

На правах рукописи

Зинина Ульяна Викторовна

**ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ
ИНФОРМАЦИИ В РОССИЙСКОМ И
ЗАРУБЕЖНОМ УГОЛОВНОМ ПРАВЕ**

Специальность 12.00.08 – уголовное право и криминология;
уголовно-исполнительное право

Автореферат

диссертации на соискание учёной степени
кандидата юридических наук

Москва – 2007 г.

Диссертация выполнена в секторе уголовного права и криминологии
Института государства и права Российской академии наук

Научный руководитель: кандидат юридических наук, доцент
Полубинская Светлана Вениаминовна

Официальные оппоненты: доктор юридических наук, профессор
Цепелев Валерий Филиппович

кандидат юридических наук, доцент,
заслуженный юрист Российской Федерации
Никулин Сергей Иванович

Ведущая организация: Государственный университет - Высшая школа
экономики

Защита состоится «10» мая 2007 г. в 12 часов 00 минут на заседании
диссертационного совета Д 002.002.04 в Институте государства и права
Российской академии наук по адресу: 119991, г. Москва, ул. Знаменка, д. 10.

С диссертацией можно ознакомиться в библиотеке Института государства и
права Российской академии наук по адресу: 119991, г. Москва, ул. Знаменка,
д. 10.

Автореферат разослан «___» _____ 2007 г.

Учёный секретарь диссертационного совета
доктор юридических наук, профессор _____ С.В.Максимов

Общая характеристика работы

Актуальность темы диссертационного исследования. Во все времена объектом права становится лишь то, что является значимым для государства, общества и человека, а одним из решающих (хотя и не единственным) критериев для наделения того или иного явления правовыми характеристиками выступает его экономическая ценность: в «поле» зрения права входит то, что может стать предметом хозяйственного оборота. В век информационных технологий таким объектом становятся информационные отношения. Быстрые способы передачи информации в наши дни являются одним из самых привлекательных объектов предпринимательской деятельности, они используются в коммерческих целях и приносят гигантские прибыли.

Одновременно с пониманием огромной ценности информации возникает и потребность в ее защите. Проблема защиты компьютерной информации и информационных систем сейчас является одной из самых актуальных во всем мире. Новые возможности, предоставляемые информационными технологиями, их широкая распространенность и доступность делают эту область чрезвычайно привлекательной для представителей криминальной среды. Стремительное развитие информационно-телекоммуникационных сетей, создание многочисленных информационных систем, разработка более совершенных технических устройств – все это создает условия, облегчающие совершение преступлений в этой сфере, число которых с каждым годом увеличивается как в России, так и в зарубежных странах.

Задача уголовного законодательства в этой связи – обеспечить пресечение наиболее общественно опасных посягательств на компьютерную информацию, информационные системы и сети. Надо отметить, что именно в указанной сфере уголовное право оказалось не вполне готовым к стремительному развитию компьютерной техники и ее внедрению в

повседневную жизнь людей. Право в целом и уголовное право, в частности, нередко отстает от развития общественных отношений, связанных с использованием информации, и поэтому процесс нахождения адекватных форм и способов их правового регулирования, в том числе противодействия компьютерным преступлениям, идет уже не один десяток лет – в США с конца 70-х годов прошлого века, в Великобритании – с конца 80-х.

В Российской Федерации с 1997 года уголовно-наказуемыми были признаны определенные деяния в сфере компьютерной информации, обладающие общественной опасностью для безопасного использования компьютерной информации и информационных технологий. Нормы о данных преступлениях зафиксированы в трех статьях УК РФ, выделенных в самостоятельную главу 28 УК РФ. К ним относят: статья 272 УК РФ «Неправомерный доступ к охраняемой законом компьютерной информации», статья 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ» и статья 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети».

Количество преступлений, совершаемых в сфере компьютерной информации, с каждым годом растет. По данным ГИЦ МВД России, если в 1997 году было зарегистрировано всего 7 преступлений в сфере компьютерной информации, то в 2002 году их число возросло до 4050 таких преступлений, а в 2005 г. составило 10214 случаев. Но при этом необходимо подчеркнуть, что указанные деяния отличаются высокой латентностью. Как показывают уголовная и судебная статистика, значительная часть таких преступлений остается за рамками реально выявленных и раскрытых. Незначительным является и число лиц, осужденных за преступления в сфере компьютерной информации: в 1998 году за все преступления, предусмотренные главой 28 УК РФ, было осуждено 7 человек, в 2002 году – 97, в 2005 году – 203¹.

¹ Официальный сайт МВД России. Общие сведения о состоянии преступности.
www.mvdinform.ru

Информационная сфера как область динамично развивающаяся нуждается в адекватном правовом регулировании. Многие законодательные акты Российской Федерации в данной сфере были приняты во второй половине 90-х годов прошлого века и уже не отвечают современному состоянию общественных отношений и техническому прогрессу, по отдельным вопросам вступают в противоречие с более поздними законодательными актами и в целом нередко тормозят развитие информационного общества. В этой связи очевидна необходимость их корректировки и совершенствования. Законодательство многих стран мира (включая и Россию) содержит явно недостаточное регулирование ответственности за преступления в сфере компьютерной информации, чтобы эффективно противодействовать их совершению. Зачастую отсутствуют и необходимые механизмы международного сотрудничества. В российском уголовном законе существуют недостатки в описании элементов и признаков соответствующих составов преступлений; неточности законодательных формулировок негативно влияют на правоприменительную практику, в том числе, на правильную квалификацию деяний в сфере компьютерной информации. Российские ученые и практические работники неоднократно обращали на это внимание. Кроме того, с появлением новых технологий появляются новые формы преступности, к примеру, взлом сотовых телефонов с использованием Bluetooth или беспроводной сети связи Wi-fi, нарушение работы информационных систем (Dos-атаки), на которые в рамках действующих редакций статей 272-274 УК РФ не всегда можно эффективно реагировать.

