-81).

Относительно характера субъективной стороны анализируемого преступления в специальной литературе высказываются различные мнения. Так, большинство авторов считает, что данное преступление возможно только с прямым умыслом[[82]](#footnote-82). 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»[[83]](#footnote-83). 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 (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.

Субъект преступления – общий, то есть вменяемое, достигшее 16-летия, физическое лицо.

Таким образом, можно сделать вывод, что создание вредоносных программ для ЭВМ, также может выступать способом совершения целого ряда преступлений – и мошенничества, и присвоения и растраты, и причинения имущественного ущерба путем обмана или злоупотребления доверием, и умышленного повреждения имущества, и незаконного распространения порнографии и т.д., что также, как и в случае с преступлением, предусмотренным ст. 272 УК РФ, ставит вопрос или о дополнении диспозиций указанных составов преступлений квалифицирующим признаком «при помощи компьютерных средств», или о выделении ряда самостоятельных преступлений.

# 2.4 Особенности характеристики нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети

Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст. 274 УК). Это преступление представляет собой невыполнение либо ненадлежащее выполнение обязательных предписаний по эксплуатации и использованию электронно-вычислительной техники, установленных государством в виде ведомственных нормативных актов, отдельными юридическими лицами, являющимися собственниками или законными владельцами информационных ресурсов или электронно-вычислительной техники, сетей или комплексов ЭВТ. Данная норма – бланкетная. Поэтому для правильного определения объективной стороны состава необходимо установление конкретного нормативного или иного акта, обязательные предписания которого нарушил виновный. Речь идет о выявлении нарушения императивных положений правил, запрещающих совершение соответствующих действий либо обязывающих лицо поступать строго определенным образом. При невыполнении рекомендательных норм речь не может идти об уголовной ответственности.

С объективной стороны преступление характеризуется как активными действиями, так и бездействием, сопряженными с нарушением установленных правил. Конкретное содержание этих правил pаскpывается в нормативных актах иных отраслей права (законах, правилах, инструкциях и т.д.). Эти правила могут быть предусмотрены в общих требованиях по технике безопасности и эксплуатации компьютерного оборудования либо в специальных правилах, pегламентиpующих особые условия (продолжительность времени, последовательность операций, максимальные нагрузки и т.д.). Во втором случае соответствующие правила устанавливаются производителями этих технических средств в инструкциях по работе с ЭВМ, их периферийными устройствами и машинными носителями и поставляются вместе с ними. Работа данных устройств рассчитана на определенные параметры, соблюдение которых обязательно. порядок пользования ЭВМ, системой ЭВМ и сетью ЭВМ в конкретных условиях может устанавливаться собственником или владельцем технических устройств.

Нарушение правил эксплуатации может выражаться в несоблюдении, ненадлежащем соблюдении, в прямом нарушении установленных правил, обеспечивающих безопасность эксплуатации ЭВМ, системы ЭВМ или их сети.

Состав преступления сформулирован как материальный. Для признания преступления оконченным необходимо наступление одного из последствий, перечисленных в ст. 274 УК. К таковым, в частности, относятся: уничтожение, блокирование или модификация охраняемой законом информации ЭВМ. При этом последние должны повлечь причинение существенного вреда. Понятие «существенный вред» является оценочным, и в каждом случае зависит от конкретных обстоятельств дела. В первую очередь он определяется ценностью и значимостью охраняемой информации, уничтожение, блокирование либо модификация которой произошла. Существенный вред будет также наличествовать при экономических (материальных) потерях государства, организаций и граждан, остановках производственных процессов и т.п. Однако эти последствия не должны быть тяжкими, в противном случае речь должна идти о квалифицированном составе, предусмотренном ч. 2 данной статьи.

С субъективной стороны в данном составе возможна вина в форме умысла и неосторожности, что соответствует содержанию ст. 24 УК РФ.

Субъект преступления специальный – физическое вменяемое лицо, достигшее 16 лет и имеющее доступ к системе ЭВМ или их сети.

Квалифицированный состав преступления предусмотрен в ч. 2 ст. 274 УК. Для него характерно наступление тяжких последствий, причиненных по неосторожности. В данном случае преступление может совершаться только по неосторожности.

