содержание

[Введение 3](#_Toc224484452)

[Глава 1. Компьютерные преступления: исторические и теоретические аспекты 7](#_Toc224484453)

[1.1. Эволюция уголовной ответственности за компьютерные преступления 7](#_Toc224484454)

[1.2. Понятие и общая характеристика компьютерных преступлений 11](#_Toc224484455)

[1.3. Проблемы классификации компьютерных преступлений 14](#_Toc224484456)

[Глава 2. Отдельные виды компьютерных преступлений 19](#_Toc224484457)

[2.1. Неправомерный доступ к компьютерной информации (ст.272 УК РФ) 19](#_Toc224484458)

[2.2. Создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ) 25](#_Toc224484459)

[Заключение 31](#_Toc224484460)

[Список использованной литературы 34](#_Toc224484461)

# Приложение 38ВВЕДЕНИЕ

В связи с социально-экономическими изменениями, произошедшими в России в конце XX в., переходом к информационному обществу, появился новый вид общественных отношений – отношения в области обращения информации. Информация стала одним из необходимых элементов жизни общества. Разные ее виды проникли практически во все сферы общественной жизни.

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.

Быстрота развития информационных технологий требует динамичности законодательства. Уголовное законодательство должно отражать изменения видов преступлений в сфере компьютерной информации, способов их совершения, а также современное состояние развития информационных технологий и соответствующего отраслевого законодательства. 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.

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.

В 2006 году, как и в 2005 году, число компьютерных преступлений в России составило 14 тыс. В 2007 году число зарегистрированных преступлений данного вида сократилось на 14,3%, хотя и продолжает оставаться весьма высоким — 12 тысяч. Треть совершенных в 2007 году компьютерных преступлений подпадают под действие ст. 272 Уголовного кодекса Российской Федерации (далее – УК РФ)[[1]](#footnote-1) («Неправомерный доступ к компьютерной информации»). В 2008 году в российском киберпространстве было совершено на две тысячи преступлений больше, чем годом ранее, а общее число правонарушений в Интернете превысило 14 тысяч[[2]](#footnote-2).

Только в сфере компьютерной информации количество зарегистрированных преступлений в 2005 году составило – 10214, в 2006 году – 8889, в 2007 году – 6763, в 2008 году – 9010 (Приложение)[[3]](#footnote-3).

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 главой 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.

Повышенная уязвимость информационной сферы обуславливает необходимость перманентного совершенствования уголовного законодательства в данной области, практики его применения, совершенствования организационно-правовых мер предупреждения и пресечения компьютерных преступлений.

Наибольшую общественную опасность в настоящее время представляют преступления, предусмотренные ст. 272 УК РФ, то есть неправомерный доступ к компьютерной информации. Однако норма, предусмотренная ст. 274 УК РФ (нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети), не находит применения на практике. За это время произошли как социально-экономические, так и научно-технические перемены. Как в теории, так и в практике применения ст. 272–274 УК РФ выявились значительные противоречия. Среди основных их причин можно выделить следующие: не совсем удачные конструкции норм о преступлениях в сфере компьютерной информации, неверное их толкование, не соответствующее действительности представление о значении указанных норм в охране общественных отношений.

Уголовно-правовые и криминологические аспекты компьютерных преступлений получили развитие в общетеоретических работах в области уголовного права и криминологии: трудах Ю.М.Батурина, Н.И.Ветрова, В.Б.Вехова, А.Г.Волеводза, Ю.В.Гаврилина, В.А.Голубева, А.Э.Жалинского, У.В.Зининой, В.Е.Козлова, А.Н. Копырюлина, В.Н.Кудрявцева, Н.Ф.Кузнецовой, Т.М.Лопатиной, 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. Однако требуется дальнейшая теоретическая разработка, так как не достаточно полно в юридической литературе освящена проблема определения понятия и классификации компьютерных преступлений.

С учетом всех этих обстоятельств анализ соответствия действующих норм об ответственности за преступления в сфере компьютерной информации современному законодательству и практике представляется весьма актуальным.

Объектом исследования является совокупность общественных отношений, складывающихся в сфере уголовно-правовой защиты компьютерной информации.

Предмет исследования включает уголовно-правовая характеристика компьютерных преступлений и их классификация.

Методологическую основу исследования составляет совокупность общенаучных и частно-научных методов. В числе общенаучных методов были использованы: диалектический метод, метод анализа и синтеза составных частей, логический метод. Применялись также и специальные методы: сравнительного правоведения, исторический.

Цель исследования заключаются в выяснении уголовно-правовой природы преступлений в сфере компьютерной информации, а также проблемы классификации компьютерных преступлений.

Достижение указанной цели обеспечивается решением задач:

– рассмотрение исторических аспектов развития уголовной ответственности за компьютерные преступления;

– определение понятия компьютерных преступлений и краткая характеристика преступлений в сфере компьютерной информации;

– анализ проблемы компьютерных преступлений;

– раскрытие объективных и субъективных признаком преступлений, предусмотренных главой 28 УК РФ, а также особенностей их квалификации.

Теоретической базой исследования явились труды видных ученых в области уголовного права и криминологии: труды У.В.Зининой, Н.Г.Кадникова, А.Н.Копырюлина, Л.Л. Кругликова, Т.М. Лопатиной, Е. Маслаковой, А.И. Рарога и др.

Структура работы определяется целями и задачами исследования, спецификой рассматриваемой проблемы и внутренней логикой подхода к изучению. Курсовая работа состоит из введения, двух глав, пяти параграфов, заключения и списка использованной литературы.

# ГЛАВА 1. КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ: ИСТОРИЧЕСКИЕ И ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ

## 1.1. Эволюция уголовной ответственности за компьютерные преступления

До 1 января 1997 г. – даты вступления в действие нового УК РФ, в России отсутствовала возможность эффективно бороться с неправомерным доступом к компьютерной информации. Несмотря на явную общественную опасность, данное посягательство не было противозаконным, то есть не упоминалось нашим уголовным законодательством. Ситуация, сложившаяся в обществе, потребовала разработки норм уголовного права, которые предусматривали бы ответственность за совершение компьютерных преступлений. Основным средством борьбы с преступными нарушениями нормального функционирования компьютерной техники должно было стать уголовное законодательство.

Непосредственно законодательство России в области информатизации начало формироваться с 1991 г. и включало до 1997 г. десять основных законов, где определяются основные термины и понятия в области компьютерной информации (например, такие, как компьютерная информация, программа для ЭВМ, ЭВМ (компьютер), сеть ЭВМ, база данных), регулируются вопросы ее распространения, охраны авторских прав, имущественные и неимущественные отношения, возникающие в связи с созданием правовой охраной и использованием программного обеспечения и новых информационных технологий[[4]](#footnote-4).

Первой попыткой решить обозначенную проблему стала разработка в 1991 г. 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. Прорывом в этом направлении правотворчества явилось принятие Верховным Советом России 23 сентября 1992 г. Закона «О правовой охране программ для электронных вычислительных машин и баз данных»[[5]](#footnote-5), 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 г. принимается в общей сложности около 60 актов Верховного Совета России, Президента и Правительства в данной области, а в 1993 г. – уже более 100[[6]](#footnote-6).

