На правах рукописи

ЧИСЛИН ВИТАЛИЙ ПЕТРОВИЧ

УГОЛОВНО-ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ ОТ НЕПРАВОМЕРНОГО ДОСТУПА

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

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата юридических наук

Москва 2004

Работа выполнена на кафедре уголовно-правовых дисциплин и кафедре правоведения Коломенского государственного педагогического института

Научный руководитель доктор юридических наук, доцент
Середа Елена Васильевна

Научный консультант доктор технических наук, профессор
Чернышов Владимир Николаевич

Официальные оппоненты: доктор юридических наук, доцент
Просвирнин Юрий Георгиевич

кандидат юридический наук, доцент

Побрызгаева Елена Владимировна

Ведущая организация Тамбовский государственный педагогический университет им. Г.Р. Державина

Защита диссертации состоится «___» _____ 2004 года, в ____ ч. на заседании диссертационного совета К 521.005.01 Института международного права и экономики им. А.С. Грибоедова по адресу: 105066,
г. Москва, ул. Спартаковская, д. 2/1, стр. 5

С диссертацией можно ознакомиться в библиотеке Института международного права и экономики им. А.С. Грибоедова

Автореферат разослан «___» _____2004 г.

Ученый секретарь
диссертационного совета Н.П. Шарыло

Подписано к печати 29.04.2004
Гарнитура Times New Roman. Формат 60 × 84/16. Бумага офсетная.
Печать офсетная. Объем: 1,16 усл. печ. л.; 1,2 уч.-изд. л.
Тираж 100 экз. С. 338^{M}

Издательско-полиграфический центр ТГТУ
392000, Тамбов, Советская, 106, к. 14

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Современный период развития цивилизации характеризуется переходом от индустриального общества к обществу информационному. Информация признается все более значимым видом общественных ресурсов, требующим, как и любая другая ценность, принятия соответствующих мер защиты от неправомерных действий. Все более актуальной становится проблема обеспечения информационной безопасности как одной из составляющих национальной безопасности Российской Федерации.

Основными мерами обеспечения информационной безопасности выступают правовые средства, составной частью которых являются уголовно-правовые меры, направленные на противодействие наиболее опасным посягательствам на информационные общественные отношения. Признание социальной ценности информации определяет необходимость комплексного уголовно-правового подхода к ее защите.

Важнейшей проблемой уголовно-правовых мер обеспечения информационной безопасности является проблема защиты информации от неправомерного доступа. Наличие данной проблемы заключается в том, что защите от неправомерного доступа подлежит наиболее ценная охраняемая законом информация, а также в том, что неправомерный доступ к охраняемой законом информации влечет, как правило, значительные общественно опасные последствия, в частности, нарушение ее конфиденциальности, целостности и доступности.

Вместе с тем, современные уголовно-правовые меры защиты информации от неправомерного доступа основаны на приоритетности защиты информации, находящейся на определенных носителях (компьютерной информации), что, в силу несоответствия данного подхода положениям информационного законодательства, влечет отсутствие четкой системы уголовно-правовой защиты информации от неправомерного доступа.

Вышеуказанные обстоятельства выступают причиной необходимости разработки системы преступлений в сфере информационных отношений, одной из составляющих которой должен выступить неправомерный доступ к охраняемой законом информации. При этом степень уголовно-правовой защиты информации должна определяться ее содержанием, а не свойствами носителя. Все это требует детальной разработки элементов нового общего состава преступления, заключающегося в неправомерном доступе к охраняемой законом информации.

Степень разработанности темы исследования. Неправомерный доступ к охраняемой законом информации привлекал внимание многих исследователей, в частности, таких как: Ю.М. Батурин, Н.Н. Безруков,
С.В. Бородин, Т.А. Бушуева, В.В. Вехов, А.Г. Волеводз, А.М. Жодзишский, И.А. Клепицкий, В.С. Комиссаров, В.В. Крылов, В.Д. Курушин, В.А. Мазуров, В.А. Минаев, С.А. Пашин, Н.С. Полевой, С.В. Полубинская, А.Н. Попов, К.С. Скоромников, Н.Г. Шурухнов и др. Однако большинство данных исследований носят преимущественно криминалистическую или криминологическую направленность. Но и уголовно-правовые исследования, как правило, заключаются в рассмотрении основных элементов состава преступления, предусмотренного статьей 272 Уголовного кодекса Российской Федерации. При этом комплексный уголовно-правовой анализ, основанный на признании актуальности понятия преступлений в сфере информационных отношений как более широкого по отношению к преступлениям в сфере компьютерной информации, на уровне диссертационного исследования еще не проводился.

Изложенное позволяет говорить о том, что в настоящий момент проблема комплексного уголовно-правового подхода к защите информации от неправомерного доступа, независимо от типа носителя, требует детального изучения и возможно внесение соответствующих изменений в действующее законодательство. Указанные обстоятельства определили выбор темы и актуальность диссертационной работы, призванной в какой-то мере решить вышеуказанную проблему.

Объектом исследования являются общественные отношения, складывающиеся при применении уголовно-правовых норм в области защиты информации от неправомерного доступа, проблемы, полноты и необходимости регулирования уголовным законодательством отношений, связанных с обращением охраняемой законом информации.

Предмет исследования – понятия и нормы уголовного законодательства, регулирующие ответственность за неправомерный доступ к охраняемой законом информации

Цель исследования заключается в проведении комплексного изучения закрепленных в действующем законодательстве уголовно-правовых мер защиты информации от неправомерного доступа, выявлении проблем в данной сфере и предложении вариантов решения данных проблем.