Анализируя систему компьютерных преступлений (ст. 272-274 УК РФ) в целом, можно сделать вывод, что уголовный кодекс РФ помимо описанных выше составов, предметом которых является компьютерная информация, не содержит в других главах специальных или квалифицированных составов, связанных с использованием компьютерных технологий. 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 в вышеупомянутой монографии даже не упоминает о нормах гл. 28 УК. Автор последовательно[[84]](#footnote-84) 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. По этому же пути идет и судебная практика, которая, правда, весьма скудна. 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»[[85]](#footnote-85). 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. На наш взгляд, именно она представляется предпочтительной. Да, при хищении безналичных денег с помощью компьютера последний является только средством, однако средством не простым – его нельзя приравнять к «фомке» или топору. 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. Более того, в соответствии со ст. 20 УПК РФ ч. 1 ст. 146 УК является делом частно-публичного обвинения. 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.

В связи с этим представляется целесообразным дополнить диспозиции ряда статей УК РФ, например, следующим образом:

«Статья 165. Причинение имущественного ущерба путем обмана, злоупотребления доверием или модификации охраняемой законом компьютерной информации

1. Причинение имущественного ущерба собственнику или иному владельцу имущества путем обмана или злоупотребления доверием либо путем модификации охраняемой законом компьютерной информации, при отсутствии признаков хищения или иного завладения чужим имуществом – наказывается...».

«Статья 183. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну

1. Собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, путем перехвата в средствах связи, незаконного доступа к охраняемой законом компьютерной информации, использования специальных технических средств, а равно иным незаконным способом – наказывается...».

Таким образом, анализируя все изложенное во второй главе настоящего дипломного исследования, можно сделать ряд выводов.

Недооценка общественной опасности посягательств на интересы, охраняемые гл. 28 УК РФ, в сочетании с конструктивными недостатками диспозиций этих уголовно-правовых норм, а также недостаточным уровнем подготовки правоприменительных органов, призванных вести борьбу с компьютерными преступлениями, привели к тому, что уголовно-правовые нормы, предусматривающие ответственность за названные преступления, применяются очень редко.

Сложившееся положение объясняется рядом причин, среди которых в первую очередь представляется необходимым выделить:

а) недостаточную разработанность теоретической модели компьютерных преступлений;

б) недостаточную изученность криминологической характеристики компьютерных преступлений и в этой связи неразработанность более совершенных методик по раскрытию и расследованию преступлений, комплекса мер предупредительного характера и рекомендаций по виктимологической профилактике.

Необходимость разработки новой системы компьютерных преступлений возникает еще и потому, что в ст. 272 – 274 УК РФ совершенно не учтены общественно опасные последствия неправомерного доступа в чужую компьютерную информацию.

Если в результате преступления причиняется ущерб, содеянное квалифицируется по статьям о преступлениях против собственности.

Представляется, что уголовно-правовые нормы об ответственности за преступления, совершенные с использованием высоких технологий, лицами, обладающими большим интеллектуальным потенциалом, влекущие тяжелые последствия, должны предусматривать более строгое наказание, чем обычные преступления против собственности. При построении системы компьютерных преступлений следует учесть опыт зарубежных государств, где компьютерная преступность оказалась более распространенной и нанесла более серьезный ущерб.

С учетом распространенности отдельных видов преступлений, совершаемых с использованием компьютерной информации, система компьютерных преступлений может быть построена следующим образом.

А. Преступления против личности:

* компьютерная клевета;
* компьютерное вторжение в частную жизнь;
* нарушение тайны электронной корреспонденции.

Б. Преступления в сфере экономики:

* компьютерное хищение;
* компьютерный экономический шпионаж;
* кража компьютерных услуг;
* торговля компьютерными паролями.

В. Преступления против общественной безопасности, общественного порядка и общественной нравственности:

* неправомерный доступ к компьютерной информации;
* кибертерроризм;
* создание, использование и распространение вредоносных программ для ЭВМ;
* компьютерное хулиганство;
* компьютерная порнография.

Г. Преступления против государственной безопасности: компьютерный шпионаж.

Представляется, что построение такой системы приведет к более удачной борьбе с компьютерными преступлениями.

# ЗАКЛЮЧЕНИЕ

В заключение можно сделать ряд выводов.

В конце восьмидесятых и начале девяностых годов прошлого столетия ответственность за компьютерные преступления была предусмотрена во многих государствах мира.

«Информационная революция» застала Россию в сложный экономический и политический период. Необходимость досрочной разработки правовых основ охраны информационных отношений, еще слабая развитость электронно-вычислительных систем, незначительное количество выявленных общественно опасных посягательств на эти отношения, отсутствие необходимого опыта привело к тому, что во вновь принятом в 1996 года Уголовном кодексе РФ в гл. 28 «Преступления в сфере компьютерной информации» содержалось три статьи, предусматривающие ответственность за «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). Названные в ст. 272 и 274 УК РФ деяния относятся к преступлениям небольшой тяжести, а эти же преступления, совершенные при отягчающих обстоятельствах, – к преступлениям средней тяжести.