По своей сути преступления в сфере компьютерной информации являются трансграничными, и потому все международные организации призывают государства в сотрудничестве с другими заинтересованными сторонами разрабатывать необходимое законодательство, предусматривающее проведение совместных расследований указанных

деяний с использованием существующего международного права, и, в частности, Конвенции Совета Европы по киберпреступности.

Все вышеизложенное подтверждает необходимость совершенствования конструкций норм УК РФ, устанавливающих ответственность за преступления в сфере компьютерной информации, на основе исследования действующего российского телекоммуникационного и информационного законодательства, практики применения статей 272-274 УК РФ, изучения зарубежных уголовных законов и судебной практики, а также международно-правовых документов, разработанных и принятых в этой области.

Объектом диссертационного исследования являются правовые отношения, юридические факты и процессы, складывающиеся по поводу противодействия преступлениям в сфере компьютерной информации в России и зарубежных странах, а также проблемы применения норм уголовного закона, устанавливающих ответственность за такие преступления.

Предметом диссертационного исследования являются законодательные акты, регламентирующие уголовную ответственность за преступления в сфере компьютерной информации, а также информационные и телекоммуникационные отношения, российская и зарубежная судебная практика, международно-правовые акты, принятые по вопросам противодействия компьютерным преступлениям.

Цель и задачи исследования. Основные цели исследования заключаются в выяснении уголовно-правовой природы преступлений в сфере компьютерной информации, оценке степени соответствия российского и зарубежного уголовного законодательства современному состоянию развития информационных технологий и криминологическим реалиям, изучении основных направлений и форм международного сотрудничества в

области противодействия рассматриваемым преступлениям. Также целью данной работы является выработка рекомендаций по улучшению формулировок составов преступлений в сфере компьютерной информации в УК РФ и совершенствованию международного сотрудничества в противодействии таким преступлениям путем выделения приоритетных направлений его развития.

Реализация указанных целей предполагает решение следующих конкретных задач:

- раскрыть место, роль и важность противодействия преступлениям в сфере компьютерной информации;

- обосновать авторское понимание компьютерной информации как уголовно-правовой категории и определить ее соотношение со смежными правовыми понятиями;

- раскрыть содержательные характеристики новых видов преступлений в сфере компьютерной информации и последствий таких преступлений, отражающих их общественную опасность;

- обосновать с точки зрения телекоммуникационного и информационного законодательства недостатки положений УК РФ и выявить возникающие в этой связи проблемы их практического применения;

- провести сравнительно-правовой анализ предписаний, содержащихся в российском и зарубежном уголовном законодательстве, а также изучить и проанализировать практику их применения в России и зарубежных странах, и на этой основе сформулировать конкретные рекомендации по совершенствованию главы 28 УК РФ;

- исследовать основные направления и формы международного сотрудничества в противодействии преступлениям в сфере компьютерной информации, роль различных международных организаций в этой области, выявив тенденции развития такого сотрудничества.

Методология и методика. Методологической основой диссертационного исследования являются актуальные методы познания, в том числе как общенаучного (системный подход, логический, диалектический, социологический, исторический), так и специально-познавательного (сравнительно-правовой, организационно-функциональный, лингво-юридический, дедукции и индукции, формально-логический) характера.

Формулировка и обоснование теоретических положений, практических рекомендаций и выводов осуществлены с использованием апробированных методов, применяемых в науках уголовного, информационного, международного права, а также общей теории права, философии, социологии, экономики.

Теоретическая основа исследования определена комплексным характером проблемы противодействия преступлениям в сфере компьютерной информации. Для диссертационного исследования важное значение имели как общетеоретические работы в области уголовного права и криминологии, так и труды, в которых рассматриваются проблемы информационного законодательства, как основной отрасли в сфере использования информации и информационных технологий.

К первым относятся, прежде всего, труды Ю.М.Батурина, Н.И.Ветрова, В.Б.Вехова, А.Г.Волеводза, Ю.В.Гаврилина, В.А.Голубева, А.Э.Жалинского, В.Е.Козлова, В.Н.Кудрявцева, Н.Ф.Кузнецовой, Н.А.Лопашенко, В.В.Лунеева, Ю.И.Ляпунова, А.В.Наумова, С.И.Никулина, В.А.Номоконова, С.В.Полубинской, Н.Г.Шурухнова, В.Ф.Цепелева.

В рамках второй группы следует назвать, прежде всего, труды И.Л.Бачило, Е.А.Войниканис, Е.К.Волчинской, В.Б.Наумова, В.О.Калятина, Б.В.Кристалного, В.Н.Лопатина, А.А.Стрельцова, Л.К.Терещенко, М.В.Якушева, М.А.Федотова и других.

Существенный научно-практический интерес для изучения проблем преступлений в сфере компьютерной информации представляют также работы, посвященные различным аспектам телекоммуникационного законодательства.

Нормативную базу исследования составляют: Конституция Российской Федерации, российское федеральное законодательство, решения судов общей юрисдикции Российской Федерации, а также судов зарубежных стран, содержащие правовые позиции по многим проблемам, являющимся объектом диссертационного исследования, законодательство зарубежных стран об ответственности за преступления в сфере компьютерной информации, таких как Великобритания, США, Япония, Нидерланды, ФРГ, Франция, Бразилии, Испания, КНДР, Италия, страны-участницы СНГ и другие.

Кроме того, значительную часть объекта исследования составили международно-правовые нормы, содержащиеся в руководящих документах Организации Объединенных Наций, Совета Европы, Европейского Союза, Организации Экономического Сотрудничества и Развития, Группы Восьми, Интерпола, Содружества Независимых Государств.

Эмпирическую основу работы составляют опубликованная судебная практика судов общей юрисдикции Российской Федерации и решения судов зарубежных государств; данные официальной статистики органов внутренних дел, статистические и аналитические данные международных организаций; материалы уголовных дел и постановлений об отказе в возбуждении уголовных дел УСТМ ГУВД г. Москвы.

