На правах рукописи

Ефремова Марина Александровна

УГОЛОВНО-ПРАВОВАЯ ОХРАНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специальность 12.00.08 – «Уголовное право и криминология; уголовно-исполнительное право»

Автореферат
диссертации на соискание ученой степени
доктора юридических наук

Москва – 2018

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Академия Генеральной прокуратуры Российской Федерации»

Научный консультант: доктор юридических наук, доцент **Агапов Павел Валерьевич**

Официальные оппоненты: **Кузнецов Александр Павлович** доктор юридических наук, профессор, ФГКОУ ВО «Нижегородская академия Министерства внутренних дел Российской Федерации», кафедра уголовного и уголовно-исполнительного права, профессор

Цепелев Валерий Филиппович доктор юридических наук, профессор, ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», кафедра уголовного права, профессор

Лопатина Татьяна Михайловна доктор юридических наук, профессор, ФГБОУ ВО «Смоленский государственный университет», кафедра права, заведующая

Ведущая организация: ФГБОУ ВО «Государственный университет управления»

Защита диссертации состоится 17 мая 2018 г. в 14.30 на заседании диссертационного совета Д 170.001.02 в Академии Генеральной прокуратуры Российской Федерации по адресу: 123022, Москва, ул. 2-я Звенигородская, 15, конференц-зал.

С диссертацией и авторефератом можно ознакомиться в библиотеке Академии Генеральной прокуратуры Российской Федерации по адресу: 123022, Москва, ул. 2-я Звенигородская, 15.

С электронной версией автореферата можно ознакомиться на официальном сайте Академии Генеральной прокуратуры Российской Федерации: http://www.agprf.org, а также на сайте Высшей аттестационной комиссии при Министерстве образования и науки Российской Федерации: http://vak.ed.gov.ru

Автореферат разослан 12.02.2018 года.

Ученый секретарь
диссертационного совета Н.В. Буланова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования обусловлена тем, что роль информации в жизни личности, общества и государства в последние годы не просто значительно возросла, а отчасти стала одной из основ развития. В Российской Федерации, вслед за ведущими мировыми державами, начался процесс становления информационного общества, основу которого составляют информация и знания. Орудием труда в информационном обществе становятся информационные технологии. В Послании Федеральному Собранию Российской Федерации Президент В.В. Путин подчеркнул, что IT-индустрия стала одной из самых быстроразвивающихся отраслей, объем экспорта которой составляет 7 миллиардов долларов[1].

В связи со становлением информационного общества перед государством появляются новые задачи. Одна из таких задач – обеспечение информационной безопасности. Не случайно вопросы обеспечения информационной безопасности включены практически во все разделы, посвященные реализации стратегических национальных приоритетов, новой редакции Стратегии национальной безопасности Российской Федерации[2]. Обозначенные в Стратегии положения получили свое развитие и в новой редакции Доктрины информационной безопасности Российской Федерации[3]. В этом документе не только дана оценка современному состоянию информационной безопасности Российской Федерации, но и определен перечень угроз, а также совокупность средств, способных обеспечить должный уровень защиты информационной безопасности Российской Федерации. При этом правовые средства обеспечения

---

[1] Послание Президента Российской Федерации Федеральному Собранию Российской Федерации 01.12.2016. URL: http://kremlin.ru/events/president/news/53379 (дата обращения: 01.12.2016).

[2] Стратегия национальной безопасности Российской Федерации (утв. Указом Президента РФ от 31.12.2015. № 683). URL: http://www.scrf.gov.ru/security/docs/document133/ (дата обращения: 15.01.2016).

[3] Доктрина информационной безопасности Российской Федерации (утв. Указом Президента РФ от 05.12.2016 № 646). URL: http://www.scrf.gov.ru/documents/1/133.html (дата обращения: 15.01.2017).

информационной безопасности отнесены к приоритетному направлению деятельности.

На современном этапе к правовым средствам обеспечения информационной безопасности Российской Федерации следует отнести необходимость подготовки и принятия новых нормативных правовых актов, а также уточнение существующих концептуальных и доктринальных документов, которые адекватно отражали бы национальные интересы России, в том числе в информационной сфере, и способствовали бы реализации задач обеспечения информационной безопасности Российской Федерации, исходя из динамики современных угроз информационной безопасности Российской Федерации[4]. Безусловно, это комплексная задача и она не только может, но и должна быть реализована в рамках различных отраслей права. Наряду с другими отраслями права особое место в механизме правового обеспечения информационной безопасности должно занять уголовное право.

Следует отметить, что информационные отношения стали объектом преступного посягательства и получили в действующем Уголовном кодексе Российской Федерации (далее – УК РФ) определенную уголовно-правовую защиту. Подтверждением этому служат уголовно-правовые нормы, включенные законодателем в главу 28 УК РФ «Преступления в сфере компьютерной информации». Однако за последние несколько лет компьютерная преступность существенно трансформировалась и проникла в экономическую сферу и нашла проявление в таких преступлениях как незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну; мошенничество в сфере компьютерной информации, также и в сферу частной жизни граждан, о чем свидетельствует рост совершения таких преступлений, как нарушение неприкосновенности частной жизни, нарушение тайны переписки с использованием информационно-телекоммуникационных технологий, в том числе сети

[4] Куняев Н.Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: дис. … д-ра юрид. наук. – М., 2010. – С. 321.

Интернет. Расширение сфер областей применения информационных и информационно-телекоммуникационных технологий позволяет прогнозировать и дальнейший рост киберпреступности, появление новых видов и форм преступлений против информационной безопасности Российской Федерации.

В настоящее время в России отсутствует уголовная политика в сфере противодействия преступлениям против информационной безопасности. Действующее уголовное законодательство уже исчерпало свой как профилактический, так и карательный потенциал в этой сфере. Находящиеся в различных разделах и главах Особенной части УК РФ нормы, направленные на обеспечение информационной безопасности, лишенные институциональных связей друг с другом, имеющие существенные юридико-технические различия едва ли могут быть способными эффективно реагировать на стремительно меняющиеся реалии. Поэтому сегодня одним из актуальных вопросов в науке уголовного права является исследование проблемы уголовно-правовой охраны информационной безопасности.

Степень научной разработанности темы исследования. Вопросы правового обеспечения информационной безопасности нашли отражение в трудах таких ученых, как И.Л. Бачило, Г.Г. Горшенков, В.Н. Лопатин, В.А. Копылов, П.У. Кузнецов, Н.Н. Куняев, Т.А. Полякова, А.А. Стрельцов и других. Все они внесли существенный вклад в разработку обозначенной проблематики с позиции информационного права.

В юридической литературе проблема уголовно-правовой охраны информационной безопасности изучена мало, хотя отдельные ее аспекты становились объектом научных исследований. Большинство работ затрагивают лишь отдельные вопросы охраны информации.

Так, уголовно-правовым аспектам охраны компьютерной информации были посвящены работы Р.М. Айсанова, Ю.М. Батурина, С.Д. Бражника, С.Ю. Бытко, А.Г. Волеводза, В.В. Воробьева, В.И. Гладких, М.Ю. Дворецкого, К.Н. Евдокимова, Д.А. Зыкова, А.Ж. Кабановой, В.С. Карпова, А.П. Кузнецова,

Т.М. Лопатиной, Д.Г. Малышенко, Т.Г. Смирновой, В.Г. Степанова-Егиянца, С.И. Ушакова, А.Е. Шаркова и других.

Отдельные вопросы уголовно-правовой охраны информационных отношений поднимались в исследованиях В.Н. Додонова, А.Ф. Жигалова, Р.В. Жубрина, У.В. Зининой, О.С. Капинус, Л.Р. Клебанова, В.А. Мазурова, Н.И. Пикурова, А.А. Рожнова, И.В. Смольковой, А.А. Тер-Акопова, А.А. Фатьянова, В.Ф. Цепелева, С.П. Щербы, И.А. Юрченко и других.

Непосредственно уголовно-правовой охране информационной безопасности были посвящены работы Л.А. Букалеровой[5], Д.А. Калмыкова[6], Е.А. Красненковой[7].

Данные работы заложили научные основы уголовно-правовой охраны информационной безопасности в Российской Федерации. Однако с тех пор уголовное законодательство претерпело изменения. При этом проблема уголовно-правовой охраны информационной безопасности осталась неразрешенной как на практическом, так и теоретическом уровне. Например, не решен вопрос о том, какие посягательства следует относить к преступлениям против информационной безопасности, не сформулировано само понятие информационной безопасности как объекта уголовно-правовой охраны, не выработана четкая позиция по вопросу совершенствования УК РФ в части противодействия преступлениям против информационной безопасности. В этой связи информационная безопасность как объект уголовно-правовой охраны нуждается в дальнейшем исследовании и изучении.

Объект и предмет исследования. Объектом диссертационного исследования выступают правоотношения по обеспечению информационной безопасности, в том числе посредством установления и реализации уголовной

---

[5] Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: дис. … д-ра юрид. наук. – М., 2007.

[6] Калмыков Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны: дис. … канд. юрид. наук. – Ярославль, 2005.

[7] Красненкова Е.А. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: дис. … канд. юрид. наук. – М., 2006.

ответственности за посягательства на нее.

Предмет исследования составляют нормы международного права, зарубежного законодательства, нормы уголовного законодательства Российской Федерации, положения иных нормативных актов, направленных на обеспечение информационной безопасности РФ, а также практика применения вышеуказанных норм.

Цель и задачи исследования. Цель исследования состоит в разработке теоретических основ уголовно-правовой охраны информационной безопасности Российской Федерации, предложений по совершенствованию правового регулирования в указанной сфере и практики правоприменения.

Задачи диссертационного исследования обусловлены целью и состоят в следующем:

1. исследовать понятие информационной безопасности;
2. разработать методологические основы изучения информационной безопасности;
3. проанализировать социальную обусловленность уголовно-правовой охраны информационной безопасности;
4. сформулировать понятие информационной безопасности как объекта уголовно-правовой охраны;
5. рассмотреть международно-правовые основы охраны информационной безопасности;
6. провести сравнительное исследование составов преступлений против информационной безопасности по уголовному законодательству Российской Федерации и уголовному законодательству зарубежных стран;
7. дать уголовно-правовую характеристику составов преступлений против информационной безопасности по уголовному законодательству Российской Федерации;
8. определить способы совершенствования уголовно-правовой охраны информационной безопасности в Российской Федерации;
9. разработать комплекс изменений и дополнений в действующий УК РФ.

Методология и методика исследования. Методологическую основу диссертационного исследования составляет совокупность философских, общенаучных и частнонаучных методов научного познания, среди которых: формально-логический, сравнительно-правовой, историко-правовой, социологический (анкетирование, обобщение материалов уголовных дел, экспертные оценки).

В основу научного исследования положен системный подход, заключающийся в исследовании информационной безопасности как системы общественных отношений, которая регулируется различными отраслями российского права.

Теоретическую основу исследования составили научные исследования, изложенные в трудах ученых в области общей теории права, ведущих российских и зарубежных ученых в области информационного права, уголовного права, социологии уголовного права, криминологии, административного права, а также других, имеющих отношение к проблематике проводимого исследования, гуманитарных наук.

Нормативную основу исследования образуют: Конституция Российской Федерации; нормы российского уголовного, уголовно-процессуального, уголовно-исполнительного и административного законодательства; положения иных нормативных правовых актов, а также нормы зарубежного уголовного законодательства.