В 1994 г. 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 УК РФ преступлений в области компьютерной информации.

В январе – феврале 1995 г. 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[[7]](#footnote-7).

Важное место в ряду нормативных правовых актов в области информационного права занял Федеральный закон от 20 февраля 1995 г. «Об информации, информатизации и защите информации»[[8]](#footnote-8), давший определение многих терминов данной сферы деятельности. Этот Закон подготовил правовое поле для принятия нового уголовного законодательства. По отдельным подсчетам, за период с 1992 по июль 1995 г. 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 г. был принят Модельный уголовный кодекс государств – участников СНГ, содержавший нормы об ответственности за компьютерные преступления.

Таким образом, до 1 января 1997 г. на уровне действующего законодательства России не получили достойного отражения в законодательстве права граждан на доступ к информации и защита информации, то есть то, что напрямую связано с компьютерными преступлениями и непосредственно с неправомерным доступом к компьютерной информации.

Первое преступление, совершенное на территории СССР с использованием компьютера, официально зарегистрировано в 1979 г. в г. Вильнюсе. Данный факт явился своеобразной отправной точкой в развитии нового вида преступности в нашей стране. Одновременно начался поиск путей уголовно-правового регулирования вопросов ответственности за совершение таких преступлений[[10]](#footnote-10).

С 1 января 1997 г. был введен в действие УК РФ, 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».

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.). 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[[11]](#footnote-11).

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.

## 1.2. Понятие и общая характеристика компьютерных преступлений

Компьютерные преступления – чрезвычайно многогранные и сложные явления. Законодательное определение компьютерных преступлений в УК РФ отсутствует. Глава 28 УК РФ именуется «Преступления в сфере компьютерной информации». В учебной литературе по уголовному праву приводится определение преступлений в сфере компьютерной информации как равнозначное компьютерным преступлениям: «Преступления в сфере компьютерной информации (компьютерные преступления) – это запрещенные уголовным законом виновные посягательства на безопасность в сфере использования компьютерной информации, причинившие существенный вред или создавшие угрозу причинения такого вреда личности, обществу или государству»[[12]](#footnote-12).

Некоторые правоведы считают, что компьютерные преступления представляют собой все преступления, при котором компьютер является орудием, средством или целью их совершения, а другие объединяют под этим термином все противозаконные действия, которые причиняют ущерб имуществу и связаны с электронной обработкой информации. Ю.М. Батурин считает, что компьютерных преступлений как особой группы преступлений в юридическом смысле не существует, однако при этом отмечает, что многие традиционные виды преступлений модифицировались из-за вовлечения в них вычислительной техники и поэтому правильнее было бы говорить лишь о компьютерных аспектах преступлений, не выделяя их в обособленную группу[[13]](#footnote-13). Другого, более определенного взгляда придерживается А.Н. Караханьян. Под компьютерными преступлениями он понимает противозаконные действия, объектом или орудием совершения которых являются электронно-вычислительные машины[[14]](#footnote-14).

Что касается определения преступлений в сфере компьютерной информации, то, надо сказать, таких определений достаточно, хотя между ними существуют и определенные отличия. Так, по мнению Н.Г.Кадникова, преступление в сфере компьютерной информации — это предусмотренное уголовным законом виновное нарушение чужих прав и интересов в сфере автоматизированной обработки данных, совершенное во вред подлежащим правовой охране правам и интересам физических и юридических лиц, общества и государства (личные права и неприкосновенность частной сферы, имущественные права и интересы, общественная и государственная безопасность, конституционный строй)[[15]](#footnote-15).

Через предмет посягательства определяет преступления в сфере компьютерной информации А.И.Рарог. Преступления в сфере компьютерной информации – это общественно опасные посягательства, предметом которых является информация, закрепленная на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети (компьютерная информация)[[16]](#footnote-16).

Таким образом, преступлениями в сфере компьютерной информации следует считать виновно совершенные общественно опасные деяния, посягающие на нормальный порядок обращения охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания.

Родовым объектом компьютерных преступлений являются общественные отношения в сфере обеспечения безопасности использования автоматизированных систем обработки данных, нормальных прав и интересов лиц, общества и государства, активно пользующихся электронно-вычислительной техникой. Непосредственный объект — это конкретные права и интересы по поводу использования таких систем (право владельца системы на неприкосновенность содержащейся в ней информации, заинтересованность в правильной эксплуатации системы). Предметом компьютерных преступлений является автоматизированная система обработки данных, включающая получение информации, полезной для физических и юридических лиц.

Объективная сторона представляет собой деяние в виде действий или бездействия, сопряженного с нарушением прав и интересов в части пользования компьютерными системами во вред личным правам или государственным интересам[[17]](#footnote-17).

Большинство компьютерных преступлений сконструированы как материальные составы, то есть предусматривают наступление общественно опасных последствий в виде вреда, наносимого правам и интересам пользователя ЭВМ — личности, обществу или государству.

Субъективная сторона характеризуется умышленной виной (прямым или косвенным умыслом). Виновный сознает, что незаконно совершает действия (бездействие), связанные с использованием компьютерной информации, предвидит возможность или неизбежность наступления вреда для гражданина, общества или государства и желает (не желает, но сознательно допускает) наступление этих последствий.

Субъектом преступлений признается вменяемое лицо, достигшее 16 лет (в ст. 274 и в ч. 2 ст. 272 УК РФ субъект — специальный). Субъекты могут быть подразделены на две группы: а) лица, имеющие доступ к ЭВМ, системе ЭВМ или их сети и осуществившие неправомерный доступ к охраняемой законом компьютерной информации, и б) лица, не имеющие права доступа к ЭВМ, системе ЭВМ или их сети и при этом также осуществившие неправомерный доступ к охраняемой законом компьютерной информации. При этом доступ должен рассматриваться не в фактическом понимании, а в уголовно-правовом как умышленные целенаправленные деяния на завладение охраняемой законом компьютерной информацией[[18]](#footnote-18).

На наш взгляд, заслуживает внимания вопрос о возрасте субъекта компьютерных преступлений. Как известно, за все преступления в сфере компьютерной информации уголовная ответственность установлена с 16 лет. Вместе с тем зависимость роста числа рассматриваемых общественно опасных деяний от увеличения численности парка ЭВМ и роста общего количества пользователей ЭВМ, систем ЭВМ или их сети позволяет предложить законодателю снизить возраст уголовной ответственности. Полагаем, если не за все компьютерные преступления, то, по крайней мере, за создание, использование и распространение вредоносных программ для ЭВМ уголовной ответственности должны подлежать лица, достигшие ко времени совершения преступления 14 лет.

Итак, преступление в сфере компьютерной информации – это противоправное, виновно совершенное, наказуемое в уголовном порядке общественно опасное деяние, причиняющие вред либо создающие угрозу причинения вреда общественным отношениям по законному использованию компьютерной информации.