Степень научной разработанности темы. Рассматриваемый вид преступлений уже выступал в качестве объекта диссертационного исследования, однако при этом проблема рассматривалась в основном с

криминалистической или криминологической точек зрения. В уголовно-правовом смысле данная проблема разработана на уровне публикаций в научной литературе, диссертационных исследований, посвященных отдельным аспектам проблемы, не содержащих сравнительно-правового анализа и не рассматривающих вопросы международного сотрудничества.

Монографических и диссертационных работ, подготовленных отечественными специалистами и содержащих комплексный анализ законодательства об уголовной ответственности за преступления в сфере компьютерной информации в российском, зарубежном и международном праве, недостаточно. Так, исследование преступлений в сфере компьютерной информации проводилось в диссертационных работах по уголовному праву, выполненных Смирновой Т.Г. «Уголовно-правовая борьба с преступлениями в сфере компьютерной информации» (1998 г.), Ушаковым С.И. «Преступления в сфере обращения компьютерной информации: Теория, законодательство, практика» (2000 г.), Воробьевым В.В. «Преступления в сфере компьютерной информации: Юридическая характеристика составов и квалификация» (2000 г.), Бессоновым В.А. «Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации» (2001 г.), Дворецким М.Ю. «Преступления в сфере компьютерной информации: Уголовно-правовое исследование» (2001 г.), Спириной С.Г. «Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации» (2001 г.), Бражником С.Д. «Преступления в сфере компьютерной информации: проблемы законодательной техники» (2002 г.), Карповой В.С. «Уголовная ответственность за преступления в сфере компьютерной информации» (2002 г.), Малышенко Д.Г. «Уголовная ответственность за неправомерный доступ к компьютерной информации» (2002 г.), Дорониным А.М. «Уголовная ответственность за неправомерный доступ к компьютерной информации» (2003 г.), Жмыховым А.А. «Компьютерная преступность за рубежом и ее предупреждение» (2003 г.), Тропиной Т.Л. «Киберпреступность: понятие, состояние, уголовно-правовые

меры борьбы» (2005 г.), Ястребовым Д.А. «Неправомерный доступ к компьютерной информации. Уголовно-правовые и криминологические аспекты» (2005 г.).

Указанные диссертационные исследования внесли серьезный вклад в изучение преступности в сфере компьютерной информации, однако многие из них были посвящены преимущественно одному виду данных преступлений – неправомерному доступу к компьютерной информации; другие – только криминологическим аспектам проблемы. Большинство из этих исследований основываются на уже не действующем отраслевом законодательстве и из-за изменения правового регулирования или по иным причинам, например, в связи с появлением новых форм компьютерных преступлений, утратило свою актуальность.

В связи с этим **научная новизна** диссертационного исследования заключается в том, что в работе впервые составы преступлений в сфере компьютерной информации, предусмотренные УК РФ, анализируются с учетом новейшего российского информационного и телекоммуникационного законодательства. Автором проведен системный терминологический анализ понятий, используемых в российском уголовном законе при описании элементов и признаков таких преступлений. Изучение зарубежного уголовного законодательства, российской и зарубежной правоприменительной практики позволило автору сделать выводы о тенденциях и современных направлениях развития положений уголовного права, регламентирующих ответственность за преступления в сфере компьютерной информации, и показать пути совершенствования норм, содержащихся в главе 28 УК РФ.

На основе исследования преступлений в сфере компьютерной информации как трансграничных, обобщения теории и практики международного сотрудничества в этой области предпринята попытка выявления и концептуального обоснования практической важности и

необходимости выработки унифицированных подходов к понятию, определению видов, а также способов и методов борьбы с рассматриваемыми преступлениями. Обобщение практики международного сотрудничества в противодействии рассматриваемым видам преступности позволило сформулировать выводы о необходимых шагах, которые должна предпринять Российская Федерация, чтобы не отставать в этой области от развитых западных стран.

По результатам исследования сформулированы предложения по совершенствованию российского уголовного законодательства.

На защиту выносятся следующие новые выводы и положения, имеющие принципиальное значение для теории и практики уголовно-правовой защиты компьютерной информации, информационных систем и сетей:

1. Преступления в сфере компьютерной информации имеют динамичный характер. В результате быстрого развития новых технологий не менее быстрыми темпами появляются новые формы компьютерной преступности, получающие распространение при использовании новых методов, например, технологии Bluetooth, беспроводных сетей связи Wi-fi, WiMAX, пиринговых сетей (P2P), спама и других.

Быстрота развития информационных технологий требует динамичности законодательства, включая предписания об уголовной ответственности за преступления в сфере компьютерной информации. Уголовное законодательство должно адекватно реагировать на изменения как форм преступлений в сфере компьютерной информации, появление новых способов их совершения, так и отражать современное состояние развития информационных технологий и соответствующего отраслевого законодательства.

2. Анализ УК РФ и российской судебной практики по вопросам квалификации преступлений в сфере компьютерной информации

свидетельствует, что информационное и телекоммуникационное законодательство редко принимается во внимание как при описании элементов и признаков составов преступлений в сфере компьютерной информации, так и в практике их применения.

Противодействие преступлениям в сфере компьютерной информации носит комплексный характер и должно базироваться не только на нормах уголовного права, но и на положениях информационного и телекоммуникационного законодательства.

3. Реальная статистика раскрываемых преступлений в сфере компьютерной информации в России искажена в результате не всегда правильного применения в следственной и судебной практике главы 28 УК РФ, в частности, при расширительном толковании элементов содержащихся в ней составов преступлений и фактическом непонимании технических реалий. Расширительно толкуется в практике и предмет рассматриваемых преступлений, т.е. компьютерная информация.

4. Формулировка состава преступления, предусмотренного в статье 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации - как материального не отражает криминологическую реальность. Материальный состав преступления «отсекает» целый ряд ситуаций, когда указанных в законе последствий не наступает, но сам факт того, что информация становится известна третьему лицу, причиняет существенный вред ее обладателю. Кроме того, описание в часть 2 статьи 272 УК РФ специального субъекта преступления как лица, имеющего доступ к ЭВМ, системе ЭВМ или их сети, основывается на устаревших представлениях о возможностях информационных технологий, об ЭВМ как машинах, стоящих в закрытых помещениях.