Эмпирическая база исследования базируется на:

− данных, полученных в результате анализа и обобщения обвинительных заключений, постановлений органов предварительного расследования и приговоров судов, по 250 уголовным делам о посягательствах на информационную безопасность;

− итогах обобщения опубликованной в справочной правовой системе «КонсультантПлюс» практики высших судебных инстанций Российской Федерации за период с 1996 по 2016 гг.;

− результатах анализа статистической отчетности МВД России за период с 1996 по 2016 гг.;

− результатах социологического исследования (опроса) 200 сотрудников правоохранительных органов (следователей, дознавателей, прокуроров) и судей;

− результатах анализа и обобщения материалов, опубликованных в средствах массовой информации, размещенных в сети Интернет, аналитических обзоров, справок, отчетов федеральных органов исполнительной власти, правоохранительных органов.

Использованные в процессе проведения исследования методы, объем изученного материала, личные наблюдения автора позволяют сделать вывод о репрезентативности проведенного исследования, достоверности научных выводов и достаточной обоснованности предложенных рекомендаций.

Научная новизна состоит в разработке совокупности теоретических положений об уголовно-правовой охране информационной безопасности Российской Федерации в условиях становления информационного общества.

Основные положения, отвечающие критерию научной новизны, могут быть сведены к следующему:

− обоснован авторский подход о выделении информационной безопасности в качестве самостоятельного объекта уголовно-правовой охраны и сформулировано ее определение;

− разработана нелинейная классификация структуры информационной безопасности как объекта уголовно-правовой охраны;

− обоснован системный характер информационной безопасности и на его основе выявлена потребность в институционализации ответственности за преступления против информационной безопасности путем выделения раздела в Особенной части УК РФ и интеграции видовых объектов;

− выявлены факторы, обусловливающие необходимость усиления уголовно-правовой охраны информационной безопасности в условиях

становления информационного общества в Российской Федерации и обновления документов стратегического планирования;

– предложены модели криминологического прогноза о динамике преступлений, совершенных в сфере телекоммуникаций и компьютерной информации, до 2019 г. включительно путем метода экстраполяции динамических рядов с использованием линейной и полиноминальной моделей тренда;

– в научный оборот впервые введено понятие преступлений против информационной безопасности;

– доктрина уголовного права дополнена понятиями «преступления против права на информацию и защиты информации от неправомерного доступа», «преступления против безопасности информационного ресурса»; «преступления против безопасности информационно-телекоммуникационных технологий»;

– разработан и теоретически обоснован проект раздела Особенной части УК РФ «Преступления против информационной безопасности»;

– на основе выявленных закономерностей развития многосторонней сущности информационной безопасности и взаимосвязи ее элементов внесены предложения по совершенствованию действующих уголовно-правовых норм, предусматривающих ответственность за преступления против информационной безопасности de lege ferenda.

Основные положения, выносимые на защиту:

1. *Предложения относительно общетеоретических основ уголовно-правовой охраны информационной безопасности.*

1.1. Дуалистическая сущность информационной безопасности проявляется в двух основных качествах. С одной стороны, она является частью национальной безопасности и в этом качестве выступает одним из элементов сложной многоуровневой системы различных видов безопасности, направленной на достижение состояния защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются

реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. С другой стороны, информационную безопасность следует рассматривать как объект уголовно-правовой охраны. В этом качестве она представляет собой открытую динамичную систему общественных отношений, обеспечивающих реализацию интересов личности, общества и государства в информационной сфере.

1.2. Несмотря на то, что во вновь принятых концептуальных документах, касающихся информационной безопасности, не акцентировано внимание на необходимости соблюдения «баланса интересов», эта проблема остается актуальной. Баланс интересов обеспечивается системным характером правового регулирования, предполагающим обеспечение информационной безопасности различными отраслями права. Баланс интересов в уголовном праве предполагает установление уголовной ответственности за посягательства на интересы, как личности, так и общества, и государства в информационной сфере. При этом нельзя нормативно закреплять преимущественное положение интересов отдельного субъекта, так как это приведет к нарушению системных (конституционных по своей природе) свойств такого сложного объекта уголовно-правовой охраны как информационная безопасность.

1.3. Структура информационной безопасности как объекта уголовно-правовой охраны включает в себя:

1) общественные отношения, обеспечивающие реализацию права на информацию и на охрану информации от неправомерного доступа;

2) общественные отношения, обеспечивающие безопасность информационных ресурсов;

3) общественные отношения, обеспечивающие безопасность использования информационно-телекоммуникационных технологий.

1.4. Социально-экономическая обусловленность уголовно-правовой охраны информационной безопасности связана с развитием в нашей стране

нового типа общества, в котором во главе угла стоят информация и информационные технологии. Экономическое развитие государства также зависит от этих технологий – сырьевая экономика превращается в экономику цифровую. Духовные и социальные потребности у людей переориентированы на быстрый поиск необходимой информации, своевременное и полное получение достоверной и качественной информации, возможность оперативного обмена ею.

1.5. Авторская концепция о выделении информационной безопасности в качестве самостоятельного объекта уголовно-правовой охраны, согласно которой в Особенной части УК РФ необходимо предусмотреть раздел «Преступления против информационной безопасности», состоящий из трех глав: «Преступления против права на информацию», «Преступления против безопасности информационных ресурсов», «Преступления против безопасности информационно-телекоммуникационных технологий», следовательно, информационная безопасность будет выступать родовым объектом. Однако данное предложение может быть успешно реализовано лишь в случае принятия новой редакции УК РФ.

1.6. На основании исследования международно-правовых норм в области охраны информационной безопасности, синхронного сравнения норм российского уголовного законодательства и уголовного законодательства зарубежных стран в работе обозначается определенная новая тенденция в развитии уголовного законодательства, как на международном, так и национально-государственном уровнях, направленная на систематизацию преступлений против информационной безопасности. Данная тенденция находит свое конкретное воплощение в предложении о необходимости принятия международного правового акта, направленного на уголовно-правовую охрану информационной безопасности, содержащего классификацию преступлений против информационной безопасности и рекомендации государствам по криминализации деяний против информационной безопасности в национальном законодательстве.

1.7. Правом на информацию следует считать самостоятельное личное право, включающее правомочия по свободному поиску, получению, передаче, производству, распространению информации, ограничению доступа к информации. Вытекающее из Конституции Российской Федерации и нашедшее отражение в Федеральном законе право на информацию обнаруживает тесную связь с другими правами ввиду того, что любая сфера жизни индивида тесно связана с информацией в той или иной форме.

Таким образом, правом на информацию следует считать совокупность правомочий граждан, организаций и хозяйствующих субъектов, органов государственной власти и органов местного самоуправления свободно искать, получать, передавать, производить и распространять информацию любым законным способом, разрешать или ограничивать доступ к информации, обладателями которой они являются, а также определять порядок и условия такого доступа.

1.8. Защита информации от неправомерного доступа тесно связана с категорией «тайна», под которой следует понимать информацию, известную ограниченному кругу лиц, доступ к которой возможен лишь с дозволения обладателя такой информации, а несанкционированное нарушение конфиденциальности которой влечет негативные последствия для обладателя.

1.9. К преступлениям против права на информацию и защиты информации от неправомерного доступа следует относить запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие реализацию права свободно искать, получать, передавать, производить и распространять информацию любым законным способом, а также разрешать или ограничивать доступ к информации обладателями такой информации.

1.10. Информационным ресурсом следует считать информацию (сведения), представленную в виде отдельного документа или массива документов (в том числе в электронной форме). Ввиду того, что действующее законодательство не содержит определения понятия информационного ресурса, но им оперирует,

необходимо закрепить его в Федеральном законе «Об информации, информационных технологиях и защите информации».

С этой целью предлагается дополнить ст. 2 указанного закона пунктом 21, в следующей редакции:

«Информационный ресурс – информация (сведения), представленная в виде отдельного документа или массива документов (в том числе в электронной форме)».

1.11. К преступлениям против безопасности информационного ресурса следует относить запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие сохранность, доступность, достоверность информации (сведений) в форме документов на электронных или бумажных носителях.

1.12. К преступлениям против безопасности информационно-телекоммуникационных технологий следует относить запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей.

1.13. Необходимо принятие Федеральных законов «О профессиональной тайне» и «О служебной тайне» и включение в УК РФ соответствующих норм, предусматривающих уголовную ответственность за противоправные действия в отношении этих тайн, в которых целесообразно закрепить следующие определения:

Профессиональная тайна – это охраняемая законом конфиденциальная информация, доверенная или ставшая известной в силу исполнения лицом профессиональных обязанностей, не связанных с государственной гражданской службой или муниципальной службой, несанкционированное нарушение конфиденциальности которой влечет негативные последствия для ее обладателя.

Служебная тайна – охраняемая законом информация, ставшая известной лицу в силу исполнения им служебных обязанностей, связанных с государственной гражданской и муниципальной службой, а также информация о деятельности государственных органов, доступ к которой ограничен федеральным законом, иным нормативным актом или в силу служебной необходимости, несанкционированное нарушение конфиденциальности которой влечет негативные последствия для ее обладателя.

«Статья N. Незаконное разглашение сведений, составляющих профессиональную тайну

1. Незаконные разглашение или использование сведений, составляющих профессиональную тайну, – наказываются (преступление небольшой тяжести).

2. Незаконное разглашение сведений, составляющих профессиональную тайну в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, а равно с использованием информационно-телекоммуникационных технологий, – наказывается (преступление средней тяжести).

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются (тяжкое преступление).

4. Те же деяния, повлекшие тяжкие последствия, – наказываются (тяжкое преступление)».

«Статья N. Незаконное разглашение сведений, составляющих служебную тайну

1. Незаконные разглашение или использование сведений, составляющих служебную тайну, – наказываются (преступление небольшой тяжести).

2. Незаконное разглашение сведений, составляющих служебную тайну в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, а равно с использованием информационно-телекоммуникационных технологий, – наказывается (преступление средней тяжести).

3. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются (тяжкое преступление).

4. Те же деяния, повлекшие тяжкие последствия, – наказываются (тяжкое преступление)».

2. *Предложения по совершенствованию действующего уголовного законодательства с целью усиления уголовно-правовой охраны информационной безопасности.*

2.1. Преступления, предусмотренные ст. 137, 138, 140, 144, 155, 183, 237, 283, 283.1, 284, 310, 311, 320 УК РФ, должны быть включены в единую систему преступлений, посягающих на право на информацию, и перемещены в главу «Преступления против права на информацию».

Для повышения эффективности уголовно-правовой охраны права на информацию сформулированы предложения de lege ferenda.

Ст. 137 УК РФ изложить в следующей редакции:

«Статья 137. Незаконные собирание, использование или распространение сведений, составляющих личную и семейную тайны

1. Незаконное собирание сведений, составляющих личную или семейную тайну другого лица, – наказывается (преступление небольшой тяжести).

2. Незаконные использование или распространение сведений, составляющих личную или семейную тайну другого лица, – наказываются (преступление средней тяжести).

3. Незаконное распространение сведений, составляющих личную или семейную тайну другого лица, в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации, а равно с использованием информационно-телекоммуникационных технологий, – наказывается (преступление средней тяжести).

4. Деяния, предусмотренные частями первой, второй или третей настоящей статьи, совершенные лицом с использованием своего служебного положения либо повлекшие тяжкие последствия, – наказываются (тяжкое преступление).