## 1.3. Проблемы классификации компьютерных преступлений

Как известно, существенную помощь в исследовании какого-либо предмета оказывает проведение классификации этого предмета или явления. Значительный опыт уголовно-правовой классификации преступлений в сфере компьютерной информации, накоплен в ведущих промышленно развитых государствах мира. Одной из наиболее распространенных из существующих классификаций преступлений в сфере компьютерной информации является кодификатор рабочей группы Интерпола, который был положен в основу автоматизированной информационно-поисковой системы, созданной в начале 90-х годов. В соответствии с названным кодификатором все компьютерные преступления классифицированы следующим образом. В их число входят: 1) QA – несанкционированный доступ и перехват; 2) QD – изменение компьютерных данных; 3) QF – компьютерное мошенничество; 4) QR – незаконное копирование; 5) QS – компьютерный саботаж; 6) QZ – прочие компьютерные преступления (QZB – с использованием компьютерных досок объявлений; QZE – хищение информации, составляющей коммерческую тайну; QZS – передача информации, подлежащая судебному рассмотрению; QZZ – прочие компьютерные преступления). Данная классификация применяется при отправлении запросов или сообщений о компьютерных преступлениях по телекоммуникационной сети Интерпола. Одним из ее достоинств является введение литеры «Z», отражающей прочие виды преступлений и позволяющей совершенствовать и дополнять используемую классификацию.

Однако приведенная выше система классификации, как и ряд других, например, «минимальный» и «необязательный» списки нарушений «Руководства Интерпола по компьютерной преступности», страдают одним общим недостатком – в них происходит смешение уголовно-правовых начал и технических особенностей автоматизированной обработки информации, что приводит к неоднозначности толкования и еще большей неопределенности понятия «компьютерное преступление».

С учетом распространенности отдельных видов преступлений, совершаемых с использованием компьютерной информации, система компьютерных преступлений, по мнению В.А. Широкова и Е.В. Беспалова, может быть построена следующим образом: а) преступления против личности; б) преступления в сфере экономики; в) преступления против общественной безопасности, общественного порядка и общественной нравственности; г) преступления против безопасности государства[[19]](#footnote-19).

Следует заметить, что по статистике МВД РФ показатели компьютерной преступности превышают показатели преступности в сфере компьютерной информации, что дает право считать преступления в сфере компьютерной информации всего лишь подвидом компьютерных преступлений (см. Приложение).

Полагаем, ввиду малочисленности составов преступлений в сфере компьютерной информации попытки классифицировать эти преступления представляются пока преждевременными, хотя некоторые рекомендации по этому вопросу уже имеются. В литературе, например, предлагается подразделять компьютерные преступления на две группы: преступления, связанные с вмешательством в работу компьютеров, и преступные деяния, при которых компьютеры используются как технические средства совершения преступлений[[20]](#footnote-20).

Обе группы связаны с несанкционированным доступом к сетям, серверам, машинным ресурсам. Однако, первая категория включает те преступления, в рамках которых вмешательство в работу компьютеров, направлено на к повреждение или уничтожение информации, нарушение нормального их нормального функционирования. Наиболее яркий пример – вирусы. При совершении преступлений, отнесенных ко второй категории, компьютер выступает не объектом посягательства, а его средством, а целью является получение и использование информации, в том числе, и для совершения иных преступных деяний. Например, хищений денежных средств с банковских счетов. Необходимо отметить, что во многих случаях одно нарушение может иметь признаки преступлений, относящихся к обеим их категориям. С технической же точки зрения, подобные действия либо сводятся к так называемым «взломам», либо касаются вредоносных программ.

Любая классификация носит условный характер, ее цель – облегчить анализ рассматриваемых преступлений, но не более того. Классификация – естественный инструмент познания реальной действительности, своеобразный источник знания о ней, прием, с помощью которого множество наблюдаемых явлений подразделяется на основные группы, классы, виды, входящие в общую систему и составляющие единое целое. В процессе классификации каждый исследуемый объект получает определенную оценку (рейтинг). Именно поэтому перед исследователями рано или поздно встанет вопрос о необходимости классификации тех или иных явлений общественной жизни[[21]](#footnote-21).

Предлагаем следующую классификацию компьютерных преступлений:

I. Преступления в сфере компьютерной информации (неправомерный доступ к компьютерной информации (ст.272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

II. Преступления, совершаемые с использованием компьютера:

1. Компьютерные преступления против личности (ст. клевета (ст. 129 УК РФ) или оскорбление (ст. 130 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), отказ в предоставлении гражданину информации (ст. 140 УК РФ), нарушения избирательных прав или работы избирательных комиссий (ст. 141, 141.1, 142, 142.1 УК РФ), воспрепятствование законной профессиональной деятельности журналистов (ст. 144 УК РФ), нарушение авторских и смежных прав (ст. 146 УК РФ), нарушение изобретательских и патентных прав (ст. 147 УК РФ).

2. Компьютерные преступления в сфере экономики (кража, мошенничество, хищение предметов, имеющих особую ценность, умышленное уничтожение или повреждение имущества, заведомо ложная реклама, незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, изготовление и сбыт поддельных кредитных карт, незаконный экспорт технологий, научно-технической информации (ст. 158, 159, 164, 167, 182, 183, 187, 189 УК РФ).

3. Компьютерные преступления против общественной безопасности и общественного порядка (заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237 УК РФ), изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ) и др.).

4. Компьютерные преступления против государственной власти (государственная измена (ст. 275 УК РФ), шпионаж (ст. 276 УК РФ), разглашение государственной тайны (ст. 283 УК РФ) и др.).

Данная классификация является условной и не претендует на ее всеобщность.

В связи с ограниченным объемом в настоящей работе будут подвергнуты анализу только отдельные составы преступлений в сфере компьютерной информации.

# ГЛАВА 2. ОТДЕЛЬНЫЕ ВИДЫ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

## 2.1. Неправомерный доступ к компьютерной информации (ст.272 УК РФ)

Неправомерный доступ к компьютерной информации – это несанкционированное собственником или иным законным пользователем информации проникновение к ней, в том числе с возможностью ознакомления, которое позволяет распоряжаться этой информацией (уничтожать, блокировать, модифицировать и т.д.) и создает опасность как для самой информации, так и для интересов собственника или иного законного пользователя[[22]](#footnote-22).

Видовым объектом данного преступления являются общественные отношения в сфере безопасности компьютерной информации и нормальной работы ЭВМ, системы ЭВМ или их сети.

Предметом преступления выступает электронно-вычислительная техника как комплекс информационных средств, носитель информации.

Объективная сторона преступления выражается в неправомерном доступе к информации или информационным ресурсам, содержащимся на машинном носителе, в ЭВМ, системе ЭВМ или их сети.