Учитывая современный этап развития информационных технологий, на основании оценки общественной опасности неправомерного доступа к компьютерной информации с учетом сравнительно-правового анализа уголовного законодательства зарубежных стран и международно-правовых

рекомендаций, предлагается изложить статью 272 УК РФ в следующей редакции:

«Статья 272. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к компьютерной информации, совершенный с обходом средств защиты информации с целью её уничтожения, блокирования, модификации или копирования, -

наказывается ...

2. То же деяние, если оно повлекло за собой уничтожение, блокирование, модификацию или копирование компьютерной информации, -

наказывается ...

3. Деяние, предусмотренное частью первой и второй и совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, -

наказывается ...».

5. Диспозиция статьи 274 УК РФ - нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети – сформулирована как бланкетная, т.е. требующая обращения к конкретным правилам, что затрудняет применение данной статьи в полном объеме в связи с нередким отсутствием соответствующих правил.

Более того, общественная опасность этого деяния состоит не в нарушении правил эксплуатации ЭВМ как таковых, что подтверждается анализом зарубежного законодательства, а в тех последствиях, к которым такие нарушения приводят, т.е. в нарушении работы информационных систем или информационно-телекоммуникационных сетей.

В этой связи предлагается изложить данную статью в следующей редакции:

«Статья 274. Нарушение работы информационной системы либо информационно-телекоммуникационных сетей.

Умышленные действия, направленные на временное или постоянное нарушение работы информационной системы или информационно-телекоммуникационной сети, блокирование доступа к какой-либо информации, информационной системе или информационно-телекоммуникационной сети, -
наказывается ...».

6. Трансграничный характер преступлений в сфере компьютерной информации требует межгосударственного подхода к противодействию им, эффективность которого недостижима без международного сотрудничества. В свою очередь, обеспечение такого сотрудничества требует выработки согласованных подходов к определению видов преступлений в сфере компьютерной информации, разработки согласованных процедур взаимодействия правоохранительных органов разных стран при расследовании таких преступлений, получении необходимых доказательств и выявлении виновных в них лиц. Анализ зарубежного уголовного законодательства показывает, что на данный момент отсутствует как единообразное понимание в формулировании составов преступлений в сфере компьютерной информации, так и унифицированные процедуры взаимодействия правоохранительных органов.

Международно-правовые механизмы должны играть главную роль в гармонизации национального уголовного законодательства различных стран в этой сфере. Исходя из этого, Российская Федерация должна подписать и ратифицировать Конвенцию Совета Европы по киберпреступности.

Теоретическая значимость результатов исследования состоит в том, что проведенный автором сравнительно-правовой анализ создает научные предпосылки для совершенствования норм УК РФ, предусматривающих ответственность за преступления в сфере компьютерной информации, качественного улучшения законодательной техники при формулировании

составов таких преступлений, единообразия судебной и следственной практики.

Практическое значение результатов исследования состоит в формулировании рекомендаций по совершенствованию уголовного законодательства и практики его применения.

Результаты диссертационного исследования могут быть учтены при совершенствовании УК РФ, подготовке разъяснений Пленума Верховного Суда РФ, в деятельности следственных и судебных органов при расследовании и разрешении уголовных дел, возбуждаемых по статьям 272-274 УК РФ. Положения диссертационного исследования могут использоваться при подготовке позиции Российской Федерации в международных организациях.

Материалы диссертации позволят усовершенствовать учебные курсы по уголовному и информационному праву, преподаваемые в юридических образовательных организациях.

Апробация результатов диссертационного исследования. Положения, выносимые на защиту, докладывались на научных и научно-практических конференциях, в их числе: 6-я международная конференция «Безопасность и доверие при использовании инфокоммуникационных сетей и систем» (2007, Москва); Национальный форум информационной безопасности (2005, 2006, 2007, Москва), Глобальный форум по партнерству государств и бизнеса в противодействии терроризму Группы Восьми (2006, Москва); Совещание-семинар руководителей подразделений специальных технических мероприятий МВД, ГУВД «Совершенствование оперативно-служебной деятельности УСТМ по борьбе с преступлениями, совершаемыми с использованием информационных технологий» (2006, Анапа); Международная практическая конференция по борьбе с киберпреступностью и кибертерроризмом (2006, Москва); Заседания Подгруппы по

преступлениям в сфере высоких технологий Римско-Лионской группы Группы Восьми (2005, Лондон; 2006, Москва); Парламентские слушания Государственной Думы Федерального Собрания Российской Федерации «Законодательное обеспечение в сфере информации, информационных технологий и защиты информации» (2006, Москва); Совещание экспертов Совета Европы по вопросам принятия в Российской Федерации законодательства в сфере защиты персональных данных (2005, Париж); Семинар ОБСЕ «Борьба с использованием сети Интернет в террористических целях» (2005, Вена); Заседание Комиссии по информационной безопасности Регионального Содружества Связи (2005, Баку).

Основные положения диссертационного исследования докладывались также на совещаниях органов государственной власти различных уровней, как национальных, так и международных; использовались автором при работе в рабочих группах по подготовке проектов федеральных законов, в том числе Федерального закона «Об информации, информационных технологиях и о защите информации» и Федерального закона «О персональных данных»; были опубликованы в виде научных статей, тезисов в сборниках докладов научных конференций (шесть публикаций, в том числе, в ведущих рецензируемых научных журналах, общим объёмом 2,85 п.л.), а также при подготовке главы Нового курса российского уголовного права в секторе уголовного права и криминологии Института государства и права РАН (в соавторстве); использовались в служебной деятельности в Министерстве информационных технологий и связи Российской Федерации, Координационном центре национального домена сети Интернет.

Структура работы определена целями и задачами исследования и состоит из введения, трех глав, включающих в себя восемь параграфов, заключения и списка использованной литературы.

Содержание работы

Во **введении** обоснованы актуальность и научная новизна темы, определены степень ее разработанности, предмет, цели и задачи исследования, изложены теоретические и методологические основы исследования, сформулированы положения, выносимые на защиту, отражены теоретическая и практическая значимость результатов диссертационного исследования и его структура.