В тот период времени эти нормы в минимальной степени удовлетворяли потребности правоприменительной практики. В настоящее время с компьютеризацией общества, переходом на расчеты финансовых и банковских структур с использованием электронно-вычислительных машин и в связи с транснациональным характером компьютерной преступности упомянутые нормы не могут обеспечить борьбу с компьютерными преступлениями. В них не учтено многообразие общественных отношений, на которые посягают названные преступления (это не только экономические интересы, но и государственная безопасность, конституционные права человека, его честь и достоинство т.д.).

Несмотря на новизну компьютерных преступлений для отечественного уголовного законодательства, в государствах с высоким уровнем технологического развития проблема с компьютерной преступностью давно признана одной из первостепенных задач, важность которой неуклонно возрастает.

Недооценка общественной опасности посягательств на интересы, охраняемые гл. 28 УК РФ, в сочетании с конструктивными недостатками диспозиций этих уголовно-правовых норм, а также недостаточным уровнем подготовки правоприменительных органов, призванных вести борьбу с компьютерными преступлениями, привели к тому, что уголовно-правовые нормы, предусматривающие ответственность за названные преступления, применяются очень редко.

Сложившееся положение объясняется рядом причин, среди которых в первую очередь представляется необходимым выделить:

а) недостаточную разработанность теоретической модели компьютерных преступлений;

б) недостаточную изученность криминологической характеристики компьютерных преступлений и в этой связи неразработанность более совершенных методик по раскрытию и расследованию преступлений, комплекса мер предупредительного характера и рекомендаций по виктимологической профилактике.

Необходимость разработки новой системы компьютерных преступлений возникает еще и потому, что в ст. 272 – 274 УК РФ совершенно не учтены общественно опасные последствия неправомерного доступа в чужую компьютерную информацию.

Если в результате преступления причиняется ущерб, содеянное квалифицируется по статьям о преступлениях против собственности.

Представляется, что уголовно-правовые нормы об ответственности за преступления, совершенные с использованием высоких технологий, лицами, обладающими большим интеллектуальным потенциалом, влекущие тяжелые последствия, должны предусматривать более строгое наказание, чем обычные преступления против собственности. При построении системы компьютерных преступлений следует учесть опыт зарубежных государств, где компьютерная преступность оказалась более распространенной и нанесла более серьезный ущерб.

Так, предлагается следующая система компьютерных преступлений:

А. Преступления против личности: компьютерная клевета; компьютерное вторжение в частную жизнь; нарушение тайны электронной корреспонденции.

Б. Преступления в сфере экономики: компьютерное хищение; компьютерный экономический шпионаж; кража компьютерных услуг; торговля компьютерными паролями.

В. Преступления против общественной безопасности, общественного порядка и общественной нравственности: неправомерный доступ к компьютерной информации; кибертерроризм; создание, использование и распространение вредоносных программ для ЭВМ; компьютерное хулиганство; компьютерная порнография.

Г. Преступления против государственной безопасности: компьютерный шпионаж.

В настоящее время в России нет такого размаха компьютерной преступности, которая есть в некоторых странах Американского континента, Центральной и Восточной Европы. Но успокаиваться не следует. Однако в Россию она обязательно придет, и уголовный закон наряду с другими мерами профилактического характера должен стать реальным превентивным средством, способствующим созданию условий для нормального развития телекоммуникационных систем и охраны их от преступных посягательств. Уголовно-правовые нормы об ответственности за компьютерные преступления (ст. 272 – 274 УК РФ) не отвечают этому требованию.

# СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

I. Нормативные акты

Всеобщая декларация прав человека и гражданина утв. Генеральной Ассамблеей ООН 10 декабря 1948 года // Сборник документов по международному гуманитарному праву. – М.: Проспект, 2000. – С. 131-159.

Конституция Российской Федерации (принята на всенародном голосовании 12 декабря 1993 года) // Российская газета. – 1993. – 12 декабря.

Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 года № 63-ФЗ // Российская газета. – 1996. – 18, 19, 20, 25 июня.

О безопасности: Закон РФ от 5 марта 1992 года № 2446-I // Российская газета. – 1992. – 6 мая.

1. О государственной тайне: Закон РФ от 21 июля 1993 года № 5485-1 // Собрание законодательства Российской Федерации. – 1997. – № 41. – Ст. 8220 – 8235.
2. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ // Российская газета. – 2006. – 29 июля.