5. Деяния, предусмотренные частями первой, второй, третей или четвертой настоящей статьи, совершенные в отношении несовершеннолетнего, – наказываются (тяжкое преступление)».

С учетом факта, что действующая редакция ст. 138 УК РФ находится в противоречии с Конституцией РФ в части того, что она гарантирует каждому право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, предлагается следующая редакция:

«Статья 138. Нарушение тайны сообщений

1. Нарушение тайны сообщений, – наказывается (преступление небольшой тяжести).

2. То же деяние, совершенное лицом с использованием своего служебного положения, – наказывается (преступление средней тяжести).

3. Деяния, предусмотренные частями первой и второй настоящей статьи, совершенные равно с использованием информационно-телекоммуникационных технологий, – наказываются (преступление средней тяжести)».

Исходя из того, что разглашение тайны усыновления (удочерения) лицами, обязанными хранить ее как профессиональную или служебную тайну, отличается более высокой степенью общественной опасности, нежели ее разглашение иными лицами, ст. 155 УК РФ предлагается изложить в следующей редакции:

«Статья 155. Разглашение тайны усыновления (удочерения)

1. Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, – наказывается (преступление небольшой тяжести).

2. Разглашение тайны усыновления (удочерения) лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну, – наказывается (преступление средней тяжести)».

Понятие налоговой тайны полностью охватывается понятием служебной тайны, поэтому в случае включения в УК РФ нормы, предусматривающей уголовную ответственность за противоправные действия в отношении

служебной тайны, налоговая тайна не будет нуждаться в самостоятельной уголовно-правовой охране.

Исходя из того, что понятие налоговой тайны полностью охватывается понятием служебной тайны, а понятие банковской тайны охватывается профессиональной тайной, данная категория в самостоятельной уголовно-правовой охране не нуждаются. Поэтому ст. 183 УК РФ предлагается изложить в следующей редакции:

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

1. Незаконное собирание сведений, составляющих коммерческую тайну, – наказывается (преступление небольшой тяжести).

2. Незаконные разглашение или использование сведений, составляющих коммерческую тайну, без согласия их владельца лицом, которому она была доверена или стала известна по службе или работе, – наказываются (преступление средней тяжести).

3. Деяния, предусмотренные частями первой и второй настоящей статьи, совершенные с использованием информационно-телекоммуникационных технологий, – наказываются (преступление средней тяжести).

4. Те же деяния, причинившие крупный ущерб или совершенные из корыстной заинтересованности, – наказываются (тяжкое преступление).

5. Те же деяния, повлекшие тяжкие последствия, – наказываются (тяжкое преступление)».

2.2. С учетом того факта, что действующая редакция ст. 310 УК РФ не определяет, разглашение каких именно данных предварительного расследования является уголовно наказуемым, необходимо закрепить понятие тайны предварительного расследования в ст. 161 УПК РФ в следующей редакции: «Тайной предварительного расследования является конфиденциальная информация, связанная с возбуждением и расследованием уголовного дела, разглашение которой препятствует установлению истины по делу либо может повлечь иные негативные последствия. Не могут составлять

тайну предварительного расследования сведения: о факте совершения преступления; о возбуждении уголовного дела; об окончании предварительного расследования».

2.3. Преступления, предусмотренные ст. 324, 325, 327 УК РФ, должны быть включены в единую систему преступлений, посягающих на безопасность информационных ресурсов, и включены в главу «Преступления против безопасности информационных ресурсов».

Для повышения эффективности уголовно-правовой охраны информационных ресурсов сформулированы предложения de lege ferenda.

С учетом необходимости более подробной дифференциации ответственности за посягательства на официальные документы, штампы, печати и бланки, а также государственные награды предлагается:

Ст. 324 УК РФ изложить в следующей редакции:

«Статья 324. Приобретение или сбыт официальных документов

Незаконные приобретение или сбыт официальных документов, предоставляющих права или освобождающих от обязанностей, – наказываются (преступление небольшой тяжести)».

Ст. 325 УК РФ изложить в следующей редакции:

«Статья 325. Похищение или повреждение документов

1. Похищение официальных документов, – наказывается (преступление небольшой тяжести).

2. Уничтожение, повреждение или сокрытие официальных документов, совершенные из корыстной или иной личной заинтересованности, – наказываются (преступление средней тяжести).

3. Похищение паспорта гражданина или другого официального личного документа, – наказывается (преступление средней тяжести)».

Ст. 327 УК РФ изложить в следующей редакции:

«Статья 327. Подделка, изготовление или сбыт поддельных документов

1. Подделка удостоверения или иного официального документа, предоставляющего права или освобождающего от обязанностей, в целях его использования, – наказывается (преступление небольшой тяжести).

2. То же деяние, совершенное с целью скрыть другое преступление или облегчить его совершение, – наказывается (преступление средней тяжести).

3. Использование заведомо подложного документа, а равно сбыт такого документа, – наказываются (преступление средней тяжести)».

Включить в УК РФ ст. 327.3 следующего содержания:

«Статья 327.3. Незаконные уничтожение, повреждение, приобретение или сбыт официальных документов в электронной форме

1. Уничтожение, повреждение или сокрытие официальных документов в электронной форме, совершенные из корыстной или иной личной заинтересованности, – наказываются (преступление небольшой тяжести).

2. Незаконное приобретение, а равно сбыт официальных документов в электронной форме, – наказываются (преступление средней тяжести).

3. Те же деяния, совершенные с целью скрыть другое преступление или облегчить его совершение, – наказываются (преступление средней тяжести)».

В целях усиления уголовно-правовой охраны информационных ресурсов необходимо сформулировать ч. 3 ст. 292 УК РФ в следующей редакции: «Деяния, предусмотренные частями 1 и 2 настоящей статьи, совершенные в отношении официальных электронных документов».

2.4. Преступления, предусмотренные ст. 272, 273 УК РФ, должны быть включены в единую систему преступлений, посягающих на безопасность информационно-телекоммуникационных технологий, и включены в главу «Преступления против безопасности информационно-телекоммуникационных технологий».

2.5. Авторский подход о необходимости замены понятия «компьютерная информация»», используемого в УК РФ, на «электронная информация», благодаря чему достигается унификация и единообразие терминов и определений на законодательном уровне.

2.6. Ввиду того, что использование средств вычислительной техники существенно упрощает процесс совершения преступления, следует дополнить ст. 137, 138, 144, 146, 147, 158, 160, 163, 176, 183, 185.6, 205, 207, 275, 276 УК РФ квалифицирующим признаком «с использованием информационно-телекоммуникационных технологий».

Теоретическая значимость исследования связана с решением теоретических, законотворческих и правоприменительных задач. В диссертации заложены теоретические основы уголовно-правовой охраны информационной безопасности, предложено решение ряда существующих уголовно-правовых проблем. Положения и выводы, содержащиеся в диссертации, могут быть использованы при дальнейшем научном осмыслении теоретических вопросов уголовно-правовой охраны информационной безопасности, в процессе дальнейшего совершенствования уголовного законодательства и законодательства иных отраслей права, а также в правоприменительной деятельности.

Практическая значимость исследования состоит в том, что положения и выводы, содержащиеся в диссертации, могут быть использованы при дальнейшем изучении информационной безопасности как объекта уголовно-правовой охраны, в процессе совершенствования уголовного законодательства, а также в правоприменительной деятельности. Сформулированные в диссертации выводы и предложения могут быть использованы и образовательном процессе в высших учебных заведениях при преподавании дисциплин уголовно-правового цикла.

Апробация результатов исследования. Основные положения и выводы, содержащиеся в диссертации, нашли отражение в печатных трудах: в 2 монографиях, 48 научных статьях, в том числе в 19 статьях, опубликованных в изданиях, рекомендуемых Высшей аттестационной комиссией при Министерстве образования и науки РФ, и 2 статьях в изданиях, входящих в международные реферативные базы данных и системы цитирования (Scopus).

Результаты проведенного исследования докладывались и обсуждались на 19 международных и всероссийских и многочисленных региональных научных и научно-практических конференциях, круглых столах, семинарах и совещаниях, в том числе: Международном научно-практическом форуме «Процессуальные, криминалистические, уголовно-правовые и криминологические проблемы ответственности за тяжкие и особо тяжкие преступления в России и Германии» (г. Казань, 2013), Международной научно-практической конференции «Кутафинские чтения»: «Конституционализм и правовая система России: итоги и перспективы» (г. Москва, 2013), IX Российском конгрессе уголовного права: «Уголовное право в эпоху финансово-экономических перемен» (г. Москва, 2014), Совместной XV Международно-практической конференции и VII Международной научно-практической конференции «Кутафинские чтения»: «Судебная реформа в России: прошлое, настоящее, будущее» (г. Москва, 2014), XII Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (г. Москва, 2015) и др.

Результаты и положения диссертационного исследования используются в учебном процессе в Казанском филиале ФГБОУ ВО «Российский государственный университет правосудия» на факультете подготовки специалистов для судебной системы (юридическом факультете) при преподавании дисциплин «Уголовное право», «Уголовное право зарубежных стран», «Квалификация преступлений».

Отдельные положения и выводы по диссертации нашли практическое воплощение в деятельности Центра специальной связи и информации Федеральной службы охраны Российской Федерации в Республике Татарстан.

Структура исследования определяется его целями и задачами. Диссертация состоит из введения, пяти глав и четырнадцати параграфов, заключения, библиографического списка и четырех приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальность темы, формулируются цель и задачи исследования, его объект и предмет, характеризуются методологическая, нормативная, теоретическая и эмпирическая основы диссертации, определяются ее научная новизна и положения, выносимые на защиту, доказывается их теоретическая ценность и практическая значимость, содержатся сведения об апробации основных выводов и предложений.

Глава первая диссертации **«Теоретико-методологические основы исследования информационной безопасности»** состоит из четырех параграфов.

В первом параграфе данной главы исследуется понятие информации с позиций научно-технического, философского и социально-гуманитарного подходов. В рамках обозначенных выше подходов сложились и различные интерпретации понятия информационной безопасности. В контексте социально-гуманитарной парадигмы информационную безопасность принято рассматривать как безопасность информационной среды. Вместе с тем практически в каждой из гуманитарных наук имеется свое определение информационной безопасности, адаптированное к сфере его применения. Не исключением является и право, которое имеет собственное определение как понятия информации, так и информационной безопасности. Используя термин «информация» в различных сферах правового регулирования, юридическая наука стремится дать ему всеохватывающее определение. Проблема обеспечения информационной безопасности в юридической науке традиционно связывается с обеспечением безопасности компьютерных сетей и систем, информационно-телекоммуникационных технологий и т.п. Такой подход нередко встречается и в исследованиях уголовно-правового цикла. Применительно к уголовному праву информационная безопасность, прежде всего, есть система общественных отношений, так как в науке уголовного права под объектом преступления традиционно понимаются общественные отношения, охраняемые уголовным законом.