Достижение указанной цели предполагает решение ряда взаимосвязанных **задач**, к числу которых относятся:

- определение пределов применения уголовно-правовых мер защиты информации от неправомерного доступа;
- раскрытие информационных отношений как самостоятельного объекта преступных посягательств;
- исследование понятия информации в праве и ее носителей;
- проведение классификации преступных посягательств на информацию;
- четкое определение предмета посягательства в виде неправомерного доступа к охраняемой законом информации;
- подробное рассмотрение элементов состава преступления, предусмотренного статьей 272 УК РФ (неправомерный доступ к компьютерной информации);
- выявление основных проблем ныне действующего порядка уголовно-правовой защиты информации от неправомерного доступа;
- внесение предложений по изменению действующих уголовно-правовых норм в области защиты информации от неправомерного доступа.

Методологической основой диссертационного исследования являются основные теоретические положения науки уголовного права, теории защиты информации, криминалистики, информационного права. При проведении исследования использовались такие научные способы познания как наблюдение, сравнение, системный подход, аналитический метод и другие. Применение указанных методов позволило изучить объект исследования целостно и всесторонне.

Исследование базируется на действующем информационном и уголовном законодательстве. В исследовании использованы нормативные акты иных отраслей российского права.

Нормативную базу исследования составили Конституция РФ, действовавшее и действующее уголовное, гражданское, административное законодательство, а также нормативно-правовые акты, регулирующие порядок обращения информации с режимом ограниченного доступа.

Научная новизна исследования состоит в том, что впервые на диссертационном уровне проанализирована существующая система уголовно-правовых мер защиты информации от неправомерного доступа. Новыми также являются вносимые автором предложения, направленные на повышение эффективности и гарантий защиты информации от неправомерного доступа.

Новизной обладает обоснованное автором положение о необходимости более широкого применения уголовно-правовых мер защиты в отношении охраняемой законом информации от неправомерного доступа.

Положения, выносимые на защиту. Проведенное исследование дало возможность обосновать и вынести на защиту следующие наиболее важные положения.

1 Защита охраняемой законом информации от неправомерного доступа является важной составляющей обеспечения информационной безопасности. Данное обстоятельство определяется значительной социальной ценностью информации, имеющей режим ограниченного доступа.

2 Действующее уголовное законодательство не содержит комплексного подхода к проблеме обеспечения информационной безопасности уголовно-правовыми мерами, в силу того, что информационные отношения не представлены в действующем Уголовном кодексе Российской Федерации (далее – УК РФ) в качестве самостоятельного объекта защиты. Однако данное состояние не соответствует объективной ценности информационных ресурсов в современном обществе.

3 На современном этапе развития информационных технологий в России возникла необходимость разработки в уголовном законодательстве системы преступлений в сфере информационных отношений, составной частью которых должны выступить уже закрепленные в УК РФ преступления в сфере компьютерной информации.

4 Система современного российского информационного законодательства основана на единственном критерии классификации информации как объекта правового регулирования: разделении информации по содержанию на общедоступную и с режимом ограниченного доступа. Данная классификация воспринята действующим уголовным законодательством лишь частично и имеет еще один критерий классификации информации, основанный на типе носителя, в частности, в УК РФ выделена категория «компьютерной информации». Данные обстоятельства являются причиной того, что в действующем законодательстве уголовно-правовые меры защиты информации от неправомерного доступа реализованы не последовательно и не системно.

5 Уголовно-правовой защите от неправомерного доступа подлежит весь массив документированной информации, содержащей сведения, отнесенные законом к государственной тайне или конфиденциальной информации.

6 Под доступом к информации следует понимать ознакомление с охраняемой законом информацией и (или) получение возможности совершать операции с данной информацией, в частности, ее копи-

рование, блокирование, модификацию и уничтожение. При этом не имеет принципиального значения тот факт, осуществляется доступ к самой информации или к ее носителям.

7 Возникает необходимость внесения изменений в действующее уголовное законодательство, обеспечивающих полноту защиты всего массива охраняемой законом информации от неправомерного доступа, в частности, разработки общего состава неправомерного доступа к охраняемой законом информации.

8 Автор предлагает внести следующие изменения в УК РФ:

а) название главы 28 УК РФ изложить в следующей редакции: «Преступления в сфере информационных отношений»;

б) диспозицию статьи 272 УК РФ изложить в следующей редакции:

«Статья 272. Неправомерный доступ к охраняемой законом информации.

1 Неправомерный доступ к охраняемой законом информации, т.е. документированной информации, содержащей сведения, отнесенные законом к государственной тайне или конфиденциальной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование данной информации, – …

2 То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения или с использованием ЭВМ, системы ЭВМ или их сети, – …»;

в) часть 1 статьи 274 изложить в следующей редакции:

«1 Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ или неправомерно получившим доступ к ЭВМ, системе ЭВМ, или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом информации ЭВМ, если это деяние причинило существенный вред, – …».

Научно-теоретическое и практическое значение диссертации состоит в том, что положения и выводы, изложенные в диссертационной работе, могут служить частью основы теоретической разработки системы преступлений в сфере информационных отношений. Кроме того, предложенные изменения в уголовное законодательство могут быть использованы в законотворческом процессе.

Апробация результатов исследования. Основные положения диссертации обсуждались на совместном заседании кафедр уголовно-правовых дисциплин и правоведения Коломенского государственного педагогического института, были обсуждены на заседании кафедры криминалистики и информатизации правовой деятельности Тамбовского государственного технического университета, отражены в опубликованных научных работах автора.

Основные теоретические выводы, рекомендации и положения диссертационного исследования докладывались на всероссийских и межвузовских конференциях. Диссертант, в частности, выступал на Межрегиональной научно-практической конференции «Проблемы теории, законодательства и практики правоохранительных органов по стабилизации и снижению роста преступности в России» (Тамбов, 2000), международном семинаре «Вопросы квалификации и расследования преступлений в сфере экономики» (Тамбов, 2000), научно-практической конференции «Правоохранительная система России и правовой механизм обеспечения законности и правопорядка, защиты прав и свобод личности» (Тамбов, 2001), Межрегиональной научно-практической конференции «Власть и общество на востоке России: итоги десятилетия и перспективы развития» (Тамбов, 2001), заочной Межвузовской научно-практической конференции «Политика. Власть. Право» (Санкт-Петербург, Коломна, 2001 – 2003).