О коммерческой тайне: Федеральный закон от 29 июля 2004 года № 98-ФЗ // Собрание законодательства Российской Федерации. – 2004. – № 32. – Ст. 3283

О персональных данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.). – Ст. 3451.

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 9 сентября 2000 года № Пр-1895) // Парламентская газета. – 2000. – 30 сентября.
2. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 6 марта 1997 года № 188 (ред. от 23 сентября 2005 года) // Собрание законодательства Российской Федерации. – 1997. – № 10. – Ст. 1127.

О федеральной целевой программе «Электронная Россия (2002 – 2010 годы): Постановление Правительства РФ от 28 января 2002 года № 65 // Собрание законодательства Российской Федерации. – 2002. – № 5. – Ст. 531

О правовой охране программ для электронных вычислительных машин и баз данных: Закон РФ от 23 сентября 1992 года // Российская газета. – 1992. – 20 октября (утратил силу).

Об информации, информатизации и защите информации: Федеральный закон № 24-ФЗ от 20 февраля 1995 года // Российская газета. – 1995. – 22 февраля (утратил силу).

II. Уголовное законодательство зарубежных стран

Уголовный кодекс Азербайджанской Республики // www.zakon.msk.su

Уголовный кодекс Армении // www.base.spinform.ru/show.fwx?Regnom=7472

Уголовный кодекс Грузии // www.urbia.gol.ge/kodeksi/59.htm

Уголовный кодекс Молдовы // www.yk-md.ru

Уголовный кодекс Нидерландов // www.icpo.at.tut.by/crimru.htm

Уголовный кодекс Республики Беларусь // www.pravo.levonevsky.org/kodeksby

Уголовный кодекс Республики Казахстан // http://www.base.spinform.ru/show.fwx?Regnom=1365

Уголовный кодекс Республики Кыргызстан // www.prison.memo.ru/laws.htm

Уголовный кодекс Республики Таджикистан // http://www.crime.vl.ru/index.php?p=1323&more=1&c=1&tb=1&pb=1

Уголовный кодекс Республики Туркменистан // www.turkmenistan.gov.tm/\_ru/laws/?laws=40

Уголовный кодекс Республики Узбекистан // http://www.kodeks.uz/ugolkod

Уголовный кодекс Украины // www.crime.org.ua

Уголовный кодекс Испании // www.icpo.at.tut.by/crimru.htm

Уголовный кодекс Франции // www.icpo.at.tut.by/crimru.htm

III. Литература

1. Абов А.И., Ткаченко С.Н. Международный и отечественный опыт борьбы с компьютерными преступлениями. – М., 2004. – С. 5–28.
2. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М., 2005. – 611 с.
3. Батурин Ю.М. Проблемы компьютерного права. – М., 1991. – 201 с.
4. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М., 1991. – 321 с.
5. Боер В.М. Информационно-правовая политика России. – СПб., 2008. – 908 с.
6. Борчева Н. А. Компьютерное право и ответственность за компьютерные преступления за рубежом // На пути к информационному обществу: криминальный аспект: Сборник статей. – М., 2002. – С. 10-22.
7. Букалерова Л.А. Уголовно-правовая охрана официального информационного оборота. – М.: Юрлитинформ, 2006. – 111 с.
8. Вассер Э.С. Преступления в предпринимательской и банковской сферах за рубежом. – М., 2005. – 519 с.
9. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. – М.: Право и закон, 1996. – 342 с.
10. Виннер Н. Кибернетика и общество. – М., 1958. – 399 с.
11. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – 456 с.
12. Вус М.А., Войтович Н.А., Гусев В.С. Россия на пороге информационного общества // Россия на пороге информационного общества. Материалы семинара 22 апреля 1997 года. – СПб., 1997. – С. 77-101.
13. Гасанов Р.М. Шпионаж особого рода. – М., 2002. – 213 с.
14. Григоренко С. В. Об уголовной ответственности за преступления в сфере компьютерной информации в зарубежных странах (на примере США и Великобритании) // Государство, общество, личность: современные тенденции и проблемы развития: Сборник статей. Вып. 2. – М., 2003. – С. 34-77.
15. Григоренко С.В., Ткаченко С.Н., Каспаров А.А. Преступления в сфере компьютерной информации. – М., 2003. – 265 с.
16. Гринберг М.С. Преступления против общественной безопасности. – Свердловск, 1974. – 316 с.
17. Гурьянов К.В. Файлы CRACK как идентификационный признак совершения преступлений в сфере производства компьютерного (информационного) контрафакта // Эксперт-криминалист. – 2007. – № 3. – С. 12-20.
18. Жельников В. Криптография от папируса до компьютера. – М., 1996. – 567 с.
19. Женило В.Р. Проблемы развития цифровых информационных технологий в органах внутренних дел // Компьютерные технологии в криминалистике и информационная безопасность. – Труды академии МВД РФ. – М., 1997. – С. 32-45.
20. Иногамова-Хегай Л.В. Международное уголовное право. – СПб., 2003. – 657 с.