По мнению А. Копырюлина, неправомерным доступом следует считать также и доступ к информационным ресурсам сети Интернет без согласия собственника или иного законного владельца информации, если это привело к уничтожению, блокированию, модификации или копированию информации, при обязательном условии отсутствия у лица права доступа к ней[[23]](#footnote-23). Однако, по нашему мнению, неправильно квалифицировать действия лица как неправомерный доступ к информации, если оно использует чужое сетевое имя и пароль доступа, поскольку основной массив информации в глобальной сети носит открытый характер, информация не запрещена к копированию. Таким образом, уголовно наказуемым данное деяние будет только при условии доступа к информации, охраняемой законом. Например, нормы ст. 183 УК РФ должны применяться, если виновный, имея умысел на собирание сведений, составляющих коммерческую тайну, при помощи незаконно полученных реквизитов доступа осуществляет копирование информации (баз данных, служебной документации и т.п.) с внутренней локальной сети коммерческой организации. При этом собирание сведений, составляющих коммерческую тайну, должно быть совершено с прямым умыслом, то есть виновный знает, что его действия направлены на получение сведений, составляющих коммерческую тайну, что искомая информация заведомо обладает всеми признаками коммерческой тайны и желает собрать именно такую информацию. Для обоснования сказанного обратимся к примеру из судебной практики.

Судебная коллегия по уголовным делам Верховного Суда РФ по делу № 69-о07-5 установила, что действия К. суд правильно квалифицировал по ч. 1 ст. 272 и ч. 1 ст. 273 УК РФ.

Органы предварительного следствия предъявили обвинение по ч. 1 ст. 272, ч. 1 ст. 273 и ч. 1 ст. 183 УК РФ инженеру-электронщику ООО «Электроприбор-Сервис» К., в служебные обязанности которого входила настройка серверов, подключение рабочих станций к локальной сети и регистрация пользователей. Согласно материалам дела, К. совершил неправомерный доступ к компьютерной информации, не имея соответствующего разрешения для работы с ней, посредством служебной ЭВМ, получив доступ к файловым системам в локальной сети, осуществил несанкционированное копирование на ЭВМ файлов, содержащих информацию об именах пользователей и паролях локальной сети завода. К. имел право использовать только сетевые ресурсы, предоставленные ему для выполнения служебных обязанностей. Доступ же к базам данных отдела кадров, экономического отдела был ограничен четко определенным кругом лиц, к которому К. не относился, то есть доступа на законных основаниях к указанной информации не имел.

Приговором суда К. был признан виновным по ч. 1 ст. 272 и ч. 1 ст. 273 УК РФ. Суд счел ч. 1 ст. 183 УК РФ вмененной излишне, исключил ее из обвинения и оправдал К. по ней за отсутствием в действиях состава преступления, поскольку умысел К. на сбор информации, составляющей коммерческую тайну, в ходе судебного следствия подтверждения не нашел[[24]](#footnote-24).

Защите подлежит любая документированная информация, неправомерное обращение с которой может нанести ущерб ее собственнику, владельцу, пользователю и иному лицу[[25]](#footnote-25).

Компьютерная информация — это сведения (данные) о лицах, предметах, фактах, событиях, явлениях и процессах, подлежащие вводу в ЭВМ, хранимые в ее памяти, обрабатываемые на ЭВМ и выдаваемые пользователем.

Машинный носитель информации — это техническое средство (комплекс технических средств), предназначенное для фиксации, хранения, обработки, анализа и передачи компьютерной информации пользователем. К машинным носителям информации можно отнести, например, основной микропроцессор, математический сопроцессор, гибкие магнитные диски (дискеты), жесткие магнитные диски (винчестеры) и др.

Под электронно-вычислительной машиной (ЭВМ) следует понимать комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач. Система ЭВМ — это совокупность взаимосвязанных и взаимодействующих процессоров или ЭВМ, периферийного оборудования и программного обеспечения, предназначенных для автоматизации процессов приема, хранения, обработки, поиска и выдачи информации потребителям по их запросам.

Способы неправомерного доступа к охраняемой законом компьютерной информации могут быть самыми разнообразными. Например, соединение с тем или иным компьютером, подключенным к телефонной сети, путем автоматического перебора абонентских номеров (внедрение в чужую информационную систему посредством «угадывания кода»), использование чужого имени (пароля) посредством использования ошибки в логике построения программы и др.

Средством совершения рассматриваемого преступления выступает компьютерная техника, то есть различные виды ЭВМ, аппаратные средства, периферийные устройства, а также линии связи, с помощью которых вычислительная техника объединяется в информационные сети[[26]](#footnote-26).

Состав данного преступления — материальный. Преступление считается оконченным с момента наступления хотя бы одного из альтернативно перечисленных в диспозиции ч. 1 ст. 272 УК РФ последствий: уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. В силу этого неправомерный доступ к охраняемой законом компьютерной информации является причиной, а наступившие вредные последствия следствием, то есть причинная связь — необходимый признак объективной стороны рассматриваемого преступления. Если уничтожение, блокирование, модификация либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети не выступало в качестве следствия неправомерного доступа к компьютерной информации, а явилось результатом иной деятельности виновного, то состав преступления, выраженный в ст. 272 УК РФ, отсутствует.

Уничтожение — это полное либо частичное удаление информации с машинных носителей, не подлежащее прежнему восстановлению (например, стирание информации, удаление важных записей и др.).

Блокирование представляет собой закрытие информации, характеризующееся недоступностью ее использования по прямому назначению правомочному на это пользователю.

Модификация заключается в переработке первоначальной информации, несанкционированной ее законным собственником или владельцем, если такая переработка включает в себя любые изменения информации, не меняющие сущности объекта (например, реструктурирование или реорганизация базы данных, удаление либо добавление записей, содержащихся в ее файлах и т.д.).

Под копированием понимают перенос информации или части информации с одного физического носителя на другой, если такой перенос осуществляется помимо воли собственника или владельца этой информации (например, запись информации в память ЭВМ).

Нарушение работы ЭВМ, системы ЭВМ или их сети включает в себя сбой в работе ЭВМ, системы ЭВМ, системы ЭВМ или их сети, препятствующий нормальному функционированию вычислительной техники при условии сохранения ее физической целостности и требований обязательного восстановления (например, отображение неверной информации на мониторе).

Субъективная сторона преступления характеризуется умышленной формой вины в виде прямого или косвенного умысла. Виновный сознает, что он осуществляет именно неправомерный доступ к охраняемой законом компьютерной информации, предвидит, что в результате его действий может наступить или неизбежно наступит хотя бы одно из указанных в законе последствий и желает или сознательно допускает их наступление, либо относится к ним безразлично[[27]](#footnote-27).

Субъект преступления — лицо 16-летнего возраста, не наделенное в силу характера выполняемой им работы возможностью доступа к ЭВМ, системе ЭВМ или их сети.

Часть 2 ст. 272 УК РФ предусматривает квалифицированный состав данного преступления, если оно совершено: а) группой лиц по предварительному сговору; б) организованной группой; в) лицом с использованием своего служебного положения; г) лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении именно этого деяния.

Организованная группа — это устойчивая группа лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Использование служебного положения означает, что лицо незаконно получает доступ к компьютерной информации, злоупотребляя правами, предоставленными ему исключительно в силу служебного положения (занимаемой должности или в силу закона).