Положения и выводы диссертации апробированы в процессе преподавания курсов уголовного права, защиты информации на юридическом факультете Тамбовского государственного технического университета.

Материалы диссертационного исследования используются автором при чтении специальных курсов и специальных семинаров на юридическом факультете Коломенского государственного педагогического института.

Структура и объем диссертационной работы соответствует логике проведенного исследования. Диссертация состоит из введения, трех глав, объединяющих восемь параграфов, заключения и библиографического списка.

СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновывается актуальность, научная новизна и практическая значимость темы, определяются цели и задачи исследования, дается характеристика методологических основ работы, формулируются основные положения, выносимые на защиту.

Глава первая **«Информация как объект уголовно-правовой защиты»** состоит из трех параграфов.

Параграф первый ***«Информационные отношения как новый объект преступных посягательств»*** посвящен проблеме выделения особой категории преступлений в сфере информационных отношений, а также рассмотрению основного критерия выделения данного вида преступлений – информационным отношениям как объекту преступления.

Первоначально автор рассматривает информационные отношения с точки зрения информационного права. В частности, отмечается, что информационные отношения возникают и развиваются в процессе сбора, обработки, накопления, поиска и распространения информации.

Объектами данных отношений могут выступать: информация, информационные процессы, информационные системы и ресурсы, информационная сфера (среда) и продукты; информационная безопасность, средства обеспечения автоматизированных информационных систем и их технологий; словари, тезаурусы и классификаторы; инструкции и методики, программы для ЭВМ; базы и банки данных; топологии интегральных микросхем и сами интегральные микросхемы; средства международного информационного обмена.

Специфика информационных отношений определяется их субъектным составом. В частности, Федеральный закон «Об информации, информатизации и защите информации» в статье 2 выделяет следующие особые категории субъектов информационных отношений: собственник информационных ресурсов, владелец информационных ресурсов, пользователь (потребитель) информации.

Однако понятие информационных отношений как объекта преступления в уголовном праве имеет свою специфику. Традиционно в науке уголовного права объектом преступления признаются общественные отношения, охраняемые уголовным законом от преступных посягательств. При этом информационные отношения в УК РФ не выделены в качестве самостоятельного видового объекта преступления, но, безусловно, являются дополнительным объектом целого ряда различных преступлений, например, нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (статья 138 УК РФ), незаконного получения и разглашения сведений, составляющих коммерческую, налоговую или банковскую тайну (статья 183 УК РФ), государственной измены (статья 275 УК РФ).

Тем самым широкое распространение информационных отношений в качестве дополнительного объекта преступления и отсутствие четкой системы классификации преступлений в сфере информационных отношений позволяет говорить о возможной необходимости выделения информационных отношений в виде самостоятельного видового объекта преступления и, соответственно, выделения самостоятельной главы в Особенной части УК РФ с последующей разработкой общих составов преступлений в сфере информационных отношений.

По нашему мнению, данное утверждение особенно актуально для такого вида преступлений в сфере информационных отношений как неправомерный доступ к охраняемой законом информации, поскольку на практике неправомерный доступ к информации является одним из самых распространенных видов информационных преступлений, а также влекущим наиболее опасные последствия, в частности, нарушение конфиденциальности, а зачастую, целостности и доступности информации.

Закрепленная в статье 272 УК РФ уголовная ответственность за неправомерный доступ к компьютерной информации не обеспечивает защиты всех видов информационных ресурсов от неправомерного доступа, а ограничивается лишь уголовно-правовой защитой информационных ресурсов на компьютерных носителях. Данная логика законодателя не совсем понятна, поскольку значимость информации не определяется ее нахождением на конкретном виде носителя.

Во втором параграфе ***«Понятие информации в теории права и законодательстве. Особенности компьютерной информации и ее носителей»*** рассмотрено понятие информации с точки зрения общей теории информации. В частности, проанализирована категория отражения как основа информационных систем, сущность сигналов как носителей информации, информационные процессы (восприятие, фиксация информации на носителях, передача, прием и хранение информации).

Далее в работе отражены вопросы истории закрепления термина «информация» в отечественном законодательстве. В настоящее время в соответствии с Федеральным законом от 20 февраля 1995 № 24-ФЗ «Об информации, информатизации и защите информации» под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их представления.

Как отмечено в диссертации, правовому регулированию подлежит преимущественно количественно ограниченная совокупность информации, а именно, документ или документированная информация.

При этом документированная информация в качестве организационной формы выступает как совокупность: содержания информации; реквизитов, позволяющих установить источник, полноту информации, степень ее достоверности, принадлежность и ее параметры; материального носителя информации, на котором закреплены ее содержание и реквизиты.

В правовом смысле документом может быть признан не каждый носитель, содержащий информацию, а лишь тот, который имеет реквизиты, позволяющие его идентифицировать по отношении к собственнику, владельцу и пользователю информации. При этом одним из пробелов действующего законодательства является то, что конкретные признаки, позволяющие идентифицировать тот или иной документ, законом не установлены. Представляется, что свойства реквизитов и порядок идентификации документа должны определяться в каждом случае отдельно в зависимости от физических свойств носителя информации.

Одним из особых видов информации, подпадающих под правовое регулирование и уже закрепленных в российском уголовном законодательстве в качестве предмета неправомерного доступа, является компьютерная или машинная информация. В диссертации рассматриваются различные точки зрения относительно определения понятия компьютерной информации, приоритетным из которых является легальное толкование данного термина в уголовном законодательстве и определение под компьютерной информацией – информации на машинном носителе.