Диссертант полагает, что информационная безопасность являет собой открытую динамичную систему общественных отношений. Открытость этой системы обусловлена тем, что информационная безопасность не может иметь постоянный, неизменный характер. В качестве объекта уголовно-правовой охраны информационная безопасность представляет собой открытую динамичную систему общественных отношений, обеспечивающих реализацию интересов личности, общества и государства в информационной сфере. Структура информационной безопасности как объекта уголовно-правовой охраны не может быть определена линейно. Нелинейная классификация структуры информационной безопасности обусловлена сложностью самой информационной сферы. Ядро информационной сферы составляет информация, а право на доступ к ней и ее охрану от неправомерного доступа является одним из основополагающих прав в условиях становления информационного общества. Материализуясь, информация находит свое воплощение в информационном ресурсе. Одним из средств реализации права на доступ к информации и ее охраны от неправомерного доступа, а также средств обеспечения функционирования объектов информатизации являются информационно-телекоммуникационные технологии. Поэтому структура информационной безопасности включает в себя: 1) общественные отношения, обеспечивающие реализацию права на информацию и на охрану информации от неправомерного доступа; 2) общественные отношения, обеспечивающие безопасность информационных ресурсов; 3) общественные отношения, обеспечивающие безопасность использования информационно-телекоммуникационных технологий.

Информационная безопасность может выступать как основным, так и дополнительным объектом преступления. Информационная безопасность в качестве дополнительного объекта преступления присутствует в значительном количестве составов преступлений, ответственность за которые предусмотрена нормами Особенной части УК РФ. Их следует относить к посягательствам на информационную безопасность с некоторой долей условности.

Во втором параграфе первой главы диссертационного исследования излагаются методологические основы исследования информационной безопасности. Исследование строится на системном подходе как совокупности принципов, формирующих концепцию исследования. Системный подход позволяет представить знания в упорядоченном виде, пригодном для понимания и использования в научной и законодательной деятельности. В настоящем исследовании системный подход находит свое проявление при рассмотрении информационной безопасности как системы общественных отношений, а также в сформулированных на его основе предложениях по систематизации норм уголовного законодательства, направленных на охрану информационной безопасности. Системный подход как отражение и выражение системного характера информационных общественных отношений и самого права занимает важное место при формировании основы информационной сферы. Базисом в исследовании проблемы уголовно-правовой охраны информационной безопасности выступает совокупность философских принципов, относящихся к всеобщему уровню методов научного познания.

В третьем параграфе первой главы диссертации анализируются факторы, обусловливающие необходимость выделения информационной безопасности как объекта уголовно-правовой охраны. К ним относятся: социально-экономический, исторический, политический и социально-правовой. Все перечисленные факторы тесным образом связаны с процессом становления информационного общества в Российской Федерации.

На выявление социальной обусловленности уголовно-правовых норм направлен социологический метод в части обобщения и анализа официальных статистических данных. Так как нормы об ответственности за преступления против информационной безопасности рассредоточены по всей Особенной части УК РФ, то анализ статистических данных о количестве зарегистрированных преступлений по отдельным статьям не будет иметь научной и практической значимости в контексте рассматриваемого вопроса социальной обусловленности переноса их в единый раздел. В диссертации

исследуются данные ГИАЦ МВД России по форме 1-ВТ «Сведения о преступлениях, совершенных в сфере телекоммуникаций и компьютерной информации», включающей в себя сведения о зарегистрированных преступлениях, ответственность за которые предусмотрена ч. 1 ст. 138, ст. 138.1, ст. 272, ст. 273, ст. 274, ст. 146, ст. 158, ст. 159, ст. 165, ст. 171.2, ст. 183, ст. 242, ст. 242.1, ст. 242.2 УК РФ.

Если в 2014 г. было зарегистрировано 10968 таких преступлений, то в 2015 г. – 43816. Такой рост произошел за счет увеличения числа краж (ст. 158 УК РФ), совершаемых с использованием компьютерной информации и телекоммуникаций с 2540 в 2014 г. до 9146 в 2015 г., а также мошенничества (ст. 159 УК РФ) с 2511 в 2014 г. до 14610 в 2015 г. Кроме того возросло количество преступлений, ответственность за которые предусмотрена ст. 171.2 УК РФ «Незаконные организация и проведение азартных игр»: с 49 в 2014 г. до 492 в 2015 г. Исходя из данных 2016 г. снова виден рост анализируемой категории преступлений. Он произошел вновь за счет увеличения мошенничества (ст. 159 УК РФ) с использованием компьютерной информации и телекоммуникаций до 32875, что составило на 18265 преступлений больше, по сравнению с предыдущим периодом. Приведенные данные свидетельствуют о том, что для совершения таких «классических» преступлений как кража и мошенничество, все чаще стали использоваться информационно-телекоммуникационные технологии, в том числе сеть Интернет. Конечно же, нельзя говорить о том, что они полностью переместились в виртуальную среду, однако наметилась определенная тенденция к росту числа хищений посредством телекоммуникаций.

Метод экстраполяции динамических рядов с использованием линейной и полиноминальной моделей тренда позволил автору предложить две модели криминологического прогноза о динамике преступлений, совершенных в сфере телекоммуникаций и компьютерной информации до 2019 г. включительно. При экстраполяции с использованием линейной модели тренда отсутствует резкий рост преступлений в сфере телекоммуникаций и компьютерной информации.

Их динамику в будущем можно назвать равномерной. Прогноз с использованием полиноминальной модели существенно отличается своими результатами и характеризуется ожидаемым ростом количества таких преступлений в 2019 г. Понимая, что любой прогноз носит вероятностный характер, следует отметить, что данные экстраполяции с использованием линейной модели, с одной стороны, могут быть более достоверными, если резкий рост количества зарегистрированных преступлений в сфере телекоммуникаций и компьютерной информации в 2015 г., а затем и в 2016 г. обусловлен субъективными причинами. Поэтому данные прогноза не предполагают такого роста в будущем. С другой стороны, полиноминальная модель дает более четкое описание фактических данных, но данные прогноза показывают резкий рост количества зарегистрированных преступлений в 2019 г.

Преступность как динамическая социальная система является открытой. Поэтому при ее прогнозировании следует устанавливать тесную связь с эволюцией других социальных явлений. Усиление проникновения информационно-телекоммуникационных технологий практически во все сферы жизнедеятельности, в совокупности с обозначенными выше факторами, позволяет предположить в будущем рост количества преступлений, совершаемых в сфере телекоммуникаций и компьютерной информации. Поэтому данные экстраполяции с использованием полиноминальной модели видятся более точными.

В четвертом параграфе первой главы диссертации раскрывается состояние уголовно-правовой охраны информационной безопасности на современном этапе. Современное состояние российского уголовного законодательства позволяет констатировать, что институт ответственности за преступления против информационной безопасности в нем в настоящее время отсутствует. Действительно, при анализе Особенной части УК РФ видно, что нормы, направленные на обеспечение уголовно-правовой охраны информационной безопасности, расположены в различных разделах и главах УК РФ. Необходимо

вести речь об информационной безопасности как объекте уголовно-правовой охраны и об информационной безопасности как о институте уголовного права, который должен быть сформирован путем объединения уголовно-правовых норм одной правовой природы в единое целое. Такое объединение придаст уголовному закону целостность, единство и гармоничность.

Исходя из обоснованной автором позиции о необходимости выделении информационной безопасности в качестве объекта уголовно-правовой охраны, предлагается предусмотреть в Особенной части УК РФ раздел «Преступления против информационной безопасности», состоящий из трех глав: «Преступления против права на информацию»; «Преступления против безопасности информационных ресурсов»; «Преступления против безопасности информационно-телекоммуникационных технологий». Диссертант поддерживает позицию ведущих российских ученых по вопросу о необходимости принятия нового УК РФ и считает, что данное предложение может быть успешно в нем реализовано, а информационная безопасность может стать родовым объектом, образуя самостоятельный институт Особенной части УК РФ.

Одним из дискуссионных в настоящее время остается вопрос о том, какие же преступления могут войти в систему преступлений против информационной безопасности, которые все чаще именуют «информационными преступлениями». Объектом информационных преступлений являются общественные отношения, обеспечивающие информационную безопасность. Таким образом, преступлениями против информационной безопасности следует считать виновно совершенные общественно-опасные деяния, посягающие на общественные отношения, обеспечивающие реализацию интересов личности, общества и государства в информационной сфере. В свою очередь, исходя из структуры информационной безопасности как объекта уголовно-правовой охраны, систему информационных преступлений образуют: преступления против права на информацию и охраны информации от неправомерного доступа; преступления против безопасности информационных

ресурсов; преступления против безопасности информационно-телекоммуникационных технологий. Каждая из предложенных подсистем строится по признаку наличия единого видового объекта. Вместе с тем, всех их объединяет единый родовой объект – информационная безопасность. Так, рассматривая в качестве критерия единый видовой объект посягательства, представляется возможным предложить систему преступлений против информационной безопасности в следующем виде: 1) преступления против права на информацию и охраны информации от неправомерного доступа: ст. 137, 138, 140, 144, 155, 183, 283, 283.1, 284, 310, 311, 320 УК РФ; 2) преступления против безопасности информационных ресурсов: ст. 170.1, 324, 325, 327, 285.3 УК РФ; 3) преступления против безопасности информационно-телекоммуникационных технологий: ст. 272, 273, 274 УК РФ.

Таким образом, институционализация ответственности за преступления против информационной безопасности должна строиться путем объединения соответствующих уголовно-правовых норм, имеющих единый родовой объект – информационную безопасность, в соответствующий раздел УК РФ. В рамках раздела данные нормы группируются в соответствующие главы по признаку видового объекта.

Вторая глава диссертации **«Ответственность за посягательства на информационную безопасность в международных правовых актах и в зарубежном законодательстве»** состоит из двух параграфов.

В первом параграфе исследуются международно-правовые основы обеспечения информационной безопасности.

Конвенция Совета Европы «О киберпреступности» 2000 г. впервые рекомендовала странам-участницам включить в национальное законодательство единую систему норм об уголовной ответственности за преступления в сфере киберпространства[8]. Конвенция преследует три главные

[8] Конвенция Совета Европы о киберпреступности от 23 ноября 2001 г. // Международное уголовное право в документах, в 2 т. – т.1. – Казань: Казанский государственный университет В.И. Ульянова-Ленина, 2005. С. 467-482.

цели: определяет составы киберпреступлений, содержит рекомендации по унификации соответствующих норм, действующих в разных странах, а также раскрывает юридические процедуры и средства совместной борьбы с подобными преступлениями.

Одним из немногих документов, направленных на обеспечение международной информационной безопасности, стало подписанное 16 июня 2009 г. в Екатеринбурге межправительственное Соглашение государств-членов Шанхайской организации сотрудничества «О сотрудничестве в области обеспечения международной информационной безопасности»[9]. В Приложении 1 к соглашению приводится перечень основных понятий в области обеспечения международной информационной безопасности, а в приложении 2 – перечень основных видов угроз в области международной информационной безопасности, их источников и признаков. Подписание этого документа имеет важное значение, так как в нем определены основные направления, принципы, формы и механизмы сотрудничества, проанализированы основные угрозы международной информационной безопасности.

Несмотря на то что мировое сообщество достаточно давно осознало важность обеспечения информационной безопасности, «общего понимания» по ряду ключевых вопросов так и не удается достигнуть. Работа в области обеспечения международной и региональной информационной безопасности ведется выборочно, принимаются акты, затрагивающие лишь отдельные составляющие информационной безопасности. Российская Федерация исходит из того, что в настоящее время назрела необходимость разработки нового универсального документа, который заменил бы Конвенцию Совета Европы о киберпреступности 2001 г. Предполагается, что разработка такой конвенции должна вестись под эгидой ООН. Это позволит, с одной стороны, максимально учесть озабоченность всех стран мира противостоянию новым угрозам, а с другой – придать документу действительно глобальный масштаб, без которого

---

[9] https://ccdcoe.org/sites/default/files/documents/SCO-090616-IISAgreementRussian.pdf (дата обращения 13.04.2014).