К лицам, имеющим доступ к ЭВМ, системе ЭВМ или их сети следует относить пользователей информации (например, операторов ЭВМ, программистов, абонентов системы ЭВМ), а также лиц, по характеру своей деятельности имеющих допуск к ЭВМ, системе ЭВМ или их сети (например, технический персонал, обслуживающий ЭВМ или их сеть).

Как справедливо отмечает Т.М. Лопатина, к числу таких сотрудников нельзя отнести тех, кто имеет возможность просто прикасаться к компьютеру, поскольку круг их функциональных обязанностей не предусматривает обслуживание ЭВМ, системы ЭВМ или их сети и не представляет возможности соприкосновения с информацией, хранящейся в ЭВМ. В данном случае речь идет лишь о профессиональном доступе, а не о доступе в помещение, где находится ЭВМ. Поэтому причислять их к лицам, имеющим доступ к ЭВМ, системе ЭВМ или их сети нет оснований[[28]](#footnote-28).

Нам представляется, что в круг лиц, имеющих доступ к ЭВМ, системе ЭВМ или их сети, должны включаться: а) лица, которые обладают правом работы с компьютерной информацией, делегированное им собственником (или законным владельцем) информации, в силу занимаемого служебного положения или выполняемых функциональных обязанностей; б) лица, которые по характеру своей трудовой деятельности осуществляют техническое обслуживание компьютерной техники. При этом лицо не должно обладать правом допуска к охраняемой законом компьютерной информации, находящейся в ЭВМ, системе ЭВМ или их сети.

Анализ состава преступления, предусмотренного ст. 272 УК РФ, свидетельствует о принципиально правильной позиции законодателя, который отнес его к посягательствам в сфере компьютерной информации. В данном случае налицо признание компьютерной информации, информационной компьютерной инфраструктуры или ее части как предметом преступного посягательства, так и обязательной составляющей объективной стороны состава преступления.

## 2.2. Создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ)

Одним из наиболее распространенных сетевых преступлений, направленных на нарушение нормального функционирования объектов глобальных компьютерных сетей, является создание, использование и распространение вредоносных программ для ЭВМ. Объектом данного преступления являются общественные отношения в сфере безопасного использования ЭВМ, ее программного обеспечения и информационного содержания.

Объективная сторона преступления состоит: а) в создании вредоносных программ для ЭВМ или внесении изменений в существующие программы, приводящие их к качеству вредоносных; б) использовании и в) распространении вредоносных программ для ЭВМ или машинных носителей с такими программами[[29]](#footnote-29). При этом деяние, выразившееся в создании вредоносных программ или внесении изменений в существующие программы, образует преступление только тогда, когда такое деяние объективно создавало реальную угрозу несанкционированного уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. В противном случае действия лица по созданию, использованию или распространению вредоносных программ нельзя рассматривать как преступление. Например, не будут являться преступными действия лица, создавшего довольно безобидную программу — вирус, которая высвечивает на экране монитора штрих и тут же исчезает. Поэтому в тех случаях, когда вредоносная программа не представляет опасности для собственника или владельца информации и объективно не может привести к последствиям, указанным в диспозиции ч. 1 ст. 273 УК РФ, действия лица обоснованно расценивать как малозначительные и на основании ч. 2 ст. 14 УК РФ освобождать его от уголовной ответственности и наказания.

Согласно Закону РФ «О правовой охране программ для электронных вычислительных машин и баз данных» под программой для ЭВМ понимается объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин и других компьютерных устройств с целью получения определенного результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе ее разработки, и порождаемые ею аудиовизуальные отображения (ст. 1 Закона).

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[[30]](#footnote-30).

Вредоносная программа — это специально написанная (созданная) программа, которая, получив управление, способна причинить вред собственнику или владельцу информации в виде ее уничтожения, блокирования, модификации или копирования, а также нарушения работы ЭВМ, системы ЭВМ или их сети.

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[[31]](#footnote-31). Такие программы переносятся при копировании с диска на диск либо по вычислительной сети.

Создание вредоносной программы представляет собой комплекс операций, состоящий из подготовки исходных данных, предназначенных для управления конкретными компонентами системы обработки данных в целях уничтожения, блокирования, модификации или копирования информации, а также нарушения работы ЭВМ, системы ЭВМ или их сети.

Внесение изменений в существующие программы — это процесс модификации программы (переработка программы или набора данных путем обновления, добавления или удаления отдельных фрагментов) до такого ее качества, когда эта программа способна вызвать вредные последствия, указанные в диспозиции ч. 1 ст. 273 УК РФ.

Под использованием вредоносных программ или машинных носителей с такими программами следует понимать их непосредственный выпуск в свет, воспроизведение, распространение и иные действия по их введению в хозяйственный оборот (в том числе в модификационной форме) (ст. 1 Закона РФ «О правовой охране программ для электронных вычислительных машин и баз данных»). Например, использованием вредоносной программы является ее ввод (установка) в память компьютера.

Распространение вредоносных программ заключается в предоставлении доступа к воспроизведенной в любой материальной форме программе для ЭВМ или базе данных, в том числе сетевым и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы, включая импорт для любой из этих целей (ст. 1 указанного выше Закона). Например, распространение таких программ может быть осуществлено при работе виновного на чужом компьютере, путем использования дискеты с записью, содержащей вирус, распространение вредоносной программы через модем или передачу по компьютерной сети и т.п.

Следует обратить внимание, что создание, использование и распространение вредоносных программ для ЭВМ всегда предполагает активные действия со стороны лица, совершившего это преступление. Бездействием совершить рассматриваемое преступление представляется невозможным.

Состав преступления, сконструированный в ч. 1 ст. 273 УК РФ, является формальным. Следовательно, для признания преступления оконченным не требуется наступления вредных последствий в виде уничтожения, блокирования, модификации либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети. Достаточно установить сам факт совершения хотя бы одного из альтернативно-обязательных действий, перечисленных в диспозиции ч. 1 ст. 273 УК РФ.

Создание, использование и распространение вредоносной программы для ЭВМ, повлекшее вывод из строя вычислительной техники, выступающей в качестве аппаратной структуры (например, повреждение физической целостности электронно-вычислительной машины, ее основных устройств, не подлежащие восстановлению), квалифицируются по совокупности преступлений, устанавливающих ответственность за умышленное уничтожение или повреждение имущества (ст. 167 УК РФ) и за создание, использование и распространение вредоносных программ для ЭВМ (ст. 273 УК РФ).

С субъективной стороны анализируемое преступление совершается с прямым умыслом. Виновное лицо сознает, что им создается или модифицируется из обычной такая программа, которая способна уничтожить, блокировать, модифицировать либо скопировать информацию, нарушить работу ЭВМ, системы ЭВМ или их сети, либо используется или распространяется такая программа, и желает совершить эти действия.

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[[32]](#footnote-32). Мотивы этого преступления и его цели не являются обязательными признаками состава и учитываются лишь при назначении наказания.