Касперски К. Компьютерные вирусы: внутри и снаружи. – М., 2006. – 303 с.

1. Ковалева Н.Н., Холодная Е.В. Комментарий к Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – М.: ООО «Новая правовая культура», 2007. – 364 с.
2. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – Минск, 2002. – 98 с.
3. Комиссаров В. С. Терроризм, бандитизм, захват заложников и другие тяжкие преступления против безопасности общества по новому УК РФ. – М., 1997. – 201 с.
4. Концепция информационной безопасности / Под ред. Д. С. Черешкина. – М.: ИСА РАН, 1994. – 156 с.
5. Костенко Н.И. Международная уголовная юстиция. Проблемы развития. – М., 2003. – С. 134 – 247.

Крутских А.В. Информационный взрыв безопасности на рубеже XXI века // Международная жизнь. – 1999. – № 2. – С. 82 – 89.

Крылов В.В. Информационные компьютерные преступления. – М., 1987. – 312 с.

Крылов В.В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право. – 1998. – № 3. – С. 84-91.

1. Крылов В.В. Расследование преступления в сфере информации. – М.: Издательство «Городец», 1998. – 221 с.
2. Кузнецова Н.Ф. Квалификация сложных составов преступлений // Уголовное право. – 2000. – № 1. – С. 26-33.

Курочкина Л.А. Принципы и нормы Совета Европы в уголовном судопроизводстве Российской Федерации // Журанал российского права. – 2006. – № 4. – С. 16-22.

1. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М., 1998. – 103 с.
2. Лукашук И.И., Наумов А.В. Международное уголовное право. – М., 1999. – 923 с.
3. Максимов В.Ю. Компьютерные преступления (вирусный аспект). – Ставрополь: Книжное издательство, 1999. – 97 с.

Маслакова Е.А. История правового регулирования уголовной ответственности за компьютерные преступления // Информационное право. – 2006. – № 4. – С. 23-26.

1. Международное уголовное право / Под общ. ред. В.Н. Кудрявцева. – М., 1999. – 509 с.

Модельный уголовный кодекс стран-участников СНГ // СНГ: Сборник документов. – 2006. – С. 34-58.

Мосин О. В. Компьютерная преступность: как с ней бороться? – М., 2008. – 306 с.

1. Осипенко А.Л. Борьба с преступлениями в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – 311 с.
2. Панов В.П. Сотрудничество государств в борьбе с международными уголовными преступлениями. – М., 1993. – 456 с.
3. Панфилова Е.И., Попов А.С. Компьютерные преступления. Серия «Современные стандарты в уголовном праве и уголовном процессе» / Науч. ред. Б. В. Волженкин. – СПб., 1998. – С. 45-79.

Расследование неправомерного доступа к компьютерной информации / Под ред. Н.Г. Шурухнова. – М.: Щит-М, 1999. – 121 с.

1. Симкин Л.С. Как остановить компьютерное пиратство? // Российская юстиция. – 1996. – № 10. – С. 22-29.

Соловьев Л.Н. Вредоносные программы: расследование и предупреждение преступлений. – М.: Собрание, 2004. – 109 с.