борьба с киберпреступностью не может быть достаточно эффективной. Советом безопасности РФ совместно с МИД РФ был разработан проект Конвенции об обеспечении международной информационной безопасности[10]. Проект имеет более широкую сферу применения, в отличие от Конвенции Совета Европы. Разработанный же РФ проект направлен на регулирование деятельности государств по обеспечению международной информационной безопасности и сохраняет преемственность с принятыми ранее документами ООН.

В настоящее время на международном уровне не только отсутствует правовой акт, регулирующий вопросы в сфере уголовно-правовой охраны информационной безопасности, но и не достигнуто как таковое единое понимание информационной безопасности, ее основных угроз, возможных совместных мер по их предупреждению и устранению. Российские инициативы в этом правлении видятся нам весьма удачными. Не возникает сомнений, что такой акт должен быть принят на уровне ООН. В этом акте следует привести классификацию преступлений против информационной безопасности, а также дать рекомендации государствам по криминализации деяний против информационной безопасности в национальном законодательстве. В то же время отсутствие такого акта может быть выгодно ряду развитых зарубежных стран, так как это позволяет использовать информационное пространство в политических целях, особенно в нынешних условиях осложнившейся международной политической обстановки. Становление глобального информационного общества без такого документа затруднительно. Межгосударственное информационное противоборство будет продолжаться и набирать новые обороты. Поэтому такой международный акт сегодня просто необходим.

Во втором параграфе данной главы проводится сравнительно-правовое исследование уголовного законодательства зарубежных стран об ответственности за посягательства на информационную безопасность.

[10]URL: http://www.scrf.gov.ru/documents/6/112.html (дата обращения 13.04.2014).

Уголовное законодательство зарубежных стран характеризуется преимущественно отсутствием системного подхода к уголовно-правовой охране информационной безопасности. Однако в некоторых странах информация, охраняемая законом, выделена в качестве родового или видового объекта. Так, в УК Республики Польша глава XXXIII получила название «Преступления против охраны информации».

В остальных зарубежных странах регламентация ответственности за посягательства на информационную безопасность решается иным образом. И хотя отдельные главы имеют название «Преступления против информационной безопасности», они включают в себя уголовно-правовые нормы, предусматривающие ответственность за преступления, против безопасного использования информационно-телекоммуникационных технологий.

В целом же в зарубежных странах различно решается вопрос об уголовно-правовой охране информационной безопасности. Лишь в уголовном законодательстве Польши можно увидеть системный подход к уголовно-правовой охране информации. Еще ряд зарубежных государств системно охраняют посредством уголовного закона различные виды тайн. В целом же, в большинстве зарубежных стран, как и в России, нормы, устанавливающие ответственность за посягательства на информационную безопасность рассредоточены по всей Особенной части уголовного закона. В то же время в отдельные разделы или главы выделены статьи, предусматривающие в качестве преступлений незаконные деяния в отношении компьютерной информации.

Третья глава диссертации **«Преступления против права на информацию и охраны информации от неправомерного доступа: понятие видового объекта и особенности составов»** включает в себя три параграфа.

В первом параграфе третьей главы исследуется понятие объекта преступлений против права на информацию и защиты информации от неправомерного доступа.

Правом на информацию следует считать совокупность правомочий граждан, организаций и хозяйствующих субъектов, органов государственной

власти и органов местного самоуправления свободно искать, получать, передавать, производить и распространять информацию любым законным способом, разрешать или ограничивать доступ к информации, обладателями которой они являются, а также определять порядок и условия такого доступа. Защита же информации от неправомерного доступа в УК РФ тесным образом связана с такой категорией как «тайна». Непосредственным объектом посягательства на конфиденциальность того или иного вида тайны будут выступать общественные отношения, обеспечивающие реализацию права на информацию и защиту информации от неправомерного доступа. По своей правовой природе тайны, охраняемые уголовным законом, делятся на: личные тайны; тайны, связанные с особым характером деятельности субъекта права на тайну; тайны, связанные с особым статусом субъекта; государственная тайна.

К преступлениям против права на информацию и защиты информации от неправомерного доступа следует относить запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие реализацию права свободно искать, получать, передавать, производить и распространять информацию любым законным способом, а также разрешать или ограничивать доступ к информации обладателями такой информации.

Исходя из высказанного диссертантом предложения о включении в УК РФ раздела «Преступления против информационной безопасности», содержащего, помимо прочих, главу «Преступления против права на информацию», право на информацию будет выступать видовым объектом посягательств. Следовательно, в данную главу должны быть включены составы преступлений, имеющие единый видовой объект – право на информацию.

Во втором параграфе данной главы произведен анализ объективных признаков преступлений против права на информацию и защиты информации от неправомерного доступа. Как уже отмечалось, все преступления против права на информацию и защиты информации от неправомерного доступа имеют единый видовой объект – общественные отношения, обеспечивающие

реализацию права на информацию и защиту информации от неправомерного доступа.

Непосредственным объектом отказа в предоставлении гражданину информации (ст. 140 УК РФ) являются общественные отношения, обеспечивающие реализацию права гражданина на информацию, затрагивающую его права и свободы.

Непосредственным объектом воспрепятствования законной профессиональной деятельности журналистов (ст. 144 УК РФ) являются общественные отношения, обеспечивающие реализацию права на получение достоверной, полной, актуальной информации.

Непосредственным объектом сокрытия информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237 УК РФ), являются общественные отношения, обеспечивающие право гражданина на получение достоверной информации об обстоятельствах, создающих опасность для жизни или здоровья.

Непосредственным объектом нарушения неприкосновенности частной жизни (ст. 137 УК РФ) являются общественные отношения, обеспечивающие реализацию права на защиту тайны частной жизни (личной и семейной тайн) от неправомерного доступа. Личной тайной следует считать охраняемую законом информацию о частной жизни лица, несанкционированное нарушение конфиденциальности которой влечет негативные последствия для ее обладателя. Семейной тайной является охраняемая законом информация о частной жизни семьи, несанкционированное нарушение конфиденциальности которой влечет негативные последствия для ее обладателей.

Непосредственным объектом нарушения тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ) выступают общественные отношения, обеспечивающие реализацию права на защиту тайны переписки от неправомерного доступа. Категории «тайна связи» и «тайна переписки» следует признать синонимами. Тайну связи или тайну переписки следует понимать как охраняемую законом информацию,

передаваемую лицом посредством любого вида корреспонденции, несанкционированное нарушение конфиденциальности которой влечет негативные последствия для ее обладателя.

Непосредственным объектом разглашения тайны усыновления (ст. 155 УК РФ) являются общественные отношения, обеспечивающие защиту тайны усыновления от неправомерного разглашения. Под тайной усыновления следует понимать охраняемую законом информацию о факте усыновления и иных, связанных с этим фактом обстоятельствах, несанкционированное нарушение конфиденциальности которой влечет негативные последствия для ее обладателей.

Среди тайн, связанных с особым характером деятельности субъекта права на тайну, следует выделить профессиональную и служебную тайны. Действующее российское законодательство характеризуется отсутствием комплексного подхода к вопросам правовой охраны профессиональной тайны. Федерального закона «О профессиональной тайне» в Российской Федерации в настоящий момент нет. Однако ее основные черты и особенности усматриваются из ряда других нормативных актов. Вопрос о включении в УК РФ специальных норм, предусматривающих ответственность за посягательства на неприкосновенность профессиональной и служебной тайн, является преждевременным. Это обусловлено тем, что пока отсутствуют Федеральный закон «О профессиональной тайне» и Федеральный закон «О служебной тайне», включение таких составов в УК РФ приведет лишь к несогласованности законодательства, так как эти нормы должны быть бланкетными. Поэтому необходимо комплексно подойти к решению данной проблемы: принять соответствующие Федеральные законы и одновременно внести изменения в УК РФ.

К тайнам, связанным с особым характером деятельности субъекта, относятся и коммерческая, и банковская тайны, ответственность за незаконное получение и разглашение которых предусмотрена в ст. 183 УК РФ.

Непосредственными объектами рассматриваемого состава преступления являются:

− общественные отношения, обеспечивающие реализацию права на защиту коммерческой тайны от неправомерного доступа;

− общественные отношения, обеспечивающие реализацию права на защиту налоговой, банковской тайны от неправомерного доступа;

− общественные отношения, обеспечивающие реализацию права на защиту банковской тайны от неправомерного доступа.

Налоговая тайна полностью охватывается понятием служебной тайны, а банковская – профессиональной, поэтому в самостоятельной уголовно-правовой охране не нуждаются.

Среди тайн, связанных с особым статусом субъекта, значительное место занимает следственная тайна, ответственность за разглашение которой предусмотрена ст. 310 УК РФ. Непосредственным объектом данного преступления выступают общественные отношения, обеспечивающие реализацию права на защиту тайны предварительного расследования от неправомерного разглашения. Действующая редакция ст. 310 УК РФ не определяет, разглашение каких именно данных предварительного расследования является уголовно наказуемым. При этом не решен вопрос и о том, что следует понимать под данными предварительного расследования. Таким образом, можно сделать вывод о том, что перечень сведений, относимых к категории тайны следствия, в настоящее время не определен. Более того, он может варьироваться в зависимости от тех или иных обстоятельств дела.

Следующий вид тайны, связанной с особым статусом субъекта и охраняемой уголовным законом, – тайна безопасности участников уголовного судопроизводства. Тайну безопасности участников уголовного судопроизводства следует рассматривать как охраняемую законом информацию о мерах безопасности, применяемых в отношении участников уголовного процесса, а равно в отношении их близких, несанкционированное нарушение конфиденциальности которой влечет негативные последствия.

От рассмотренной выше тайны безопасности участников правосудия ее отличает лишь субъектный состав тех лиц, к которым применяются соответствующие меры государственной защиты. Тайну безопасности субъектов порядка управления можно определить как охраняемую законом информацию о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа, а равно в отношении их близких, несанкционированное нарушение конфиденциальности которой влечет негативные последствия.

Уголовная ответственность за разглашение тайны безопасности участников уголовного судопроизводства предусмотрена ст. 311 УК РФ, а за разглашение тайны безопасности субъектов порядка управления – ст. 320 УК РФ. Непосредственным объектом разглашения тайны безопасности участников уголовного судопроизводства выступают общественные отношения, обеспечивающие право государства на защиту сведений о мерах безопасности, применяемых в отношении участников уголовного процесса, а равно в отношении их близких от неправомерного разглашения. Непосредственным объектом разглашения тайны безопасности субъектов порядка управления следует считать общественные отношения, обеспечивающие право государства на защиту сведений о мерах безопасности, применяемых в отношении должностных лиц правоохранительных или контролирующих органов, а равно в отношении их близких от неправомерного разглашения.

Целый блок норм УК РФ посвящен защите сведений, составляющих государственную тайну – это ст. 275, 276, 283, 283.1, 284 УК РФ. Особенности объекта преступлений в ст. 283, 283.1 и 284 УК РФ заключаются в том, что таковым являются общественные отношения, обеспечивающие право государства на защиту сведений, составляющих государственную тайну, от неправомерного доступа. Государство, как и любой другой собственник информации, вправе ограничивать доступ к информации для обеспечения ее конфиденциальности. Поэтому преступления, ответственность за которые предусмотрена ст.283, 283.1 и 284 УК РФ, относятся к группе преступлений

против права на информацию и защиту информации от неправомерного доступа.