В итоге нами отмечено, что информационное законодательство содержит определение информации, соответствующее современному уровню законодательного регулирования информационных отношений, однако существенным недостатком при этом выступает отсутствие общих законодательных критериев определения реквизитов документированной информации, в первую очередь, подпадающей под правовое регулирование, а также отсутствие легального толкования таких понятий, как «машинный носитель», «ЭВМ», «система ЭВМ», «сеть ЭВМ», порождающее неоднозначные трактовки данных понятий в научной литературе и правоприменительной практике.

Третий параграф ***«Понятие и виды охраняемой законом информации»*** направлен на проведение анализа понятия и проведения классификации охраняемой законом информации.

По нашему мнению уголовно-правовые меры обеспечения информационной безопасности, в силу наибольшей строгости уголовной ответственности по сравнению с другими видами ответственности, могут быть направлены на защиту от неправомерного доступа не всякой информации, а только информации, охраняемой законом. Следовательно, возникает проблема отграничения данного вида информации от иного массива информационных ресурсов, не попадающих в сферу уголовно-правового регулирования.

Подвергнута критике точка зрения некоторых авторов, допускающих слишком широкое толкование понятия охраняемой законом информации и включающей туда всю документированную информацию. Основываясь на нормах информационного законодательства, определены критерии отнесения информации к категории охраняемой законом. В частности, указано, что в данном случае информация должна обладать определенной ценностью, а также наличием статуса ограниченного доступа.

Что касается порядка отнесения информации к информации с режимом ограниченного доступа, то в диссертационной работе не разделяется точка зрения ряда авторов о том, что для отнесения информации к категории охраняемой законом достаточно установления собственником (владельцем) порядка обращения с последней.

Однако, несмотря на то, что собственнику информации предоставлено право самостоятельно устанавливать режим доступа к ней, в данном случае он ограничен законом и может получить уголовно-правовую защиту лишь в отношении той информации, отнесение которой к конфиденциальной прямо предусмотрено правовыми актами. В противном случае произошло бы неоправданное расширение предмета уголовно-правового регулирования защиты информации. Та информация, которая имеет определенную ценность для собственника, но законодательными актами не определена как конфиденциальная, может быть защищена собственником правовыми средствами в гражданско-правовом или ином порядке.

Далее в работе отмечается то обстоятельство, что в настоящее время в российском законодательстве не существует четкой системы нормативно-правовых актов, касающихся обращения с информацией ограниченного доступа, а также четкого перечня видов информации с режимом ограниченного доступа. По подсчетам различных авторов в законодательстве упоминается до нескольких десятков различных видов конфиденциальной информации.

Что касается классификации конфиденциальной информации, то в диссертационной работе воспринят распространенный в литературе подход, классифицирующий охраняемую законом информацию, исходя из критерия принадлежности информации конкретному собственнику, либо владельцу. Отсюда

выделяют: личную конфиденциальную информацию, конфиденциальную информацию юридических лиц, государственную конфиденциальную информацию.

Как считает автор, охраняемая законом информация как предмет неправомерного доступа – это документированная информация, содержащая сведения, отнесенные законом к государственной тайне или конфиденциальной информации.

В данном разделе работы отмечается что, четкой системы законодательных актов, регулирующих отношения в области отнесения информации к категории закрытой, в настоящее время не существует, это зачастую порождает неоднозначные решения в уголовно-правовой теории и правоприменительной практике. При этом существующий у ряда авторов расширительный подход к проблеме отнесения информации к категории, охраняемой законом, не соответствует основным принципам криминализации деяний, требующим наличия в деяниях, относимым к преступным, такого признака, как общественная опасность. Практика показывает, что слишком широкое применение уголовной ответственности не всегда является эффективной мерой противодействия противоправным деяниям.
В сфере правовых мер защиты информации от неправомерного доступа еще не достаточно использован потенциал более мягких мер ответственности, в частности, дисциплинарной, административной, гражданской.

Вторая глава **«Уголовно-правовые меры защиты информации»** состоит из двух параграфов.

В параграфе первом **«*Правовые меры обеспечения информационной безопасности*»** автор обращает внимание на актуальность проблемы обеспечения информационной безопасности в Российской Федерации. Справедливо указывается на то, что информационная безопасность на современном этапе выступает важной составляющей национальной безопасности в целом.

Возникновение проблемы обеспечения информационной безопасности во многом обусловлено переходом современного общества от индустриального к информационному, а также значительным повышением социальной ценности информационных ресурсов.

В работе отмечено, что традиционно среди мер обеспечения информационной безопасности выделяют следующие меры: правовые, организационно-технические и экономические. Правовые меры, являющиеся базовыми, заключаются в формировании нормативно-правовой базы в области информатизации, отвечающей принципам полноты правового регулирования, устранения пробелов в системе нормативных актов, реализации принципов единства и отсутствия противоречивости законодательных норм.

Среди правовых мер обеспечения информационной безопасности важное место занимают уголовно-правовые меры, направленные на противодействие самым опасным правонарушениям в информационной сфере – информационным преступлениям.

Однако, несмотря на значимость информации, как объекта уголовно-правовой защиты, в современном российском уголовном законодательстве, а также в теории уголовного права не существует системного подхода к данной проблеме. В уголовном законодательстве самостоятельно обозначены лишь преступления в сфере компьютерной информации, хотя в современных условиях правомернее говорить о более широком понятии, а именно, о преступлениях в сфере информационных отношений, включающих в себя все общественно опасные деяния, совершенные в информационной сфере, а не только в сфере компьютерной информации.