Первая глава диссертационного исследования «Общая характеристика преступлений в сфере компьютерной информации» состоит из двух параграфов.

В первом параграфе «Понятие компьютерной информации» анализируется предмет преступлений в сфере компьютерной информации. В связи с тем, что нормы УК РФ базируются на нормах федеральных законов, регламентирующих отношения, связанные с использованием информации и информационных технологий, анализ этих законов проведен в первом параграфе диссертационного исследования. Прежде всего, это Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Тем не менее, в соответствии с УК РФ не вся компьютерная информация подлежит уголовно-правовой защите. Основным требованием, предъявляемым к такой информации, применительно к нормам уголовного закона, является то, что такая информация должна быть ограничена в доступе. Все тайны, составляющие информацию с ограниченным доступом, опираясь на триаду «личность, общество, государство», можно разделить на три категории: личная тайна; семейная тайна, коммерческая тайна, профессиональные тайны; государственная и служебная тайны.

В диссертации приведены примеры конкретных проблем, возникающих из-за расширительного и не вполне корректного толкования понятия компьютерной информации как предмета рассматриваемых преступлений. Так, в течение последних лет правоприменительные органы

исходят из того, что программа для ЭВМ, записанная на машинный носитель, является компьютерной информацией, поэтому неправомерный доступ к программе на машинном носителе квалифицируется как доступ к «информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети» по статье 272 УК РФ. По мнению автора, подобная правоприменительная практика не соответствует действующему законодательству. Программа для ЭВМ является объектом авторского права, и незаконные действия по отношению к ней не являются неправомерным доступом к компьютерной информации в смысле статьи 272 УК РФ, а должны квалифицироваться по статье 146 УК РФ (Нарушение авторских и смежных прав).

Во втором параграфе «Понятие и виды преступлений в сфере компьютерной информации» рассматриваются различные подходы к пониманию преступлений в сфере компьютерной информации, их соотношение с понятием компьютерных преступлений, киберпреступлений, преступлений в сфере высоких технологий.

В 2000 году американские ученые провели глобальное исследование уголовного законодательства 52 стран и пришли к выводу, что в тех странах, в которых предусмотрены преступления, совершаемые в «информационном пространстве» (cyberspace), можно выделить 10 видов таких преступлений, объединенных в четыре категории:

1. преступления, связанные с информацией, включая ее перехват, модификацию и кражу;
2. преступления, связанные с компьютерными сетями, включая вмешательство в их работу и саботаж;
3. преступления, связанные с доступом, включая хакерство и распространение вирусов; а также
4. преступления, связанные с использованием компьютеров, включая оказание помощи и соучастие в преступлении, компьютерное мошенничество и компьютерный подлог.

Принимая во внимание результаты научных исследований и законодательную практику различных государств, а также международного сообщества, к числу компьютерных преступлений можно отнести преступления в сфере компьютерной информации и преступления, совершаемые с использованием информационных технологий.

В зависимости от объекта и предмета посягательства все компьютерные преступления, предусмотренные как в российском, так и зарубежном уголовном праве, можно разделить на две группы:

1. Преступления в сфере компьютерной информации. Предметом в таких преступлениях выступает компьютерная информация, как, например, в деяниях, предусмотренных статьями 272-274 УК РФ, статьями 361-363 УК Украины, §1030 (a)(1) Свода Законов США «Несанкционированный доступ к информации с ограниченным доступом, касающейся национальной безопасности, международных отношений, атомной энергетики», статьей 478.1 УК Австралии «Несанкционированный доступ или модификация охраняемой компьютерной информации или программы» и рядом других.

2. Преступления, где компьютерная информация является орудием или средством совершения другого преступления. Эти составы преступлений находятся в других главах уголовных кодексов, к примеру, в статье 212 УК Республики Беларусь «Хищение путем использования компьютерной техники»; §1030(a)(7) Свода Законов США «Вымогательство, угрозы причинения вреда с использованием компьютера»; статье 206(1)(e) УК Канады «Использование компьютерных данных и технологий в целях извлечения прибыли путем создания финансовых пирамид» и других. Применительно к УК РФ, ответственность за преступления этой группы должна наступать по иным статьям Кодекса в соответствии с их родовым и непосредственным объектами. Однако такие деяния в необходимых случаях могут квалифицироваться по совокупности с преступлениями, предусмотренными статьями 272-274 УК РФ.

В данном параграфе приведены обширные статистические данные, касающиеся преступлений в сфере компьютерной информации в России.

Вторая глава «Уголовная ответственность за преступления в сфере компьютерной информации в российском и зарубежном праве» состоит из четырех параграфов.

Первый параграф главы посвящен рассмотрению и сравнительно-правовому анализу такого состава преступления как неправомерный доступа к компьютерной информации (статья 272 УК РФ).

Исходя из формулировки диспозиции части 1 статьи 272 УК РФ, выделяется три обязательных признака объективной стороны содержащегося в ней состава преступления: общественно опасное действие (неправомерный доступ); общественно опасные последствия (уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети); причинная связь между совершенным деянием и наступившими последствиями. Отсутствие хотя бы одного из этих признаков означает отсутствие данного состава преступления и уголовной ответственности.

В соответствии со статьей 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» доступ к информации определяется как возможность получения информации и ее использования. Таким образом, полномочия по ограничению либо разрешению доступа к информации являются существенными полномочиями ее обладателя. Неправомерность доступа к компьютерной информации означает, во-первых, что виновный нарушает порядок доступа к информации, установленный законом или обладателем информации. Во-вторых, виновный получает возможность получить компьютерную информацию и использовать ее без согласия законного обладателя.

В зарубежном и международном уголовном законодательстве при описании сходных составов преступлений употребляется термин «несанкционированный доступ». На взгляд автора, данный термин является более точным для характеристики запрещенного уголовным законом действия, поскольку правомерность доступа к информации фактически означает его санкционированность (разрешенность) обладателем информации.