1. Состояние преступности за 2002-2007 годы. Статистический сборник. – М.: МВД РФ, 2008. – 456 с.
2. Толеубекова Б.Х. Компьютерная преступность: вчера, сегодня, завтра. – М., 2005. – 324 с.
3. Туманова Л.В., Снытников А.А. Обеспечение и защита права на информацию в США. – М., 2001. – 76 с.
4. Уголовное право. Особенная часть / Под ред. Н. И. Ветрова и Ю. И. Ляпунова. – М.: Новый юрист, 1998. – 713 с.
5. Черных А. Преступления компьютерного века // Советская юстиция. – 1987. – № 11. – С. 97-102.
6. Юрченко И.А. Информация конфиденциального характера как предмет уголовно-правовой охраны. – М., 2000. – 216 с.
1. Состояние преступности за 2002-2007 годы. Статистический сборник. – М.: МВД РФ, 2008. – С. 211. [↑](#footnote-ref-1)
2. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 года № 63-ФЗ // Российская газета. – 1996. – 18, 19, 20, 25 июня. [↑](#footnote-ref-2)
3. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М.: ООО Издательство «Юрлитинформ», 2002. – С. 87. [↑](#footnote-ref-3)
4. О правовой охране программ для электронных вычислительных машин и баз данных: Закон РФ от 23 сентября 1992 года // Российская газета. – 1992. – 20 октября (утратил силу). [↑](#footnote-ref-4)
5. Об информации, информатизации и защите информации: Федеральный закон № 24-ФЗ от 20 февраля 1995 года // Российская газета. – 1995. – 22 февраля (утратил силу). [↑](#footnote-ref-5)
6. Маслакова Е. А. История правового регулирования уголовной ответственности за компьютерные преступления // Информационное право. – 2006. – № 4. – С. 23. [↑](#footnote-ref-6)
7. Крылов В. В. Указ. соч. – С. 15. [↑](#footnote-ref-7)
8. Максимов В. Ю. Компьютерные преступления (вирусный аспект). – Ставрополь: Книжное издательство, 1999. – С. 42. [↑](#footnote-ref-8)
9. Крылов В. В. Указ. соч. – С. 17. [↑](#footnote-ref-9)
10. Модельный уголовный кодекс стран-участников СНГ // СНГ: Сборник документов. – 2006. – С. 34. [↑](#footnote-ref-10)
11. Мосин О. В. Компьютерная преступность: как с ней бороться? – М., 2008. – С. 12. [↑](#footnote-ref-11)
12. Крылов В. В. Расследование преступления в сфере информации. – М.: Издательство «Городец», 1998. – С. 22. [↑](#footnote-ref-12)
13. Григоренко С. В. Об уголовной ответственности за преступления в сфере компьютерной информации // Государство, общество, личность: современные тенденции и проблемы развития: Сборник статей. Вып. 2. – М., 2003. – С. 11. [↑](#footnote-ref-13)
14. Осипенко А. Л. Борьба с преступлениями в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – С. 19. [↑](#footnote-ref-14)
15. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ // Российская газета. – 2006. – 29 июля. [↑](#footnote-ref-15)
16. Панфилова Е. И. Компьютерные преступления. – М., 2006. – С. 37. [↑](#footnote-ref-16)
17. Лукашук И. И., Наумов А В. Международное уголовное право. – М., 1999. – С. 123; Международное уголовное право / Под общ. ред. В. Н. Кудрявцева. – М., 1999. – С. 50–90; Костенко Н. И. Международная уголовная юстиция. Проблемы развития. – М., 2003. – С. 134 – 247. [↑](#footnote-ref-17)
18. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. – М., 1998. – С. 12. [↑](#footnote-ref-18)
19. Борчева Н. А. Компьютерное право и ответственность за компьютерные преступления за рубежом // На пути к информационному обществу: криминальный аспект: Сборник статей. – М., 2002. – С. 10; 2004. – С. 5–28. [↑](#footnote-ref-19)
20. Уголовный кодекс Республики Беларусь // www.pravo.levonevsky.org/kodeksby [↑](#footnote-ref-20)
21. Более подробно Козлов В. Е. Теория и практика борьбы с компьютерной преступностью. – Минск, 2002. – С. 64-74. [↑](#footnote-ref-21)
22. Уголовный кодекс Республики Таджикистан // http://www.crime.vl.ru/index.php?p=1323&more=1&c=1&tb=1&pb=1 [↑](#footnote-ref-22)
23. Уголовный кодекс Украины // www.crime.org.ua [↑](#footnote-ref-23)