При этом, в работе показано, что в УК РФ отсутствует такой видовой объект преступных посягательств как информационные отношения, а также то, что большинство преступлений в сфере информационных отношений рассредоточено по разным главам Уголовного кодекса Российской Федерации, и при этом информационные отношения в большинстве своем выступают дополнительным объектом преступных посягательств. Это позволяет говорить о том, что в современном российском уголовном праве не сформировано четкое понятие и не проведена классификация преступлений в сфере информационных отношений.

Введение в УК РФ главы 28 «Преступления в сфере компьютерной информации» не решает всех проблем обеспечения информационной безопасности уголовно-правовыми мерами.

В сложившейся ситуации предлагается предусмотреть в УК РФ самостоятельную главу, содержащую в себе систему преступлений в сфере информационных отношений. Первоначальным этапом формирования такой системы должно выступить внесение изменений в действующее уголовное законодательство, расширяющих предмет неправомерного доступа к охраняемой законом информации.

Во втором параграфе **«*Виды преступных посягательств на охраняемую законом информацию*»** автором предпринята попытка провести классификацию преступлений в сфере информационных отношений.

Выделены три группы данных преступлений. В частности, преступления, связанные с посягательством на саму информацию, с распространением «вредной» (вредоносной) информации, а также с посягательством на право граждан и иных субъектов на доступ к открытой информации.

При этом в первой группе выделены две подгруппы преступлений. В первом случае предметом преступных посягательств выступает информация, находящаяся на носителях определенного рода (статьи. 138, 142, 142.1, 185, 187, 198, 199, 272, 273, 292, 325, 326, 327, УК РФ).

Вышеуказанные уголовно-правовые запреты связаны с такими деяниями, как подделка (фальсификация, искажение), изготовление, повреждение, уничтожение, похищение носителей той или иной информации. Воздействуя на конкретный материальный носитель (бухгалтерский, избирательный, официальный документ, на компьютерные носители и т.п.), преступник стремится таким способом посягнуть на содержащиеся на нем сведения, с целью добиться, например, каких-либо имущественных выгод, избежать ответственности, изменить результаты выборов и т.п. Содержание информации и конкретно определенный ее носитель в указанных составах преступления неразрывно связаны и в равной мере защищаются уголовным законом.

Во втором случае информация выступает предметом преступных посягательств в зависимости от своего содержания независимо от типа носителя (статьи 137, 155, 146, 147, 183, 195, 202, 275, 276, 284, 310 УК РФ).

Предметом преступления здесь признаются сами сведения, при этом, учитывая то, что в конечном счете указанная информация содержится на определенных материальных носителях (в широком смысле). Вид носителей в данном случае (бумага, фотопленка, магнитный диск и т.п.) и форма представления информации (письменная, устная, визуальная, в виде рисунков, чертежей и т.п.) не имеют значения.

Вторую группу преступлений в сфере информационных отношений составляют общественно опасные посягательства, предметом которых является так называемая «вредная» (вредоносная) информация (статьи 129, 130, 189, 242.1 УК РФ).

Третья группа преступлений в сфере информационных отношений связана с посягательствами на право каждого на доступ к открытой информации.

Эти преступления связаны с непредставлением общедоступной информации (статья 140 УК РФ), либо с предоставлением данной информации в ненадлежащем виде (ложной или искаженной, неполной) – статьи 237, 306, 307 УК РФ).

В работе определено, что приоритетным предметом уголовно-правовой защиты выступает охраняемая законом информация. При этом наиболее распространенным и влекущим наиболее значительные общественно опасные последствия является такой способ преступных манипуляций с данной информацией как неправомерный доступ.

Третья глава **«Уголовно-правовое регулирование неправомерного доступа к охраняемой законом информации»** состоит из трех параграфов.

В параграфе первом **«*Порядок уголовно-правового регулирования неправомерного доступа к компьютерной информации*»** основываясь на том, что единый порядок уголовно-правового регулирования неправомерного доступа к охраняемой законом информации в ныне действующем УК РФ не установлен, автор сначала обращается к уже закрепленному в уголовном законодательстве преступлению, являющемуся частным случаем неправомерного доступа к охраняемой законом информации, а именно, к неправомерному доступу к компьютерной информации.

Проведен анализ всех основных элементов состава преступления, предусмотренного статьей 272 УК РФ.

Под непосредственным объектом данного преступления понимаются отношения, обеспечивающие безопасность (неприкосновенность) компьютерной информации, а также безопасную (нормальную) эксплуатацию (работу) ЭВМ, системы ЭВМ или сети ЭВМ.

При определении предмета данного преступления в работе акцентируется внимание на толковании понятия «машинный носитель» и рассмотрении их видов (устройства памяти ЭВМ, периферийные устройства ЭВМ, компьютерные свойства связи, сетевые устройства и сети электросвязи). Кроме этого, подробно раскрываются понятия таких технических устройств, содержащих машинные носители, как «ЭВМ», «система ЭВМ» и «сеть ЭВМ».

При анализе объективной стороны подробно рассмотрен вызывающий неоднозначные трактовки термин «доступ», а также раскрыты последствия неправомерного доступа к охраняемой законом компьютерной информации – уничтожение, блокирование, модификацию или копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети.

При этом анализ последствий производится с учетом предложенной схемы трех уровней представления компьютерной информации (физического, логического и семантического). Там же автором рассмотрены пробелы построения диспозиции статьи 272 УК РФ.

Отмечено, что субъективная сторона неправомерного доступа к охраняемой законом информации характеризуется умышленной формой вины, как в форме прямого, так и косвенного умысла. Так же рассмотрен вопрос о возможности установления уголовной ответственности за неправомерный доступ к

охраняемой законом компьютерной информации с неосторожной формой вины. Рассмотрены особенности субъекта данного преступления.