Выделяется несколько способов неправомерного доступа к компьютерной информации: способы непосредственного доступа; способы опосредованного (удаленного) доступа; смешанные способы доступа. Во всем мире доля преступных деяний, совершаемых путем удаленного доступа к ЭВМ, системе или компьютерной сети, в общем числе компьютерных преступлений продолжает неуклонно расти и составляет по оценкам специалистов примерно 39,2%.²

Приведенные в работе примеры из судебной практики, показывают, что незаконное подключение к сети Интернет следственными и судебными органами часто квалифицируется как преступление по статье 272 УК РФ с использованием удаленного доступа. При подключении к сети Интернет происходит использование чужого имени пользователя и пароля, поэтому считается, что этот доступ является неправомерным. В то же время, многие авторы, исследовавшие эту проблему, не согласны с подобным подходом в правоприменительной практике, и эта позиция разделяется и автором диссертационного исследования. В подобных случаях незаконное подключение к сети Интернет приводит к изменению статистической информации в биллинговой системе. Биллинговая система (т.е. автоматизированная система расчетов) представляет собой программно-аппаратный комплекс, предназначенный для учета потребления услуг связи, управления расчетами за такие услуги, управления самими услугами

² Голубев В.А., Головин А.Ю. Проблемы расследования преступлений в сфере использования компьютерных технологий // www.crime-research.org/articles

одновременно с хранением информации об абонентах, которым оператор связи оказывает эти услуги. Исследуя объективные характеристики таких деяний, автор приходит к выводу, что непосредственного изменения информации в информационной системе оператора связи не происходит (подобная цель незаконно подключающимися к сети Интернет лицами и не ставится), а изменение данных производилось самой автоматизированной системой учёта в штатном режиме. Сама по себе автоматизированная система не может определить, правомерно или нет тот или иной субъект ввел данные абонента.

Таким образом, в официальную статистику преступности в сфере компьютерной информации включаются случаи не вполне корректного применения правоприменительными органами уголовного закона, свидетельствующие о расширительном толковании элементов состава преступления, предусмотренного статьи 272 УК РФ, а также недостаточном непонимании технических условий функционирования телекоммуникационных сервисов.

В первом параграфе приводятся примеры и дается анализ новых способов совершения неправомерного доступа к компьютерной информации с использованием беспроводных сетей связи Wi-Fi, технологии Bluetooth.

В работе обосновывается позиция, что действующая формулировка состава преступления, содержащегося в части 1 статьи 272 УК РФ, как материального является недостаточной для обеспечения защиты компьютерной информации от несанкционированного доступа в полном объеме, приводятся примеры из уголовных законов зарубежных стран, предлагается новая редакция этой статьи Кодекса.

Во *втором параграфе* главы рассматривается состав преступления, предусмотренный статьей 273 УК РФ - создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушение работы ЭВМ, системы ЭВМ или их

сети, а равно использование либо распространение таких программ или машинных носителей с такими программами.

На сегодняшний день наиболее распространенными видами вредоносных программ являются: компьютерные вирусы, троянские программы, сетевые черви. В диссертационном исследовании анализируются способы и возможные общественно опасные последствия их использования с примерами из российской и зарубежной судебной практики, приводятся аналогичные нормы зарубежного уголовного законодательства.

В диссертации обращается внимание на новую преступную деятельность, совершаемую с использованием вредоносных программ. Это создание так называемых «зомбированных сетей» (bot-net). Зомби-компьютеры представляют собой зараженные компьютеры, предоставляющие неограниченный доступ для неавторизованных и удаленных пользователей (хакеров), позволяя им рассылать с зараженных компьютеров спам или осуществлять скоординированные Dos-атаки на различные интернет-сайты или информационные системы. По оценкам специалистов, в настоящее время более 50% всего спама рассылается при помощи зомби-сетей. В 2007 г. количество зомби-компьютеров выросло на 29% по сравнению с 2006 г., составив около 6 млн., а численность контролируемых их серверов, наоборот, снизилась примерно на 25% (до 4700).³

Примером первого (и пока единственного) приговора в России за распространение спама является «дело Челябинского спамера», осужденного по статье 273 УК РФ. Правильность применения в этом случае данной уголовно-правовой нормы является спорной, как с точки зрения теоретической, так и практической. Некоторые авторы считают, что за распространение спама можно привлекать к уголовной ответственности по статье 274 УК РФ, другие с этой позицией не соглашаются. Кроме того, в последнее время в теории и практике ведется дискуссия о наличии

³ www.computerra.ru/news/311340

достаточной степени общественной опасности такого явления как спам, чтобы можно было это деяние криминализировать путем внесения соответствующих дополнений в главу 28 УК РФ. Автор считает, что распространение спама само по себе не может быть признано уголовно-наказуемым деянием.

Третий параграф главы посвящен анализу статьи 274 УК РФ, которая устанавливает уголовную ответственность за нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред.

Среди преступлений в сфере компьютерной информации данное преступление является наименее распространенным. Об этом говорят данные официальной статистики преступности, в том числе количество возбужденных уголовных дел: количество фактов совершения иных преступлений из главы 28 УК РФ превышает соответствующие показатели по статье 274 во много раз. В уголовных законах ряда стран СНГ и Прибалтики, как и многих других европейских государств, вообще не предусмотрено такое преступление как нарушение правил эксплуатации ЭВМ (например, в Великобритании, США, Японии, Казахстане, Эстонии и других).