Диссертант полагает, что преступления, предусмотренные ст. 137, 138, 140, 144, 155, 183, 237, 283, 283.1, 284, 310, 311, 320 УК РФ, имеют общий видовой объект, поэтому должны быть включены в единую систему преступлений, посягающих на право на информацию, и перемещены в главу «Преступления против права на информацию».

В третьем параграфе третьей главы диссертации исследуются субъективные признаки преступлений против права на информацию.

С субъективной стороны большинство преступлений против права на информацию и защиты информации от неправомерного доступа характеризуются виной в форме прямого умысла. Сказанное имеет место в составах преступлений, ответственность за которые предусмотрена ст. 140, 144, 237, 137, 138, 155, 310, 320, 283, 283.1 УК РФ. Что касается субъективной стороны разглашения государственной тайны (ст. 284 УК РФ), то данное преступление может быть совершено и по неосторожности.

Субъект преступлений против права на информацию и защиты информации от неправомерного доступа в большинстве составов преступлений специальный.

Четвертая глава диссертации **«Преступления против безопасности информационного ресурса: понятие видового объекта и особенности составов»** состоит из трех параграфов.

В первом параграфе данной главы исследуется понятие видового объекта преступлений против безопасности информационного ресурса. Общественные отношения, обеспечивающие безопасность информационных ресурсов, являются структурным элементом информационной безопасности как объекта уголовно-правовой охраны. Информационным ресурсом следует считать информацию (сведения), представленную в виде отдельного документа или массива документов (в том числе в электронной форме). К преступлениям против безопасности информационного ресурса следует относить запрещенные

уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие сохранность, доступность, достоверность информации (сведений) в форме документов на электронных или бумажных носителях.

Исходя из высказанного ранее предложения о включении в УК РФ раздела «Преступления против информационной безопасности», содержащего, помимо прочих, главу «Преступления безопасности информационного ресурса», видовым объектом посягательств будут выступать общественные отношения, обеспечивающие сохранность, доступность, достоверность информации (сведений) в форме документов на электронных или бумажных носителях. Следовательно, в данную главу должны быть включены составы преступлений, имеющие единый видовой объект.

Во втором параграфе четвертой главы исследуются объективные признаки преступлений против безопасности информационного ресурса (ст. 170.1, 324, 325, 327 УК РФ).

Объектом фальсификации единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учета (ст. 170.1 УК РФ) выступают общественные отношения, обеспечивающие безопасность государственных информационных ресурсов.

Целый блок статей УК РФ направлен на уголовно-правовую охрану «минимальной единицы» информационного ресурса – документа.

Непосредственным объектом приобретения или сбыта официальных документов и государственных наград (ст. 324 УК РФ) являются общественные отношения, обеспечивающие безопасность информационных ресурсов в форме документов. Предметом посягательства являются официальные документы, предоставляющие права или освобождающие от обязанностей. Так как законодательно перечень документов, предоставляющих права или освобождающих от обязанностей, не определен, то в настоящее время отнесение того или иного документа к этой категории остается на усмотрение суда. Схожий непосредственный объект имеет и подделка, изготовление или

сбыт поддельных документов, государственных наград, штампов, печатей, бланков (ст. 327 УК РФ).

На уголовно-правовую охрану информационного ресурса направлена и ст. 325 УК РФ, которая предусматривает ответственность за похищение или повреждение документов, штампов, печатей либо похищение акцизных марок, специальных марок или знаков соответствия. В отличие от предмета преступления, предусмотренного ст. 324 УК РФ, здесь предметом посягательства может быть любой официальный документ, а не только официальный документ, предоставляющий права или освобождающий от обязанностей.

Таким образом, в рассмотренных выше статьях УК РФ предметом преступления могут выступать:

− официальные документы;

− личные документы физических лиц;

− государственные награды Российской Федерации, РСФСР, СССР;

− штампы, печати, бланки;

− акцизные марки, специальные марки, знаки соответствия.

Штампы, печати и бланки являются реквизитами официальных документов, то есть обязательным элементом документа. Незаконные действия со штампами, печатями, бланками, по нашему мнению, всегда являются промежуточным звеном в цепи преступных действий. Например, они могут быть похищены с целью создания подложного официального документа, либо затем быть уничтожены. Поэтому мы полагаем целесообразным дифференцировать ответственность за посягательства на уже существующие официальные документы и на их реквизиты – штампы, печати и бланки. Посягательство на официальный документ характеризуется большей степенью общественной опасности. В то же время отличаются по степени общественной опасности их похищение, уничтожение, повреждение, сокрытие и подделка. Большей степенью общественной опасности обладает подделка, это прямо вытекает из анализа санкций ст. 325 и ст. 327 УК РФ. Затем следует похищение,

а наименьшая степень общественной опасности из рассматриваемых деяний присуща уничтожению, повреждению и сокрытию. Исходя из изложенного, следует заключить, что в УК РФ необходимо выделить отдельную статью, посвященную уголовно-правовой охране штампов, печатей и бланков. При этом наиболее строгое наказание должна влечь их подделка. Аналогичный подход, на наш взгляд, логически обоснован и в отношении государственных наград, которые являются высшей формой поощрения граждан Российской Федерации. Следовательно, документами государственные награды не являются (лишь ордена и медали вручаются вместе с соответствующим удостоверением), не являются они и реквизитами официальных документов, поэтому не совсем понятно, почему законодатель поставил их в один ряд с документами. Посягательства на них также надлежит выделить в отдельную статью УК РФ. Что касается акцизных марок, специальных марок, знаков соответствия, то в УК РФ по этому поводу имеется некая двойственность. Так, с одной стороны, наряду с официальными документами они выступают предметом преступления, предусмотренного ст. 325 УК РФ, а с другой стороны, в УК РФ имеется ст. 327.1, предусматривающая ответственность за изготовление, сбыт поддельных акцизных марок, специальных марок или знаков соответствия либо их использование. Однако, исходя из того, что похищение акцизных марок, специальных марок или знаков соответствия, защищенных от подделок, предусмотрено в ч. 3 ст. 325 УК РФ, а также наличие в УК РФ ст. 327.1, можно предположить, что законодатель выделяет их среди прочих официальных документов. Следует отметить, что отношения, связанные с оборотом указанных марок, являются финансовыми. Тем самым данное преступление должно быть предусмотрено статьями главы 22 УК РФ.

Несмотря на сложности и противоречия в определении официального документа как предмета преступлений, предусмотренных ст. 324, 325, 327 УК РФ, можно с уверенностью утверждать, что уголовно-правовой охране подлежат документы на бумажном носителе. Нигде в тексте указанных статей не упоминается об электронном документе (Л.А. Букалерова, Р.В. Шагиева).

Нам же представляется, что, с одной стороны, электронный документ может выступать предметом преступлений, предусмотренных ст. 324, 325, 327 УК РФ. Применение указанных норм исключительно к документам на бумажном носителе в УК РФ не оговаривается. С другой же стороны, ввиду всей специфики электронного документа, объективной стороне названных преступлений будет присущ ряд особенностей. Для этого еще раз обратимся к понятию электронного документа, под которым понимается документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах. Так, незаконное приобретение электронного документа в отличие от бумажного документа возможно несколькими способами: физическим и техническим. В первом случае речь идет о завладении носителем электронного документа, а во втором случае о снятии его или перехвате из системы электронного документооборота. Таким же путем возможен и сбыт электронного документа. Что касается его похищения, то не всегда возможно похитить электронный документ в буквальном смысле слова (исключение составляют, пожалуй, универсальные электронные карты гражданина, которые в настоящее время вводятся в РФ). В остальных случаях необходимо вести речь о похищении носителя с таким документом с целью получения доступа к указанному документу. При этом, если лицо преследует цель завладеть самим носителем документа, к примеру, компьютером, то имеет место преступление против собственности. Поэтому полагаем, что термин похищение не следует применять к электронному документу. Характеристика такого признака объективной стороны как уничтожение в данном случае сходна с характеристикой уничтожения как последствия неправомерного доступа к компьютерной информации, то есть удаления официального электронного документа из памяти компьютера или электронного носителя, когда доступ к нему невозможен, независимо от возможности его восстановления. Повреждение

официального электронного документа также возможно двумя способами: физическим и техническим. В первом случае воздействие производится на носитель электронного документа, то есть повреждается сам носитель, и, следовательно, хранящийся на нем электронный документ. Во втором случае арсенал воздействия на электронный документ достаточно широк и включает в себя «заражение» вредоносными программами; изменение формата документа, в результате чего утрачивается возможность его воспроизведения и т.д. Сокрытие официального электронного документа также ректуется неоднозначно. Если под сокрытием в целом следует понимать невозвращение официального документа, его перемещение, то применительно к электронному документу следует вести речь об аналогичных действиях с носителем такого документа. Кроме того, сокрытие возможно и в техническом плане, когда путем различного рода манипуляций файл с документом, база данных и т.п. становятся скрытыми от пользователя, но при этом с самого носителя они не удаляются. В связи с этим полагаем необходимым включение в УК РФ специального состава, предусматривающего ответственность за незаконные действия с электронным документом

В третьем параграфе данной главы исследуются субъективные признаки преступлений против безопасности информационного ресурса.

Субъект преступлений против безопасности информационного ресурса общий, то есть таковым выступает физическое вменяемое лицо, достигшее 16 лет. С субъективной стороны преступления против безопасности информационного ресурса характеризуются виной в форме прямого умысла.

Пятая глава диссертации **«Преступления против безопасности информационно-телекоммуникационных технологий: понятие видового объекта и особенности составов»** включает в себя три параграфа.

В первом параграфе рассматривается понятие объекта преступлений против безопасности информационно-телекоммуникационных технологий. Среди норм действующего УК РФ на уголовно-правовую охрану

информационно-телекоммуникационных технологий направлена, прежде всего, глава 28 УК РФ «Преступления в сфере компьютерной информации».

Родовым объектом преступлений в сфере компьютерной информации принято считать общественные отношения, регулирующие общественную безопасность, так как законодатель поместил данную главу в раздел IX «Преступления против общественной безопасности и общественного порядка»[11]

Вводя в УК РФ в 1996 г. главу 28, законодатель не смог определить точного места этой группы норм в системе Особенной части УК РФ. Именно поэтому глава о преступлениях в сфере компьютерной информации была помещена в соответствующий раздел. Сейчас же представляется необходимым конкретизировать родовой объект данной группы преступлений как общественных отношений, обеспечивающих информационную безопасность.

Относительно видового объекта преступлений в сфере компьютерной информации в современных исследованиях все чаще отмечается, что таковым выступает информационная безопасность.

Диссертант полагает, что информационная безопасность является родовым объектом преступлений в сфере компьютерной информации, а видовым объектом являются общественные отношения, обеспечивающие безопасное использование информационно-телекоммуникационных технологий. Кроме того, информационная безопасность не является частью общественной безопасности, а образует самостоятельный вид безопасности. Поэтому объектом преступлений против безопасности информационно-телекоммуникационных технологий выступает совокупность общественных отношений, обеспечивающих безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей. Следовательно, к

---

[11] См.: Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование): дис. канд. ... юрид. наук. – Волгоград, 2001. С. 32.; Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: дис. канд. ... юрид. наук. – Москва, 2002. С. 54.; Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореф. дис. … канд. юрид. наук. – М., 1998. С. 12.

преступлениям против безопасности информационно-телекоммуникационных технологий следует относить запрещенные уголовным законом общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей.