Во втором параграфе «***Приоритетность уголовно-правовой защиты компьютерной информации***» рассмотрена основная проблема, касающаяся защиты от неправомерного доступа охраняемой законом информации, а именно на недостаточно обоснованной приоритетности уголовно-правовой защиты компьютерной информации, по сравнению с другими видами информации.

Данный вывод основан на том, что информационное законодательство не вводит разграничения информации по ее носителям, классифицируя последнюю, лишь, по режиму доступа.

Отсюда следует такой явный признак ныне действующего уголовного законодательства, как нелогичность построения уголовных норм защиты охраняемой законом информации от неправомерного доступа. Данную нелогичность можно обнаружить при системном анализе различных статей УК РФ, а также норм иных отраслей права.

Предпосылками данного анализа является существование в УК РФ двух разноуровневых критериев классификации охраняемой законом информации, в частности:

– по содержанию, например, личная или семейная тайны, коммуникационные тайны (тайна переписки, почтовых, телеграфных или иных сообщений), коммерческая или банковская тайны, государственная тайна и т.п.;

– по типу носителя (компьютерная и иная информация).

Наличие данных, часто взаимно независимых критериев классификации, ведет к следующим последствиям.

Во-первых, при наличии только первого критерия уголовно-правовой защите от неправомерного доступа подлежит охраняемая законом информация, специально указанная в различных статьях УК РФ, за исключением статьи 272 УК РФ. Например, собирание сведений, составляющих коммерческую или банковскую тайну, находящихся на бумажных носителях в целях разглашения, либо незаконного использования этих сведений, влечет ответственность по части 1 статьи 183 УК РФ.

Во-вторых, при пересечении данных критериев одинаковая по содержанию информация получает приоритетную защиту в силу ее нахождения на машинном носителе.

Основываясь на первом примере, можно указать, что, если сбор сведений, составляющих коммерческую или банковскую тайну, производился путем правомерного доступа к той же информации, но уже находящейся на машинных носителях, данные действия должны квалифицироваться по совокупности статей 183 и 272 УК РФ.

Получается, что второе деяние имеет большую степень общественной опасности, чем первое, хотя, как уже неоднократно указывалось, носитель не имеет самостоятельного значения для определения социальной ценности находящейся на нем информации.

В-третьих, при наличии лишь того критерия, что охраняемая законом информация находится на машинном носителе, часть информации с ограниченным режимом доступа, находящаяся на иных носителях, выпадает из сферы уголовно-правовой защиты.

Например, персональные данные, отнесенные Федеральным законом «Об информации…» к конфиденциальной информации, являются предметом неправомерного доступа в соответствии со статьей 272 УК РФ в том случае, если они находятся на машинных носителях. Если же данные сведения находятся на иных типах носителей, то неправомерный доступ к ним влечет ответственность в соответствии со статьей 13.11 Кодекса Российской Федерации об административных правонарушениях (нарушение установленного законом порядка сбора, хранения, использования или распространения информации о гражданах (персональных данных)).

Понятие «компьютерные преступления» изначально возникло как определение традиционных преступлений (например, кражи и мошенничества), совершаемых с помощью компьютерной техники (только как критерий определения способа совершения преступления). Позднее, основываясь на исследованиях криминалистов, к компьютерным преступлениям стали относить также преступления, совершенные в отношении компьютерной информации, т.е. компьютерная информация была признана объектом преступлений. Основываясь на этом, в работе делается вывод о том, что появление в уголовном праве, в том числе и российском, компьютерных преступлений, обусловлено во многом влиянием криминалистики и криминологии.

С одной стороны, появление угрозы неправомерного доступа к информации с помощью компьютерной техники, а также специфика данного способа совершения преступления, привели к осознанию социальной ценности информации с ограниченным доступом и необходимости ее уголовно-правовой защиты. С другой стороны, ныне существующее признание предметом неправомерного доступа лишь компьютерной информации, позволяет говорить лишь о частичности или «однобокости» уголовно-правовой защиты информации с ограниченным доступом, поэтому уголовному праву на современном

этапе необходимо перейти от «частных» случаев защиты информации от неправомерного доступа к более общему подходу и не ставить пределы данной защиты в зависимость от вида носителей информации.

В отношении защиты информации от неправомерного доступа, объектом данной защиты должен выступить весь массив информации с ограниченным доступом, а не только компьютерная информация, и в данном смысле в отношении компьютерной информации правомернее говорить о способе совершения неправомерного доступа к охраняемой законом информации (с использованием компьютерной техники или иных специальных средств).

Решение проблемы включения в сферу уголовно-правового регулирования защиты информации с ограниченным доступом всего массива данной информации возможно путем введения в уголовное законодательство общего состава, устанавливающего ответственность за неправомерный доступ не только к компьютерной информации, но и к охраняемой законом информации вообще.

В третьем параграфе **«*Проблемы уголовно-правового регулирования неправомерного доступа к охраняемой законом информации*»** рассматривается проблема разработки общего состава преступления, устанавливающего уголовную ответственность за неправомерный доступ к охраняемой законом информации независимо от типа носителя данной информации.

При этом в качестве модели используется уже закрепленный в уголовном законодательстве состав неправомерного доступа к компьютерной информации, предусмотренный статьей 272 УК РФ.

В работе были определены и раскрыты все элементы моделируемого состава преступления, а именно, объект, объективная сторона, субъективная сторона и субъект.

Непосредственным объектом неправомерного доступа к охраняемой законом информации должны выступать общественные отношения, обеспечивающую безопасность информации (сохранение ее конфиденциальности, целостности и доступности) с режимом ограниченного доступа.