Субъектом данного преступления может выступать любое физическое лицо, достигшее к моменту его совершения 16-летнего возраста. О субъекте преступления, предусмотренного ст. 273 УК РФ, в самой статье не говорится ничего, что свидетельствует о том, что субъект общий, не обладающий никакими дополнительными признаками. Это, безусловно, верно. Вместе с тем в специальной литературе высказано мнение о том, что субъект данного преступления должен обладать таким дополнительным признаком, как осведомленность о способности программы привести к несанкционированному уничтожению, блокированию, модификации или копированию информации, а равно к нарушению работы ЭВМ, системы ЭВМ или их сети. Ученые аргументируют свои выводы тем, что в диспозиции ст. 273 УК РФ указывается на признак заведомости по отношению к предусмотренным вредоносным последствиям[[33]](#footnote-33). Игнорирование этого признака ведет к объективному вменению, то есть к нарушению основополагающего принципа уголовного права - принципа законности. Однако вряд ли можно согласиться с заключением, что этот признак относится к характеристике субъекта преступления. Признак заведомости, с точки зрения Е.А.Маслаковой, характеризует не особенности субъекта преступления, а его психическое отношение к своим действиям по отношению к компьютерной программе и к последствиям от них в виде свойств вредоносности, которые могут привести к уничтожению, блокированию, модификации или копированию информации, к нарушению работы ЭВМ, системы ЭВМ или их сети, т.е. к характеристике его вины[[34]](#footnote-34).

Часть 2 ст. 273 УК РФ в качестве квалифицирующего признака преступления предусматривает наступление тяжких последствий. Таким образом, квалифицированный состав рассматриваемого преступления сконструирован по типу материального состава. В силу этого обстоятельства для признания лица виновным в совершении преступления, ответственность за которое наступает по ч. 2 ст. 273 УК РФ, необходимо установить факт наступления или распространения вредоносных программ для ЭВМ, то есть действий, образующих объективную сторону этого преступления.

К тяжким последствиям следует отнести гибель людей, причинение тяжкого или средней тяжести вреда их здоровью, массовое причинение легкого вреда здоровью людей, наступление экологических катастроф, транспортных или производственных аварий, причинение крупного материального ущерба личности, обществу или государству. Специфика рассматриваемого более опасного вида данного 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. Это означает, что причинение тяжких последствий не охватывается умыслом виновного, однако он предвидит возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение либо не предвидит, хотя и должен был и мог предвидеть возможность наступления тяжких последствий.

# ЗАКЛЮЧЕНИЕ

Компьютерные преступления – чрезвычайно многогранные и сложные явления.

Преступлениями в сфере компьютерной информации следует считать виновно совершенные общественно опасные деяния, посягающие на нормальный порядок обращения охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания.

Необходимо дать определение понятия «компьютерная информация» и вынести его в примечание к статье 272 УК РФ. Компьютерной информацией являются положения объективной действительности, способные изменять характер общественных отношений, являющиеся результатом человеческой деятельности и закрепленные на машинном носителе, электронно-вычислительной машине, системе ЭВМ, их сети, то есть информация, представленная в электронном виде.

Специфика преступлений данной группы определяется их объектом и предметом. Родовым объектом компьютерных преступлений являются общественные отношения в сфере обеспечения безопасности использования автоматизированных систем обработки данных, нормальных прав и интересов лиц, общества и государства, активно пользующихся электронно-вычислительной техникой. Непосредственный объект — это конкретные права и интересы по поводу использования таких систем (право владельца системы на неприкосновенность содержащейся в ней информации, заинтересованность в правильной эксплуатации системы). Предметом компьютерных преступлений является автоматизированная система обработки данных, включающая получение информации, полезной для физических и юридических лиц.

Объективная сторона представляет собой деяние в виде действий или бездействия, сопряженного с нарушением прав и интересов в части пользования компьютерными системами во вред личным правам или государственным интересам.

Большинство компьютерных преступлений сконструированы как материальные составы, то есть предусматривают наступление общественно опасных последствий в виде вреда, наносимого правам и интересам пользователя ЭВМ — личности, обществу или государству.

Субъективная сторона характеризуется умышленной виной (прямым или косвенным умыслом).

Субъекты преступлений в сфере компьютерной информации подразделяются на две основные группы: а) лица, не связанные трудовыми отношениями с организацией, «атакованной» в криминальных целях; б) сотрудники – пользователи ЭВМ, злоупотребившие своим положением в компании. На наш взгляд, за создание, использование и распространение вредоносных программ для ЭВМ уголовной ответственности должны подлежать лица, достигшие ко времени совершения преступления 14 лет.

Система компьютерных преступлений может быть построена следующим образом:

I. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации (ст.272 УК РФ); создание, использование и распространение вредоносных программ для ЭВМ (ст.273 УК РФ); нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети (ст.274 УК РФ).

II. Преступления, совершаемые с использованием компьютера:

а) преступления против личности; б) преступления в сфере экономики; в) преступления против общественной безопасности, общественного порядка и общественной нравственности; г) преступления против безопасности государства.

Статью 272 УК РФ следует изложить в следующей редакции:

«1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. Неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, –

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо исправительными работами на срок до двух лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет.

3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, –

наказываются штрафом до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо лишением свободы на срок до восьми лет».

Квалифицирующий признак «нарушение работы ЭВМ, системы ЭВМ или их сети» следует исключить из статей 272–273 УК РФ, так как при совершении неправомерного доступа к охраняемой законом РФ компьютерной информации, повлекшего копирование информации и т.п., уже нарушается нормальная работа ЭВМ, системы ЭВМ или их сети.

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.

# СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативная литература

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 13.02.2009) [Текст] // Собр. законодательства Рос. Федерации. – 1996. – Ст. 2954.
2. О правовой охране программ для электронных вычислительных машин и баз данных: Закон Российской Федерации от 23 сентября 1992 г. № 3523-1 (ред. от 02.02.2006) [Текст] // Ведомости СНД РФ и ВС РФ. – 1992. – № 42. – Ст. 2325.
3. Об информации, информатизации и защите информации: Федеральный закон Российской Федерации от 20 февраля 1995 г. № 24-ФЗ (ред. от 10.01.2003) (утратил силу) [Текст] // Собр. законодательства Рос. Федерации. – 1995. – № 8. – Ст. 609.
4. Определение Верховного Суда РФ от 19 марта 2007 г. № 69-о07-5 (опубликовано не было) [Текст] // СПС КонсультантПлюс. – 2008.