С объективной стороны рассматриваемое преступление состоит в нарушении правил эксплуатации ЭВМ, их системы или сети, т.е. в неисполнении либо в ненадлежащем исполнении правил, которыми должно руководствоваться лицо, имеющее доступ к ЭВМ. Нарушение правил может быть совершено как в форме действия, так и бездействия, например, выражаться в несоблюдении правил, установленных для обеспечения нормального функционирования ЭВМ. Существуют два вида таких правил: 1) правила, которые разрабатываются изготовителями ЭВМ и поставляются вместе с ЭВМ; 2) правила, которые устанавливаются владельцем информации или оператором информационных систем. Установленные

правомочным субъектом правила должны доводиться до сведения лиц, работающих за компьютерами. По смыслу статьи 274 УК РФ при наличии нормативных документов любого уровня, устанавливающих определенные правила эксплуатации ЭВМ, их системы или сети, их нарушение влечет за собой уголовную ответственность по данной статье Кодекса. Именно это является одной из причин, почему данная статья «не работает»: далеко не во всех организациях имеются такие правила. Кроме того, практически никто при приеме на работу не знакомится с ними, что подтверждается изучением автором оснований отказов в возбуждении уголовных дел по рассматриваемой статье в УСТМ ГУВД г.Москвы. Поэтому нельзя вменить в вину нарушение каких-либо правил, если лицо даже не знало об их существовании.

В качестве еще одной из причин неэффективности статьи 274 УК РФ отмечается конструкция состава содержащегося в ней преступления, когда наступление определенных в законе последствий, в свою очередь, должно причинять существенный ущерб, чтобы содеянное стало уголовно наказуемым.

В этой связи автором предлагается исключить статью 274 УК РФ в ее действующей редакции и заменить ее новой нормой, содержащей ответственность за нарушение работы информационной системы или информационно-телекоммуникационной сети, блокирование доступа к какой-либо информации, информационной системе или информационно-телекоммуникационной сети.

В четвертом параграфе главы проводится сравнительно-правовой анализ наказуемости преступлений в сфере компьютерной информации. На взгляд автора, российским законодателем предусмотрены весьма мягкие санкции за совершение преступлений в сфере компьютерной информации, принимая во внимание, к примеру, какими серьезными могут быть последствия неправомерного доступа к такой информации не только для какой-либо компании, но и для национальной безопасности. Но подобная

мягкость санкций характерна не только для России, что подтверждается примерами из зарубежного законодательства.

Третья глава «Международное сотрудничество в борьбе с компьютерными преступлениями» посвящена изучению и анализу основных направлений и тенденций международного сотрудничества в сфере борьбы с компьютерными преступлениями и состоит из двух параграфов.

Значительная доля преступлений в сфере компьютерной информации совершается с использованием информационно-телекоммуникационных сетей, что является одной из причин активного международного сотрудничества различных стран в борьбе с данным видом преступности. Наиболее плодотворная деятельность с выработкой действенных международных механизмов (применимых и для Российской Федерации) проводится в рамках Организации экономического сотрудничества и развития (ОЭСР), Интерпола, Группы Восьми (G 8), Совета Европы, ООН, СНГ.

В рамках такого сотрудничества можно выделить два основных направления:

- 1) определение понятия «компьютерное преступление» и выделение видов таких преступлений;
- 2) выработка согласованных мер по борьбе с такими преступлениями.

В первом параграфе приводится историческая справка по вопросу выработки необходимых понятий («компьютерное преступление», «преступление в сфере компьютерной информации», «киберпреступление») и выделении категорий таких преступлений. Рассмотренные основные международные документы наглядно показывают, как менялись понятийный аппарат и содержательное наполнение компьютерных преступлений. Можно сказать, что в соответствии с международными нормами к компьютерным преступлениям относится весьма широкий спектр деяний, включая и преступления в сфере компьютерной информации в строгом смысле этого

слова. Однако не все эти деяния были восприняты в национальных уголовных законах (так, в УК РФ лишь часть таких деяний отнесена к уголовно-наказуемым).

В марте 2001 года был представлен доклад Комиссии по предупреждению преступности и уголовному правосудию ООН, в котором все компьютерные преступления были классифицированы следующим образом:

1) Преступления, совершаемые против технологий и их пользователей, - несанкционированный доступ к компьютерам или информационным системам; несанкционированное использование информационных систем; несанкционированное прочитывание, копирование и использование данных; создание и распространение вредоносных программ; компьютерный вандализм или саботаж.

2) Традиционные преступления, совершаемые с использованием компьютерных или коммуникационных технологий, - преступления, связанные с информацией незаконного содержания; похищение человека с использованием сети Интернет; мошенничество; коммерческий или промышленный шпионаж; преступления, связанные с нарушением прав интеллектуальной собственности; игорный бизнес; легализация средств, полученных преступным путем.

3) Использование компьютерных технологий для поддержки другой преступной деятельности.

Рост компьютерной преступности, включая преступления в сфере компьютерной информации, и необходимость согласованного подхода государств к выработке уголовно-правовых и уголовно-процессуальных процедур, направленных на борьбу с ней, привели к созданию в 1997 году Комитетом Министров Совета Европы Комитета экспертов по преступности в киберпространстве. По результатам этой работы в 2000 году был разработан проект Конвенции Совета Европы по киберпреступности. Конвенция была открыта к подписанию до 23 ноября 2001 году в Будапеште

и вступила в силу 18 марта 2004 году. По состоянию на 7 апреля 2007 года Конвенцию ратифицировали 19 государств.⁴

Европейская Конвенция по киберпреступности является комплексным документом, содержащим нормы различных отраслей права: уголовного, уголовно-процессуального, авторского, гражданского, информационного.

В Конвенции не дается определения понятия «компьютерное преступление» или «преступление, связанное с использованием компьютерных технологий», которые использовались в принятых ранее международных документах. В документе используется понятие «киберпреступление», содержание которого раскрывается с помощью перечня, включающего в себя:

1) деяния, направленные против компьютерной информации (как предмета преступного посягательства),

2) деяния, посягающие на иные охраняемые законом блага, при этом информация, компьютеры и т.д. являются одним из элементов их объективной стороны, выступая в качестве, к примеру, орудия их совершения либо составной части способа их совершения или сокрытия.

В ноябре 2005 года Президент Российской Федерации поручил МИД России подписать Конвенцию Совета Европы по киберпреступности 2001 года.