В свою очередь, видовым объектом данного преступления должна выступать часть информационных общественных отношений, направленных на обеспечение информационной безопасности, а родовым объектом – отношения общественной безопасности. Что касается конкретного расположения нового состава в Особенной части УК РФ, то следует отметить следующее. Поскольку информационные отношения как видовой объект преступлений в уголовном законодательстве не выделены, в частности, в отдельную главу УК РФ, а глава 28 «Преступления в сфере компьютерной информации» не охватывает совокупности всех отношений информационной безопасности, есть практический смысл переименовать главу 28 УК РФ и обозначить ее как «Преступления в сфере информационных отношений». При этом необходимость переименования данной главы обусловлена не только данным частным случаем, но и проблемой необходимости формирования системы преступлений в сфере информационных отношений вообще.

При этом преступления в сфере компьютерной информации выступят частью преступлений в сфере информационных отношений. В свою очередь, состав неправомерного доступа к охраняемой законом информации выступит частью системы информационных преступлений.

Что касается предмета нового состава, то им выступит охраняемая законом информация, определенная нами как документированная информация, содержащая сведения, отнесенные законом к государственной тайне или конфиденциальной информации.

Объективная сторона состава данного преступления, при наличии целого ряда положительных моментов, построение диспозиции статьи 272 УК РФ имеет ряд недостатков, не позволяющих полностью обеспечить уголовно-правовую защиту данного вида информации от неправомерного доступа.

Поскольку предметом нового состава выступает охраняемая законом информация, то формулировка, содержащаяся в статье 272 УК РФ, «охраняемой законом компьютерной информации, т.е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети» подлежит замене на формулировку «охраняемой законом информации, т.е. документированной информации, содержащей сведения, отнесенные законом к государственной тайне или конфиденциальной информации».

Под доступом следует понимать ознакомление с охраняемой законом информацией и (или) получение возможности совершать операции с данной информацией, в частности, ее копирование, блокирование, модификацию и уничтожение. При этом не имеет принципиального значения тот факт, осуществляется доступ к самой информации или к ее носителям.

Данная формулировка термина «доступ» позволяет обеспечить комплексность защиты информации от неправомерного доступа и обеспечить ее конфиденциальность, целостность и доступность.

Что касается рассмотрения последствий данного доступа, то формулировка, содержащаяся в статье 272 УК РФ, а именно, «если это деяние повлекло уничтожение, блокирование, модификацию либо ко-

пирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети» также требует определенной доработки.

Во-первых, такие последствия, как нарушение работы ЭВМ, системы ЭВМ или их сети, имеют смысл лишь при доступе к компьютерной информации, однако в том случае, если предметом неправомерного доступа является охраняемая законом информация, независимо от типа носителя, правомерно исключить данное последствие из диспозиции нового состава.

Однако при этом возникает проблема декриминализации данных последствий, которые объективно являются общественно опасными. Выходом из данной ситуации может выступить отражение данных последствий в статье 274 УК РФ (нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети).

Диспозиция статьи 274 УК РФ представлена как нарушение 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.

Неправомерный доступ к компьютерной информации вполне можно отнести к нарушению правил эксплуатации ЭВМ, системы ЭВМ или их сети, поскольку данные правила однозначно должны содержать критерии определения субъектов, имеющих права доступа к ЭВМ, системе ЭВМ или их сети. Однако статья 274 УК РФ содержит ограничение, состоящие в том, что субъектом преступления, установленного данной статьей, может являться лишь лицо, имеющее доступ к ЭВМ, системе ЭВМ или их сети. В силу этого следует расширить субъектный состав данного преступления и отразить его следующим образом: «… лицом, имеющим доступ или неправомерно получившим доступ к ЭВМ, системе ЭВМ, или их сети…».

Во-вторых, перечень иных последствий неправомерного доступа к компьютерной информации требует также определенного уточнения. Сформулированные в статье 272 УК РФ, как «…если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации…» допускает неоднозначное толкование данных последствий, выражающееся в следующем.

С одной стороны, предметом неправомерного доступа является охраняемая законом информация. С другой стороны, определение последствий как «уничтожение, блокирование, модификацию либо копирование информации» допускает такое толкование, что, например, может быть уничтожена любая другая информация, а не только охраняемая законом. По мнению автора, данный вариант теоретически вполне возможен, когда доступ к охраняемой законом информации влечет последствия в виде уничтожения, блокирования, модификации либо копирования информации иного рода. В силу этого, следует внести в перечень последствий уточнение и обозначить их как «…если это деяние повлекло уничтожение, блокирование, модификацию либо копирование данной информации…».

В работе обозначена диспозиция общего состава неправомерного доступа к охраняемой законом информации в следующем виде: «1. Неправомерный доступ к охраняемой законом информации, т.е. документированной информации, содержащей сведения, отнесенные законом к государственной тайне или конфиденциальной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование данной информации, – …».

Помимо этого, в работе уточняется и то обстоятельство, что если законодатель считает, что использование технических средств (в том числе компьютерной техники) повышает общественную опасность деяний определенного рода, то необходимо предусмотреть этот признак в качестве квалифицирующего.

В данном случае это выражается в необходимости наличия второй части разрабатываемой статьи УК РФ. При этом конкретная формулировка будет выражаться в следующем виде: «2. То же деяние, совершенное лицом с использованием ЭВМ, системы ЭВМ или их сети…». Кроме этого, имеет смысл сохранить такие квалифицирующие признаки, отраженные в части 2 статьи 272 УК РФ, как «…совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения». Такой признак, как совершение неправомерного деяния лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, в нашем случае не имеет смысла сохранять, поскольку отражает отношение лица к носителю информации, который в конструируемом нами составе значения не имеет.

Конечный результат формулировки второй части статьи можно представить в следующем виде: «2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения или с использованием ЭВМ, системы ЭВМ или их сети».

Что касается субъективной стороны данного состава преступления, то по аналогии с неправомерным доступом к компьютерной информации данное преступление может быть совершено только умышленно: с прямым или косвенным умыслом.