Специальная литература

1. Батурин, Ю.М. Проблемы компьютерного права [Текст] / Ю.М.Батурин. - М.: Юрид. лит., 1991. - 272 c.
2. Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Текст] / А.Г. Волеводз. – М.: Юрлитинформ, 2002. – 197 с.
3. Григорьев, А.Н. Компьютерные преступления и защита компьютерной информации. Научно-практическое пособие [Текст] / А.Н.Григорьев, В.М.Мешков, Н.Ю.Проценко. – Калининград: Изд-во Калининградского ЮИ МВД России, 2003. – 120 c.
4. Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. … канд. юрид. наук: 12.00.08 [Текст] / У.В.Зинина. – М., 2007. – 33 с.
5. Зубова, М.А. Компьютерная информация как объект уголовно-правовой охраны: автореф. дис. … канд. юрид. наук: 12.00.08 [Текст] / М.А.Зубова. – Казань, 2008. – 28 с.
6. Кадников, Н.Г. Уголовное право. Общая и особенная части. Учебник для вузов [Текст] / Н.Г.Кадников. – М.: Городец, 2006. – 944 с.
7. Компьютерные технологии в юридической деятельности: Учебное и практическое пособие [Текст] / Под ред. Н. Полевого, В. Крылова. - М.: БЕК, 1994. - 304 с.
8. Копырюлин, А. Квалификация преступлений в сфере компьютерной информации [Текст] / А. Копырюлин // Законность. – 2007. – № 6. – С.21– 22.
9. Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: автореф. дис. … канд. юрид. наук: 12.00.08 [Текст] / А.Н.Копырюлин. – Тамбов, 2007. – 22 c.
10. Кравцов, К.Н. Этапы развития российского законодательства об ответственности за преступления в сфере компьютерной информации [Текст] / К.Н. Кравцов // История государства и права. – 2006. – № 12. – С.28– 29.
11. Крылов, В.В. Расследование преступления в сфере информации [Текст] / В.В.Крылов. – М.: Городец. – 1998. – 250 с.
12. Кузнецов, А.П. Классификация преступлений в сфере экономики: теоретические аспекты исследования [Текст] / А.П.Кузнецов, И.Н.Бокова, В.Г.Ярыгин // Экономическая безопасность России: политические ориентиры, законодательные приоритеты, практика обеспечения: Вестник Нижегородской академии МВД России. – 2005. – № 5. – С. 29– 31.
13. Лопатина, Т.М. Отдельные вопросы характеристики уголовно-правовых признаков субъекта преступлений в сфере компьютерной информации [Текст] / Т.М. Лопатина // Рос. судья. – 2006. – № 1 // СПС КонсультантПлюс. – 2006.
14. Максимов, В.Ю. Компьютерные преступления (вирусный аспект) [Текст] / В.Ю.Максимов. – Ставрополь: Книжное издательство, 1999. – 215 с.
15. Маслакова, Е.А. Правовое регулирование уголовной ответственности за преступления в сфере компьютерной информации в Российской Федерации [Текст] / Е.А. Маслакова // Правовые вопросы связи. – 2006. – № 2. – С.48–49.
16. Маслакова, Е.А. История правового регулирования уголовной ответственности за компьютерные преступления [Текст] / Е.А. Маслакова // Информационное право. – 2006. – № 4. – С.44– 45.
17. Маслакова, Е. Вредоносные программы для ЭВМ в глобальных компьютерных сетях [Текст] / Е. Маслакова // Юридический мир. – 2005. – № 11 // СПС КонсультантПлюс. – 2007.
18. Милашев, В.А. Неправомерный доступ к компьютерной информации в сетях ЭВМ [Текст] / В.А. Милашев // Правовые вопросы связи. – 2006. – № 1. – С.29-31.
19. Осипенко, А.Л. Борьба с преступлениями в глобальных компьютерных сетях: Международный опыт: Монография [Текст] / А.Л.Осипенко. – М.: Норма, 2004 – 199 с.
20. Российское уголовное право. Особенная часть [Текст] / Под ред. В.Н. Кудрявцева и А.В. Наумова. – М.: Юристъ, 2002. – 629 с.
21. Скоромников, К.С. Компьютерное право Российской Федерации: Учебник [Текст] / К.С.Скоромников. – М.: Проспект, 2000. – 534 с.
22. Соловьев, Л.Н. Вредоносные программы: расследование и предупреждение преступлений [Текст] / Л.Н.Соловьев. – М.: Собрание, 2004. – 198 с.
23. Степанов-Егиянц, В. Ответственность за компьютерные преступления [Текст] / В. Степанов-Егиянц // Законность. – 2005. – № 12. – С45– 46.
24. Уголовное право Российской Федерации. Особенная часть: учебник [Текст] / Под ред. А.И. Рарога. – Изд. 2-е, перераб. и доп. – М.: Юристъ, 2004. – 655 с.
25. Уголовное право России. Часть общая: учебник для вузов [Текст] / Под ред. Л.Л. Кругликова. – М.: Волтерс Клувер, 2005. – 691 с.
26. Уголовное право Российской Федерации. Особенная часть: Учебник [Текст] / Под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. – Изд. испр. и доп. – М.: ИНФРА-М, КОНТРАКТ, 2006. – 728 с.
27. Широков, В.А. Компьютерные преступления: основные тенденции развития [Текст] / В.А. Широков, Е.В. Беспалова // Юрист. – 2006. – № 10. – С.20– 22.
28. Официальный сайт МВД России. Общие сведения о состоянии преступности [Текст] // www.mvdinform.ru

# ПРИЛОЖЕНИЕ

ОБЩИЕ СВЕДЕНИЯ О СОСТОЯНИИ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ ЗА 2005 – 2008 ГОДЫ

|  |  |  |
| --- | --- | --- |
| Период | Компьютерные преступления | Преступления в сфере компьютерной информации |
| 2005 год | 14 000 | 10 214 |
| 2006 год | 14 000 | 8 889 |
| 2007 год | 12 000 | 6 763 |
| 2008 год | 14 000 | 9 010 |