24. Позднее Закон Украины «О внесении изменений в Уголовный кодекс Украины относительно ответственности за незаконное вмешательство в работу сетей электросвязи» (№ 908-IV от 5 июня 2003 года) внес некоторые изменения в ст. 361 УК Украины, в которой теперь дополнительно предусматривается уголовная ответственность не только за незаконное вмешательство в работу электронно-вычислительных машин (компьютеров), систем и компьютерных сетей, а и за незаконное вмешательство в работу сетей электросвязи, которое привело к уничтожению, искажению, блокированию информации или к нарушению установленного порядка ее маршрутизации. [↑](#footnote-ref-24)
25. Уголовный кодекс Республики Узбекистан // http://www.kodeks.uz/ugolkod [↑](#footnote-ref-25)
26. Уголовный кодекс Республики Казахстан // http://www.base.spinform.ru/show.fwx?Regnom=1365 [↑](#footnote-ref-26)
27. Уголовный кодекс Республики Кыргызстан // www.prison.memo.ru/laws.htm [↑](#footnote-ref-27)
28. Уголовный кодекс Республики Туркменистан // www.turkmenistan.gov.tm/\_ru/laws/?laws=40 [↑](#footnote-ref-28)
29. Уголовный кодекс Азербайджанской Республики // www.zakon.msk.su [↑](#footnote-ref-29)
30. Уголовный кодекс Грузии // www.urbia.gol.ge/kodeksi/59.htm [↑](#footnote-ref-30)
31. Уголовный кодекс Молдовы // www.yk-md.ru [↑](#footnote-ref-31)
32. Предусмотрен квалифицированный состав: то же действие, совершенное: a) повторно; b) двумя или более лицами; c) с нарушением систем защиты; d) путем подключения к каналам связи; e) с использованием специальных технических средств. [↑](#footnote-ref-32)
33. Уголовный кодекс Армении // www.base.spinform.ru/show.fwx?Regnom=7472 [↑](#footnote-ref-33)
34. Так, в соответствии с УК Азербайджана, Армении, Кыргызстана, Российской Федерации, Туркменистана, где составы преступлений охватываются главой «Преступления в сфере компьютерной информации», родовым объектом являются отношения в области компьютерной информации. [↑](#footnote-ref-34)
35. Уголовный кодекс Нидерландов // www.icpo.at.tut.by/crimru.htm [↑](#footnote-ref-35)
36. Уголовный кодекс Франции // www.icpo.at.tut.by/crimru.htm [↑](#footnote-ref-36)
37. Уголовный кодекс Испании // www.icpo.at.tut.by/crimru.htm [↑](#footnote-ref-37)
38. Туманова Л. В., Снытников А. А. Обеспечение и защита права на информацию в США. – М., 2001. – С. 11. [↑](#footnote-ref-38)
39. Туманова Л. В., Снытников А. А. Указ. соч. С. 18. [↑](#footnote-ref-39)
40. Толеубекова Б. Х. Компьютерная преступность: вчера, сегодня, завтра. – М., 2005. – С. 35. [↑](#footnote-ref-40)
41. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия. – М.: Право и закон, 1996. – С. 24. [↑](#footnote-ref-41)
42. Школин И. Инвесторы против пиратства // Финанс. – 2007. – № 6. – С. 13. [↑](#footnote-ref-42)
43. Малков В. Д. Криминология: учебник для вузов. Изд. 3-е. – М., 2007. – С. 447. [↑](#footnote-ref-43)
44. Крылов В. В. Информационные компьютерные преступления. – М., 1987. – С. 12. [↑](#footnote-ref-44)
45. Вассер Э. С. Преступления в предпринимательской и банковской сферах за рубежом. – М., 2005. – С. 146. [↑](#footnote-ref-45)
46. О безопасности: Закон РФ от 5 марта 1992 года № 2446-I // Российская газета. – 1992. – 6 мая. [↑](#footnote-ref-46)
47. См.: Гринберг М. С. Преступления против общественной безопасности. – Свердловск, 1974. – С. 35, 36. [↑](#footnote-ref-47)
48. Комиссаров В. С. Терроризм, бандитизм, захват заложников и другие тяжкие преступления против безопасности общества по новому УК РФ. – М., 1997. – С. 20. [↑](#footnote-ref-48)
49. Вехов В. Б. Указ. соч. – С. 21. [↑](#footnote-ref-49)
50. Боер В. М. Информационно-правовая политика России. – СПб., 2008. – С. 187. [↑](#footnote-ref-50)
51. Доктрина информационной безопасности Российской Федерации утв. Указом Президента РФ 9 сентября 2000 года № Пр-1895 // Российская газета. – 2000. – 28 сентября. [↑](#footnote-ref-51)
52. Вус М. А., Войтович Н. А., Гусев В. С. Указ. соч. – С. 6. [↑](#footnote-ref-52)
53. Всеобщая декларация прав человека и гражданина утв. Генеральной Ассамблеей ООН 10 декабря 1948 года // Сборник документов по международному гуманитарному праву. – М.: Проспект, 2000. – С. 131-159. [↑](#footnote-ref-53)
54. Ковалева Н. Н., Холодная Е. В. Комментарий к Федеральному закону от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации». – М.: ООО «Новая правовая культура», 2007. – С. 6. [↑](#footnote-ref-54)