Термины «компьютерные преступления» и «преступления в сфере компьютерной информации», последний из которых использует отечественный законодатель, при этом включая в него все новые составы с такой формулировкой, остались далеко позади от стремительно развивающихся технологий. Технический прогресс существенно обгоняет теоретическое осмысление происходящего в области создания и применения информационных технологий, использования новых информационно-телекоммуникационных возможностей. В связи с этим многие противоправные посягательства просто выпадают за пределы действия УК РФ. Для обозначения рассматриваемой группы преступлений на законодательном уровне следует использовать термин «преступления против безопасности информационно-телекоммуникационных технологий». Компьютерная информация и устройства, на которых она зафиксирована или на которых она обращается, могут выступать средствами совершения преступления. Из чего следует, что преступления, где компьютерная информация выступает средством совершения преступления, образуют группу так называемых «смежных» преступлений и расположены в различных разделах и главах Особенной части УК РФ.

Если еще несколько лет назад, предложение дополнить ряд статей УК РФ квалифицирующим признаком «с использованием компьютерной техники» или «применением информационных технологий» было недостаточно обоснованным и своевременным, то сейчас оно обусловлено объективными причинами, однако требует некоторых уточнений.

Диссертант полагает, что такой квалифицирующий признак необходим. Так как электронная информация обращается не только в компьютерах, но и

других устройствах, а также в сети Интернет и локальных сетях, необходимо использование более широкого квалифицирующего признака – «с использованием информационно-телекоммуникационных технологий».

Анализ судебной практики показывает, что наряду с преступлениями в сфере компьютерной информации в «чистом виде» столь же часто совершаются преступления, где компьютерная техника выступает средством совершения преступлений. При этом следует обратить внимание на отсутствие в ней единообразия: позиции судов по одним и тем же вопросам порой являются кардинально противоположными. В частности, довольно распространены случаи, когда сходные деяния квалифицируются по-разному: одни суды квалифицируют их только по ст. 272 УК РФ, другие – по совокупности с соответствующей статьей Особенной части УК. РФ Поэтому она, равно как и официальная статистика МВД, едва ли отражает ситуацию в полной мере. Думается, что данная позиция неверна и решить этот вопрос возможно лишь путем дальнейшего совершенствования законодательства и принятия постановления Пленума Верховного Суда РФ. Причем постановление Пленума необходимо принять уже в ближайшее время, так как сложившаяся ситуация по сути противоречит принципам уголовного права.

В то же время ч. 1 ст. 171.2 УК РФ содержит такой квалифицирующий признак, как «с использованием информационно-телекоммуникационных сетей, в том числе сети Интернет», аналогичный квалифицирующий признак встречается также в ч. 3 ст. 242, ч. 2 ст. 242.1, ч. 2 ст. 242.2 УК РФ. Кроме того, ч. 1 ст. 185.3 УК РФ устанавливает ответственность за манипулирование рынком, в том числе через «электронные, информационно-телекоммуникационные сети (включая сеть Интернет)», аналогичный квалифицирующий признак содержится и в ч. 2 ст. 228.1 УК РФ. Столь незначительные, казалось бы, на первый взгляд, различия способны вызвать серьезные затруднения на практике. И хотя его формулировка видится нам не совсем удачной, остается не ясным вопрос, почему законодатель включил этот признак именно в указанные статьи, оставив без должного внимания другие.

Предложенный же нами квалифицирующий признак «с использованием информационно-телекоммуникационных технологий» охватил бы и «использование информационно-телекоммуникационных сетей, в том числе сети Интернет», а также через «электронные, информационно-телекоммуникационные сети (включая сеть Интернет)», так как является более широким. Автор не исключает, что возможно, в отечественном уголовном законодательстве и появятся составы преступлений с приставкой «кибер», однако сейчас об этом говорить преждевременно. Полагаем, что в настоящее время необходимо лишь дополнить ст.137, 138, 144, 146, 147, 158, 160, 163, 176, 183, 185.6, 205, 207, 275, 276 УК РФ квалифицирующим признаком «с использованием информационно-телекоммуникационных технологий».

Во втором параграфе пятой главы диссертации проводится юридический анализ объективных признаков преступлений против безопасности информационно-телекоммуникационных технологий.

К числу преступлений против безопасности информационно-телекоммуникационных технологий относится ст. 272 УК РФ «Неправомерный доступ к компьютерной информации». Непосредственным объектом данного преступления выступают общественные отношения, обеспечивающие безопасность процессов хранения, обработки, предоставления информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей. Законодатель определил предмет преступления, предусмотренного ст. 272 УК РФ, в примечании к этой же статье как «сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи». Диссертант считает, что следует отказаться от использования термина «компьютерная информация», заменив его на «электронная информация», под которой необходимо понимать сведения, сообщения данные, способные обращаться в средствах вычислительной техники.

Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) все чаще стало приобретать транснациональный и

организованный характер. Кроме этого вредоносные программные продукты внедряются преступниками в компьютеры своих жертв с целью получения самой различной информации: данных о банковских счетах и картах; сведениях, составляющих тайну частной жизни; секреты производства и т.п. Непосредственным объектом данного преступления выступают общественные отношения, обеспечивающие безопасность процессов и методов поиска, сбора, хранения, обработки, предоставления, распространения информации посредством средств вычислительной техники и информационно-телекоммуникационных сетей.

Одним из спорных в настоящее время остается вопрос о том, что же следует понимать под созданием такой программы. С одной стороны, создание вредоносной программы можно рассматривать как процесс, состоящий из нескольких этапов. С другой стороны, создание вредоносной программы есть результат целенаправленной человеческой деятельности, выразившейся в разработке специального набора данных и команд, которые заведомо предназначены для несанкционированных манипуляций с компьютерной информацией. И именно создание вредоносной программы как результат будет иметь юридическое значение. Таким образом, моментом создания вредоносной программы следует считать возможность запуска, выполнения программы, способной копировать, блокировать модифицировать, удалять информацию на компьютере.

Нельзя считать созданием программы запись ее текста на бумаге. Сам по себе текст не несет никакой, даже потенциальной опасности, пока не будет воспроизведен на компьютере или ином средстве вычислительной техники. Следует отметить тот факт, что вредоносные программы не всегда создаются с целью причинить вред в будущем. Сам факт ее создания никаких негативных последствий не влечет. Поэтому о создании вредоносной программы как уголовно-наказуемом деянии можно вести речь лишь тогда, когда, создавая такую программу, лицо намеревается ее использовать в противоправных целях, то есть чтобы несанкционированно уничтожить, блокировать, модифицировать,

копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Ст. 273 УК РФ из всех статей главы 28 УК РФ является самой «работающей», однако все же нуждается в некоторых корректировках. В первую очередь, это касается устранения неточностей в формулировках, изложенных в ч. 1 ст. 273 УК РФ – необходимо вести речь не о компьютерных программах, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, а о компьютерной программе, созданной с указанными свойствами. Кроме этого, представляется, что распространение и использование компьютерных программ и иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации характеризуются большей степенью общественной опасности, нежели их создание, поэтому уголовную ответственность за эти деяния необходимо дифференцировать.

Ст. 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Непосредственным объектом преступления выступают общественные отношения, обеспечивающие безопасность в сфере эксплуатации средств вычислительной техники и информационно-телекоммуникационных сетей.

С момента своего принятия данная статья обречена на неприменение. Она переняла все «больные места» предыдущей редакции, хотя, казалось бы, должна была их устранить. Пока отсутствуют специальные единые правила эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, закрепленные законодательно на федеральном уровне, следует обращаться к положениям ГОСТ, СанПиН, локальных актов учреждений и организаций. Однако их

нарушение должно влечь никак не уголовную, а дисциплинарную ответственность, учитывая, что наиболее строгое наказание, которое предусмотрено ч. 1. ст. 274 УК РФ, является лишение свободы на срок до двух лет (а по ч. 2 ст. 274 УК РФ – до пяти лет), что явно не соответствует общественной опасности данного деяния. Резюмируя вышеизложенное, следует признать ст. 274 УК РФ примером излишней криминализации и исключить ее из УК РФ.

В третьем параграфе данной главы рассматриваются субъективные признаки преступлений против безопасности информационно-телекоммуникационных технологий.

С субъективной стороны преступления против безопасности информационно-телекоммуникационных технологий чаще всего характеризуются умышленной формой вины.

Преступление, предусмотренное ч. 1 ст. 274 УК РФ, с субъективной стороны может характеризоваться виной как в форме умысла (чаще – косвенного), так и в форме неосторожности.

Субъект преступлений против безопасности информационно-телекоммуникационных технологий может быть как общим, так и специальным. Например, субъектом преступления, предусмотренного ч. 1 ст. 272 УК РФ, может быть лицо, достигшее 16 лет. Таким образом, не требуется, чтобы лицо занимало определенную должность, занималось определенной деятельностью, получило определенное образование. Лицо может не иметь специальных технических знаний.

В ч. 3 ст. 272 и ч. 2 ст. 273 УК РФ законодателем установлены признаки специального субъекта, то есть лица, совершавшего указанные преступления с использованием своего служебного положения. Под использованием служебного положения понимается использование возможности доступа к компьютеру, возникшего в связи с выполнением профессиональных обязанностей. В данном случае лицо имеет доступ к компьютеру на законных основаниях. Использование служебного положения для совершения данных

преступлений предполагает использование лицом тех полномочий, которыми он наделен по закону. Ошибочным является мнение о том, что лицо, использующее свое служебное положение – это должностное лицо, государственный или муниципальный служащий либо лицо, выполняющее управленческие функции в коммерческой или иной организации.

Субъект преступления, предусмотренного ст. 274 УК РФ, только специальный. Это лицо, которое в силу должностных обязанностей имеет доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационным сетям и оконечному оборудованию. Однако, на наш взгляд, основным условием привлечения лица к ответственности должна быть не возможность доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию в силу должностных обязанностей, а обязанность соблюдать установленные правила обращения со средствами хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационными сетями и оконечным оборудованием. Если же на лицо должностными или иными инструкциями, специальными актами такая обязанность не возложена, то оно не должно подлежать уголовной ответственности.

В **заключении** изложены основные результаты диссертационного исследования.

В **приложениях** представлены результаты анкетирования сотрудников правоохранительных органов, проект раздела «Преступления против информационной безопасности», статистические данные о количестве зарегистрированных преступлений против информационной безопасности в 2010-2016 гг., программа изучения уголовных дел.

Основные положения диссертации отражены в следующих работах автора:

Статьи, опубликованные в ведущих рецензируемых журналах и изданиях, указанных в перечне Высшей аттестационной комиссии при Министерстве образования и науки Российской Федерации

1. Зубова, М.А. Уголовно-правовые аспекты понятия «информация» / М.А. Зубова // Вестник Чувашского университета. –2011. –№ 2. – С. 190-194. – 0,51 п.л.

2. Зубова, М.А. Ответственность за спам по зарубежному и российскому праву / М.А. Зубова // Вестник Чувашского университета. – 2011. № 2. – С. 194-200. – 0,34 п.л.

3. Ефремова, М.А. К вопросу о понятии компьютерной информации / М.А. Ефремова // Российская юстиция. – 2012. – № 7. – С. 50-52. – 0,32 п.л.

4. Ефремова, М.А. Мошенничество с использованием электронной информации / М.А. Ефремова // Информационное право. – № 4. – 2013. – С. 19-21. – 0,39 п.л.