Признавая ценность Конвенции Совета Европы как международного механизма, способствующего гармонизации законодательства европейских стран, многие российские эксперты, однако, считали, что ряд положений Конвенции содержат иные правила, чем предусмотренные российским законодательством. Это касается, в частности, предоставления трансграничного доступа к хранящейся компьютерной информации с соответствующего согласия ее обладателя или к общедоступной

⁴ Албания, Армения, Босния и Герцеговина, Болгария, Хорватия, Кипр, Дания, Эстония, Франция, Югославия, Исландия Литва, Нидерланды, Норвегия, Румыния, Словения, Македония, Украина, США.

См. текст: www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm

информации. Российские правоохранительные органы посчитали, что пункт б статьи 32 Конвенции при определенных условиях позволяет правоохранительным органам одного государства-участника Конвенции проводить оперативно-розыскную деятельность на территории другого государства-участника без его согласия, что рассматривается как угроза национальной безопасности, и вмешательство во внутренние дела страны. С учетом этого обстоятельства, а также того, что до момента решения Россией вопроса о подписании и ратификации Конвенции ни одно государство Группы Восьми ее не ратифицировало Конвенцию (в январе 2006 года ее ратифицировала Франция, затем в сентябре 2006 года США), было сочтено возможным ограничиться пока подписанием Конвенции и определиться с ее ратификацией позже. При этом в соответствии с Конвенцией, к ней нельзя делать оговорки. Исходя из этого, Россия должна была подписать Конвенцию с заявлением об ограничении ее действия Конвенции. Однако по состоянию на 1 апреля 2007 года МИД России указанную Конвенцию не подписал.

Учитывая, что обеспечение международного сотрудничества невозможно без согласованных норм уголовного права в отношении компьютерных преступлений, а также без выработки универсальных согласованных процедур взаимодействия правоохранительных органов при расследовании таких преступлений, автором высказывается мнение о необходимости скорейшего присоединения России к Конвенции Совета Европы по киберпреступности.

Во втором параграфе главы проводится анализ процесса выработки согласованных мер по борьбе с компьютерными преступлениями.

На Десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями в 2000 году отмечалось, что быстрое распространение новых информационных технологий сопровождается их использованием в преступных целях и неспособностью государств и иных организаций справиться с возрастающим количеством юридических проблем как национального, так и международного характера. Особо подчеркивалось,

что расширение и усиление международного сотрудничества в области предупреждения преступлений, связанных с использованием информационных технологий, и борьбы с ними будут способствовать обнаружению, преследованию и задержанию правонарушителей и тем самым повысят эффективность деятельности государств-членов, направленной на борьбу с различными формами транснациональной преступности, связанной с быстрым распространением новых информационных технологий.

Страны-участницы Тунисского этапа Всемирной встречи на высшем уровне по вопросам информационного общества в конце 2005 года призвали правительства в сотрудничестве с другими заинтересованными сторонами разработать необходимое законодательство, предусматривающее проведение расследований и уголовное преследование компьютерных преступлений, используя существующую нормативную базу, например резолюции 55/63 и 56/121 Генеральной Ассамблеи ООН о борьбе с преступным использованием информационных технологий и, особенно, Конвенцию Совета Европы по киберпреступности.

На сегодняшний день при выработке согласованных мер противодействия компьютерным преступлениям особое внимание на международном уровне уделяется следующим вопросам:

- 1) обнаружение и идентификация нарушителя, совершившего компьютерное преступление;
- 2) получение доступа к содержанию передаваемых сообщений;
- 3) международное сотрудничество в области сбора доказательств и помощь в случае, если сотруднику правоохранительных органов из одной страны требуется доступ к компьютеру в другой стране для получения доказательств (т. е. «трансграничные оперативно-розыскные мероприятия»);
- 4) налаживание сотрудничества между государственными органами и соответствующими заинтересованными представителями бизнес сообщества (например, интернет-провайдерами).

Группой Восьми в 2000 году был принят План действий из 10 основополагающих пунктов по противодействию компьютерной преступности, который, среди иных мер, предусматривал рассмотрение вопросов, связанных с компьютерной преступностью, при подготовке соглашений о правовой помощи, а также рассмотрение методов сохранения электронных доказательств и их представления в рамках иностранного уголовного судопроизводства и установление судебных и других технических стандартов в отношении обеспечения информационной безопасности и использования электронных доказательств в ходе судебного разбирательства.

В этой связи в диссертации рассматривается проблема сохранения данных о трафике как электронных доказательств совершения преступления. В случае расследования компьютерного преступления оперативное сохранение и раскрытие таких данных может потребоваться для прослеживания маршрута сообщения, для сбора дополнительных доказательств и выявления подозреваемого, прежде чем эти данные будут удалены. Обычных процедур сбора и раскрытия компьютерных данных иногда недостаточно. Приводятся примеры из международного и зарубежного законодательства в области обеспечения сохранности электронных доказательств, требований к интернет-провайдерам, механизмов взаимодействия правоохранительных органов разных государств.

В **заключении** диссертационного исследования автором подводятся итоги работы, формулируются основные выводы, сделанные в ходе исследования.

Основные положения диссертации опубликованы в следующих работах:

1. Зинина У.В. Федеральный закон «О персональных данных»: принципы регулирования и механизмы реализации//Хозяйство и право. 2007 г. № 3 (0,8 п.л.).
2. Зинина У.В. Готовится Закон о персональных данных//Главная книга. 2005 г. № 20 (0,3 п.л.).
3. Зинина У.В. Международное сотрудничество в сфере борьбы с компьютерными преступлениями//Право и безопасность. 2005 г. № 3 (0,75 п.л.).
4. Зинина У.В. Проблемы борьбы с преступлениями в сфере компьютерной информации в России//Молодежь в юридической науке. Выпуск пятый. М.: Академический правовой университет. 2004 г. (0,4 п.л.).
5. Зинина У.В. Проблемы борьбы с киберпреступностью/Проблемы эффективности борьбы с преступностью в России (материалы научно-практической конференции)//Государство и право. 2003 г. № 11 (0,1 п.л.).
6. Зинина У.В. Международное сотрудничество в сфере борьбы с компьютерными преступлениями//Молодежь в юридической науке. Выпуск четвертый. М.: Академический правовой университет. 2003 г. (0,5 п.л.).