55. Панин А. А. Философия: Учебник для вузов. – М.: Проспект, 2002. – С. 401. [↑](#footnote-ref-55)
56. Юрченко И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны. – М., 2000. – С.15. [↑](#footnote-ref-56)
57. Виннер Н. Кибернетика и общество. – М., 1958. – С. 31. [↑](#footnote-ref-57)
58. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 года № 149-ФЗ // Российская газета. – 2006. – 29 июля. [↑](#footnote-ref-58)
59. Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. Л. В. Иногамовой-Хегай, А. И. Рарога, А. И. Чучаева. – М., 2006. – С. 427. [↑](#footnote-ref-59)
60. Российская газета. – 2006. – 12 мая. [↑](#footnote-ref-60)
61. Вехов В. Б. Указ. соч. – С. 17-18. [↑](#footnote-ref-61)
62. Гурьянов К. В. Файлы CRACK как идентификационный признак совершения преступлений в сфере производства компьютерного (информационного) контрафакта // Эксперт-криминалист. – 2007. – № 3. – С. 12. [↑](#footnote-ref-62)
63. О государственной тайне: Закон РФ от 21 июля 1993 года № 5485-1 // Собрание законодательства Российской Федерации. – 1993. – № 41. – Ст. 8220 – 8235. [↑](#footnote-ref-63)
64. Об утверждении Перечня сведений конфиденциального характера: Указ Президента РФ от 6 марта 1997 года № 188 (ред. от 23 сентября 2005 года) // Собрание законодательства Российской Федерации. – 1997. – № 10. – Ст. 1127. [↑](#footnote-ref-64)
65. В литературе используются различные понятия, по сути обозначающие то же самое деяние: «компьютерный взлом», «хакинг», «компьютерная атака», «компьютерное вторжение» и др. [↑](#footnote-ref-65)
66. Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. – М.: Щит-М, 1999. – С. 70. [↑](#footnote-ref-66)
67. Крылов В. В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право. – 1998. – № 3. – С. 84. [↑](#footnote-ref-67)
68. Букалерова Л. А. Уголовно-правовая охрана официального информационного оборота. – М.: Юрлитинформ, 2006. – С. 24. [↑](#footnote-ref-68)
69. Аргументы и факты. – 2007. – 16 июня. [↑](#footnote-ref-69)
70. Расследование неправомерного доступа к компьютерной информации / Под ред. Н. Г. Шурухнова. – М.: Щит-М, 1999. – С. 72. [↑](#footnote-ref-70)
71. О персональных данных: Федеральный закон от 27 июля 2006 года № 152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.). – Ст. 3451. [↑](#footnote-ref-71)
72. О коммерческой тайне: Федеральный закон от 29 июля 2004 года № 98-ФЗ // Собрание законодательства Российской Федерации. – 2004. – № 32. – Ст. 3283 [↑](#footnote-ref-72)
73. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. – М., 2005. – С. 120. [↑](#footnote-ref-73)
74. Касперски Е. Компьютерные вирусы: внутри и снаружи. – М., 2006. – С. 14-22. [↑](#footnote-ref-74)
75. О федеральной целевой программе «Электронная Россия (2002 – 2010 годы): Постановление Правительства РФ от 28 января 2002 года № 65 // Собрание законодательства Российской Федерации. – 2002. – № 5. – Ст. 531 [↑](#footnote-ref-75)
76. Жельников В. Криптография от папируса до компьютера. – М., 1996. – С. 276. [↑](#footnote-ref-76)
77. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях: Международный опыт: Монография. – М.: Норма, 2004. – С. 86. [↑](#footnote-ref-77)
78. Соловьев Л. Н. Вредоносные программы: расследование и предупреждение преступлений. – М.: Собрание, 2004. – С. 29. [↑](#footnote-ref-78)
79. Осипенко Л. А. Указ. соч. – С. 85 – 86. [↑](#footnote-ref-79)
80. Осипенко Л. А. Указ. соч. – С. 87. [↑](#footnote-ref-80)
81. Крутских А. В. Информационный взрыв безопасности на рубеже XXI века // Международная жизнь. – 1999. – № 2. – С. 82 – 89. [↑](#footnote-ref-81)
82. Уголовное право. Особенная часть / Под ред. Н. И. Ветрова и Ю. И. Ляпунова. – М.: Новый юрист, 1998. – С. 558. [↑](#footnote-ref-82)
83. Уголовное право. Особенная часть / Под ред. Н. И. Ветрова и Ю. И. Ляпунова. – М.: Новый юрист, 1998. – С. 558. [↑](#footnote-ref-83)
84. Симкин Л. С. Как остановить компьютерное пиратство? // Российская юстиция. – 1996. – № 10. – С. 22. [↑](#footnote-ref-84)
85. Кузнецова Н. Ф. Квалификация сложных составов преступлений // Уголовное право. – 2000. – № 1. – С. 26. [↑](#footnote-ref-85)