Источник: Официальный сайт МВД России // www.mvdinform.ru

1. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 13.02.2009) [Текст] // Собр. законодательства Рос. Федерации. – 1996. – Ст. 2954. [↑](#footnote-ref-1)
2. Официальный сайт МВД России. Общие сведения о состоянии преступности [Текст] // www.mvdinform.ru [↑](#footnote-ref-2)
3. Там же. [↑](#footnote-ref-3)
4. Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: автореф. дис. … канд. юрид. наук: 12.00.08 [Текст] / У.В.Зинина. – М., 2007. – С.9. [↑](#footnote-ref-4)
5. О правовой охране программ для электронных вычислительных машин и баз данных: Закон Российской Федерации от 23 сентября 1992 г. № 3523-1 (ред. от 02.02.2006) [Текст] // Ведомости СНД РФ и ВС РФ. – 1992. – № 42. – Ст. 2325. [↑](#footnote-ref-5)
6. См.: Маслакова, Е.А. История правового регулирования уголовной ответственности за компьютерные преступления [Текст] / Е.А. Маслакова // Информационное право. – 2006. – № 4. – С.45. [↑](#footnote-ref-6)
7. См.: Максимов, В.Ю. Компьютерные преступления (вирусный аспект) [Текст] / В.Ю.Максимов. - Ставрополь: Книжное издательство, 1999. – С.64-65; Волеводз, А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Текст] / А.Г. Волеводз. - М.: Юрлитинформ, 2002. – С.91. [↑](#footnote-ref-7)
8. Об информации, информатизации и защите информации: Федеральный закон Российской Федерации от 20 февраля 1995 г. № 24-ФЗ (ред. от 10.01.2003) (утратил силу) [Текст] // Собр. законодательства Рос. Федерации. – 1995. – № 8. – Ст. 609. [↑](#footnote-ref-8)
9. См.: Маслакова, Е.А. История правового регулирования уголовной ответственности за компьютерные преступления [Текст] / Е.А. Маслакова // Информационное право. – 2006. – № 4. – С.45. [↑](#footnote-ref-9)
10. Кравцов, К.Н. Этапы развития российского законодательства об ответственности за преступления в сфере компьютерной информации [Текст] / К.Н. Кравцов // История государства и права. – 2006. – № 12. – С.28. [↑](#footnote-ref-10)
11. Осипенко, А.Л. Борьба с преступлениями в глобальных компьютерных сетях: Международный опыт: Монография [Текст] / А.Л.Осипенко. – М.: Норма, 2004 – С.52; Крылов, В.В. Расследование преступления в сфере информации [Текст] / В.В.Крылов. – М.: Городец, 1998. – С.101; Скоромников, К.С. Компьютерное право Российской Федерации: Учебник [Текст] / К.С.Скоромников. – М.: Проспект, 2000. – С.200–201. [↑](#footnote-ref-11)
12. См.: Уголовное право Российской Федерации. Особенная часть: Учебник [Текст] / Под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. – Изд. испр. и доп. – М.: ИНФРА-М, КОНТРАКТ, 2006. – С.490. [↑](#footnote-ref-12)
13. Батурин, Ю.М. Проблемы компьютерного права [Текст] / Ю.М.Батурин. - М.: Юрид. лит., 1991. – С.52. [↑](#footnote-ref-13)
14. См.: Компьютерные технологии в юридической деятельности: Учебное и практическое пособие [Текст] / Под ред. Н. Полевого, В. Крылова. - М.: БЕК, 1994. – С.71. [↑](#footnote-ref-14)
15. Кадников, Н.Г. Уголовное право. Общая и особенная части. Учебник для вузов [Текст] / Н.Г.Кадников. – М.: Городец, 2006. – С.738. [↑](#footnote-ref-15)
16. Уголовное право Российской Федерации. Особенная часть: учебник [Текст] / Под ред. А.И. Рарога. – Изд. 2-е, перераб. и доп. – М.: Юристъ, 2004. – С.502. [↑](#footnote-ref-16)
17. Григорьев, А.Н. Компьютерные преступления и защита компьютерной информации. Научно-практическое пособие [Текст] / А.Н.Григорьев, В.М.Мешков, Н.Ю.Проценко. – Калининград: Изд-во Калининградского ЮИ МВД России, 2003. – С.38. [↑](#footnote-ref-17)
18. Лопатина, Т.М. Отдельные вопросы характеристики уголовно-правовых признаков субъекта преступлений в сфере компьютерной информации [Текст] / Т.М. Лопатина // Рос. судья. – 2006. – № 1 // СПС КонсультантПлюс. – 2006. [↑](#footnote-ref-18)
19. Широков, В.А. Компьютерные преступления: основные тенденции развития [Текст] / В.А. Широков, Е.В. Беспалова // Юрист. – 2006. – № 10. – С.21. [↑](#footnote-ref-19)
20. Уголовное право России. Часть общая: учебник для вузов [Текст] / Под ред. Л.Л. Кругликова. – М.: Волтерс Клувер, 2005. – С.509. [↑](#footnote-ref-20)
21. Кузнецов, А.П. Классификация преступлений в сфере экономики: теоретические аспекты исследования [Текст] / А.П.Кузнецов, И.Н.Бокова, В.Г.Ярыгин // Экономическая безопасность России: политические ориентиры, законодательные приоритеты, практика обеспечения: Вестник Нижегородской академии МВД России. – 2005. – № 5. – С. 29. [↑](#footnote-ref-21)
22. Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: автореф. дис. … канд. юрид. наук: 12.00.08 [Текст] / А.Н.Копырюлин. – Тамбов, 2007. – С.14. [↑](#footnote-ref-22)
23. Копырюлин, А. Квалификация преступлений в сфере компьютерной информации [Текст] / А. Копырюлин // Законность. – 2007. – № 6. – С.21. [↑](#footnote-ref-23)
24. Определение Верховного Суда РФ от 19 марта 2007 г. № 69-о07-5 (опубликовано не было) [Текст] // СПС КонсультантПлюс. – 2008. [↑](#footnote-ref-24)
25. Зубова, М.А. Компьютерная информация как объект уголовно-правовой охраны: автореф. дис. … канд. юрид. наук: 12.00.08 [Текст] / М.А.Зубова. – Казань, 2008. – С.14. [↑](#footnote-ref-25)
26. Кадников, Н.Г. Уголовное право. Общая и особенная части. Учебник для вузов [Текст] / Н.Г.Кадников. – М.: Городец, 2006. – С.740. [↑](#footnote-ref-26)
27. Милашев, В.А. Неправомерный доступ к компьютерной информации в сетях ЭВМ [Текст] / В.А. Милашев // Правовые вопросы связи. – 2006. – № 1. – С.29. [↑](#footnote-ref-27)
28. См.: Лопатина, Т.М. Отдельные вопросы характеристики уголовно-правовых признаков субъекта преступлений в сфере компьютерной информации [Текст] / Т.М. Лопатина // Рос. судья. – 2006. – № 1 // СПС КонсультантПлюс. – 2006. [↑](#footnote-ref-28)
29. Степанов-Егиянц, В. Ответственность за компьютерные преступления [Текст] / В. Степанов-Егиянц // Законность. – 2005. – № 12. – С45. [↑](#footnote-ref-29)
30. Маслакова, Е. Вредоносные программы для ЭВМ в глобальных компьютерных сетях [Текст] / Е. Маслакова // Юридический мир. – 2005. – № 11 // СПС КонсультантПлюс. – 2007. [↑](#footnote-ref-30)
31. Соловьев, Л.Н. Вредоносные программы: расследование и предупреждение преступлений [Текст] / Л.Н.Соловьев. – М.: Собрание, 2004. – С. 29. [↑](#footnote-ref-31)
32. Маслакова, Е. Вредоносные программы для ЭВМ в глобальных компьютерных сетях [Текст] / Е. Маслакова // Юридический мир. – 2005. – № 11 // СПС КонсультантПлюс. – 2007. [↑](#footnote-ref-32)
33. См.: Российское уголовное право. Особенная часть [Текст] / Под ред. В.Н. Кудрявцева и А.В. Наумова. – М.: Юристъ, 2002. – С. 351. [↑](#footnote-ref-33)
34. Маслакова, Е.А. Правовое регулирование уголовной ответственности за преступления в сфере компьютерной информации в Российской Федерации [Текст] / Е.А. Маслакова // Правовые вопросы связи. – 2006. – № 2. – С.49. [↑](#footnote-ref-34)