Субъект преступления также по аналогии с неправомерным доступом к охраняемой законом информации определен автором как общий субъект, а именно вменяемое физическое лицо, достигшее 16-летнего возраста.

Таким образом, предложенный в работе состав, устанавливающий уголовную ответственность за неправомерный доступ к охраняемой законом информации, является лишь одним звеном в системе преступлений в сфере информационных отношений. Состав неправомерного доступа к охраняемой законом информации должен выступить основным составом, направленным на защиту информации охраняемой законом, от действий, нарушающих ее конфиденциальность, целостность и доступность. В свою очередь, данное исследование выступает лишь частью решения проблемы необходимости разработки системы преступлений в сфере информационных отношений.

В заключении диссертации подводятся итоги и излагаются основные выводы, предложения и рекомендации.

Обеспечение безопасности является важной функцией государственной власти. Одной из важнейших составляющих национальной безопасности в современных условиях формирования информационного общества является обеспечение информационной безопасности, а также защита охраняемой законом информации от неправомерного доступа. Данное обстоятельство определяется значительной социальной ценностью информационных ресурсов, имеющих режим ограниченного доступа. Приоритетную роль в обеспечении безопасности наиболее ценной информации принадлежит мерам уголовно-правового регулирования.

Несмотря на то, что информационные ресурсы в современном обществе объективно обладают значительной ценностью, действующее уголовное законодательство не содержит комплексного подхода к проблеме обеспечения информационной безопасности уголовно-правовыми мерами. Данное обстоятельство обусловлено тем, что информационные отношения не представлены в действующем УК РФ в качестве самостоятельного объекта защиты. Уголовное законодательство ограничивается лишь фрагментарными мерами защиты охраняемой законом информации в зависимости от ее содержания или типа носителя.

На современном этапе развития процесса информатизации в России возникла необходимость разработки в уголовном законодательстве системы преступлений в сфере информационных отношений, составной частью которых должны выступить уже закрепленные в УК РФ преступления в сфере компьютерной информации.

Разработка категории преступлений в сфере информационных отношений применительно к неправомерному доступу также обусловлена особенностями системы современного российского информационного законодательства. Данная система основана на единственном критерии классификации информации как объекта правового регулирования: разделении информации по содержанию на общедоступную и с режимом ограниченного доступа. Данная классификация воспринята действующим уголовным законодательством лишь частично и имеет еще один критерий классификации информации, основанный на типе носителя. В частности, в УК РФ выделена категория «компьютерной информации». Данные обстоятельства являются причиной того, что в действующем законодательстве уголовно-правовые меры защиты информации от неправомерного доступа реализованы непоследовательно и несистемно.

Возникает необходимость внесения изменений в действующее уголовное законодательство, обеспечивающих полноту защиты всего массива охраняемой законом информации от неправомерного доступа, в частности разработки общего состава неправомерного доступа к охраняемой законом информации.

При разработке элементов состава неправомерного доступа к охраняемой законом информации автор пришел к выводу, что преступления в сфере компьютерной информации являются составной частью преступлений в сфере информационных отношений, а также неправомерный доступ к охраняемой законом информации не входит в понятие преступлений в сфере компьютерной информации, потому необходимо название главы 28 УК РФ представить как «Преступления в сфере информационных отношений».

Было установлено, что предметом неправомерного доступа будет являться весь массив документированной информации, содержащей сведения, отнесенные законом к государственной тайне или конфиденциальной информации (информация, охраняемая законом).

При разработке объективной стороны состава неправомерного доступа к охраняемой законом информации за основу была взята диспозиция статья 272 УК РФ (неправомерный доступ к компьютерной информации). При этом был внесен ряд уточнений, касающихся построения диспозиции статьи в новой редакции.

Автором было установлено, что под доступом к информации следует понимать ознакомление с охраняемой законом информацией и (или) получение возможности совершать операции с данной инфор-

мацией, в частности, ее копирование, блокирование, модификацию и уничтожение. При этом не имеет принципиального значения тот факт, осуществляется доступ к самой информации или к ее носителям.

Была сохранена модель построения неправомерного доступа в качестве материального. Основываясь на данном анализе, было предложено диспозицию статьи 272 УК РФ изложить в следующей редакции:

«Статья 272. Неправомерный доступ к охраняемой законом информации.

1 Неправомерный доступ к охраняемой законом информации, т.е. документированной информации, содержащей сведения, отнесенные законом к государственной тайне или конфиденциальной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование данной информации, – …

2 То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения или с использованием ЭВМ, системы ЭВМ или их сети, – …».

Важным выводом исследования является то, что состав неправомерного доступа к охраняемой законом информации должен выступить частью общей системы преступлений в сфере информационных отношений, требующей дальнейшего достаточно серьезного научного исследования.

По теме диссертации автором опубликованы следующие работы:

1 Числин В.П. Криминалистический портрет и свойства личности как субъекта информационных компьютерных преступлений / В.П. Числин, В.Н. Чернышов // Политика. Власть. Право: Межвуз. сб. науч. ст. – СПб.: Изд-во Юридического ин-та (Санкт-Петербург), 2000. Выпуск IV (II) – 0,5 п.л. (Числин В.П. – 0,3 п.л.)

2 Числин В.П. Классификация способов и механизмов совершения преступлений в сфере компьютерной информации / В.П. Числин // Вопросы правоведения. – Тамбов.: Изд-во Тамб. гос. техн. ун-та, 2003. – 0,5 п.л.

3 Числин В.П. Уголовно-правовые меры защиты информации / В.П. Числин. – М.: ИМПЭ Паблик, 2003. – 1,5 п.л.

4 Числин В.П. Информация как объект уголовно-правовой защиты / В.П. Числин. – М.: МАКС Пресс, 2004. – 1,8 п.л.