5. Ефремова, М.А. К вопросу об уголовно-правовом обеспечении информационной безопасности / М.А. Ефремова // Вестник Тверского государственного университета. Серия «Право». – № 35. – 2013. – С. 86-91. – 0,36 п.л.

6. Ефремова, М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения / М.А. Ефремова // Информационное право. – № 5. – 2013. – С. 10-13. – 0,43 п.л.

7. Ефремова, М.А. Информационная безопасность как объект уголовно-правовой охраны / М.А. Ефремова // Информационное право. – №5. – 2014. – С. 21-25. – 0,56 п.л.

8. Ефремова, М.А. Уголовно-правовая охрана сведений, составляющих тайну частной жизни / М.А. Ефремова // Вестник Орловского государственного университета. Серия: Новые гуманитарные исследования. – 2014. – № 6 (41). – С. 27-31. – 0,73 п.л.

9. Ефремова, М.А. Уголовно-правовая охрана сведений, составляющих коммерческую, банковскую и налоговую тайны / М.А. Ефремова // Вестник Пермского университета. Юридические науки. – 2015. – Вып. 1 (27). – С. 124-133. – 0,75 п.л.

10. Ефремова, М.А. Международно-правовые основы обеспечения информационной безопасности участников Содружества независимых государств / П.В. Агапов, М.А. Ефремова // Юридическая наука и правоохранительная практика. – 2015. – № 1 (31). – С. 176-182. (авторство не разд.). – 0,63 п.л.

11. Ефремова, М.А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ / М.А. Ефремова // Информационное право. – 2015. – № 3. – С. 12-16. – 0,63 п.л.

12. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности: современное состояние и перспективы / М.А. Ефремова // Право и безопасность. – 2015. – № 1. – С. 59-63. – 0,45 п.л.

13. Ефремова, М.А. Электронный документ как предмет преступления / М.А. Ефремова // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2015. – № 5. – С. 10-15. – 0,58 п.л.

14. Ефремова, М.А. К вопросу об уголовной ответственности за разглашение данных предварительного расследования / М.А. Ефремова // Вестник Казанского юридического института МВД России. – 2015. – № 4 (22). – С. 34-38. – 0,46 п.л.

15. Ефремова, М.А. Информационная безопасность: проблемы уголовно-правовой охраны / М.А. Ефремова // Библиотека криминалиста. Научный журнал. – 2016. – № 1 (24). – С. 25-30. – 0,47 п.л.

16. Ефремова, М.А. Статья 274 Уголовного кодекса Российской федерации: новая редакция – старые проблемы / М.А. Ефремова // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. – 2016. – № 1. – С.106-108. – 0,43 п.л.

17. Ефремова, М.А. Социальная обусловленность уголовно-правовой охраны информационной безопасности Российской Федерации / М.А. Ефремова // Вестник Пермского университета. Юридические науки. – 2017. – Вып. 36. – С. 222-230. – 0,89 п.л.

18. Ефремова, М.А. Криминологическая обусловленность уголовно-правовой охраны в сфере информационной безопасности / М.А. Ефремова // Информационное право. – 2017. – № 2 (52). – С. 17-22. – 0,65 п.л.

19. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности в условиях становления информационного общества в Российской Федерации / М.А. Ефремова // Библиотека уголовного права и криминологии. – 2017. – № 5 (23). – С. 98-105. – 0,73 п.л.

Статьи в изданиях, входящих в международные реферативные базы данных и системы цитирования

20. Efremova, M.A. Crimes against Information Security: International Legal Aspects of Fighting and Experience of Some States / M.A Efremova, P.V. Agapov // Journal of Internet Banking and Commerce. – April 2016. – vol. 21. – no. S3. (авторство не разд.). – 0,73 п.л.

21. Efremova, M.A. State of the contemporary criminal law policy of Russia / M.A Efremova, E.V. Rogova, S.A. Karnovich, O.V. Ivushkina, E.A. Laikova // Journal of Advanced Research in Law and Economics. – Vol. VII. – Issue 1 (15). – Spring 2016. (авторство не разд.). – 0,61 п.л.

Монографии, научно-практические и учебные пособия

22. Ефремова, М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. – М.: Юрлитинформ, 2015. – 12,4 п.л.

23. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности. – М.: Юрлитинформ, 2018. – 19,5 п.л.

24. Ефремова, М.А. Преступления в сфере компьютерной информации: учебное пособие. – Ульяновск: УлГУ, 2014. – 2,4 п.л.

25. Ефремова, М.А. Уголовно-правовая охрана информации с ограниченным доступом: учебное пособие. – Ульяновск: Областная типография «Печатный двор», 2014. – 4 п.л.

26. Ефремова, М.А. Нарушение правил эксплуатации средств хранения обработки или передачи компьютерной информации и телекоммуникационных сетей (ст. 274 УК РФ) // Энциклопедия уголовного права. Т. 25. Преступления в сфере компьютерной информации. / М.А. Ефремова, А.Н. Ягудин. – Спб.: Издание профессора Малинина – МИЭП при МПА ЕврАзЭС, 2017. (авторство не разд.). – 6.п.л.

Научные статьи и иные научные работы

27. Зубова, М.А. Объективные и субъективные признаки нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети / М.А. Зубова // Вестник Ульяновского государственного педагогического университета. – 2010. – Вып. 6. – С. 170-174. – 0,3 п.л.

28. Зубова, М.А. Понятие компьютерной информации по уголовному праву России / М.А. Зубова // «Модернизация современного общества: пути созидания и развития (экономические, социальные, философские, правовые тенденции)»: Материалы международной научно-практической конференции (23 марта 2011 г.): в 4-х ч. Ч. 2. / отв. ред. В.И Долгий. – Саратов, 2011. – С. 70-74. – 0,15 п.л.

29. Ефремова, М.А. Ответственность за неправомерный доступ к компьютерной информации по действующему уголовному законодательству / М.А. Ефремова // Вестник Казанского юридического института МВД России. – 2012. – № 2 (8). – С. 54-56 – 0,41 п.л.

30. Ефремова, М.А. Объект преступлений в сфере компьютерной информации / М.А. Ефремова // Всероссийская научно-практическая конференция «Государственно-правовая политика в сфере обеспечения национальной безопасности», 6 декабря 2012 г.: материалы. – Волгоград, 2012. – С. 289-293. – 0,17 п.л.

31. Ефремова, М.А. Некоторые аспекты уголовной ответственности за создание, использование и распространение вредоносных компьютерных программ/ М.А. Ефремова // Материалы IX Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики». Актуальные проблемы юридической науки. Ч. II. – Тольятти: Волжский университет им. В.Н. Татищева, 2012. – С. 162-167. – 0,21 п.л.

32. Ефремова, М.А. Преступления в сфере компьютерной информации: некоторые вопросы теории и практики / М.А. Ефремова // Социально-правовые проблемы борьбы с преступностью в современной России: материалы итоговой научно-практической конференции Казанского юридического института МВД России. – Казань, 2012. – С. 47-49. – 0,15 п.л.

33. Ефремова, М.А. Информация с ограниченным доступом как объект уголовно-правовой охраны / М.А. Ефремова // Вестник Казанского юридического института МВД России. – 2012. – № 4 (10). – С. 89-92. – 0,29 п.л.

34. Ефремова, М.А. Кибертерроризм как одна из угроз безопасности страны / М.А. Ефремова // «Процессуальные, криминалистические, уголовно-правовые и криминологические проблемы ответственности за тяжкие о особо тяжкие преступления в России и Германии»: материалы Международного научно-практического форума в рамках Года Германии в России 2012/13, 4-5 апреля 2013 г. / отв. ред. А.Г. Никитин, Э.Ю. Латыпова. – Казань, 2013. – С. 132-136. – 0,15 п.л.

35. Ефремова, М.А. Об охране информационной безопасности посредством уголовного закона / М.А. Ефремова // «Проблемы российского законодательства: история и современность»: материалы X Международной научно-практической конференции, Тольятти, 21-22 февраля 2013 г. – Самара, 2013. – С. 94-98. – 0,25 п.л.

36. Ефремова, М.А. К вопросу об уголовно-правовой охране государственной тайны в Российской Федерации / М.А. Ефремова // Актуальные проблемы информационного обеспечения ОВД: вопросы теории и практики: материалы итоговой научно-практической конференции. Первые

юридические чтения: материалы научно-практической конференции Казанского юридического института МВД России 7 июня 2013 г. – Казань, 2013. – С. 105-107. – 0,13 п.л.

37. Ефремова, М.А. Уголовно-правовая охрана общественных отношений, обеспечивающих безопасность в сфере электронного документооборота / М.А. Ефремова, К.В. Кузнецов // Вестник Казанского юридического института МВД России. – 2013. – № 2 (12). – С. 123-129. (авторство не разд.) – 0,25 п.л.

38. Ефремова, М.А. К вопросу о квалификации преступлений, совершенных с использованием информационно-телекоммуникационных технологий / М.А. Ефремова // Уголовное законодательство: вчера, сегодня, завтра: материалы межвузовской научно-практической конференции. – Спб., 2013. – С. 85-90. – 0,25 п.л.

39. Ефремова, М.А. К вопросу об уголовно-правовом обеспечении права на неприкосновенность частной жизни / М.А. Ефремова // Конституционализм и правовая система России: итоги и перспективы. Материалы секции уголовно права и криминологии V Международной научно-практической конференции «Кутафинские чтения»: сборник докладов. – М.: Проспект, 2014. – С. 20-24. – 0,25 п.л.

40. Ефремова, М.А. Информационная безопасность как объект уголовно-правовой охраны: современное состояние и перспективы / М.А. Ефремова // Материалы XI Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики. Актуальные проблемы юридической науки. Ч. II. – Тольятти, 2014. – С. 72-77. – 0,25 п.л.

41. Ефремова, М.А. Уголовное законодательство в информационном обществе / М.А. Ефремова // Уголовное право в эпоху финансово-экономических перемен: материалы IX Российского Конгресса уголовного права, состоявшегося 29-30 мая 2014 г. / отв. ред. В.С Комиссаров. – М.: Юрлитинформ, 2014. – С. 25-28. – 0,13 п.л.

42. Ефремова, М.А. Уголовно-правовая политика в сфере обеспечения информационной безопасности / М.А. Ефремова // Научные воззрения

профессоров Пионтковских (отца и сына) и современная уголовно-правовая политика / под ред. Ф.Р. Сундурова, М.В. Талан. – М.: Статут, 2014. – С. 244-248. – 0,24 п.л.

43. Ефремова, М.А. Информационная безопасность как объект уголовно-правовой охраны / М.А. Ефремова // Материалы секции уголовного права и криминологии VI Международной научно-практической конференции «Кутафинские чтения» – «Гармонизация российской правовой системы в условиях международной интеграции» / отв. ред. А.И Рарог, И.М. Мацкевич. – М.: Проспект, 2014. – С. 48-52. – 0,25 п.л.

44. Ефремова, М.А. Пути совершенствования российского уголовного законодательства в сфере противодействия компьютерным преступлениям / М.А. Ефремова // «Уголовное право: стратегия развития в XXI веке»: материалы XII Международной научно-практической конференции (29-30 января 2015 г.). – М.: РГ-Пресс, 2015. – С.405-408. – 0,23 п.л.

45. Ефремова, М.А. Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений / М.А. Ефремова // Вестник Казанского юридического института МВД России. – 2015. – № 1 (19). – С. 55-58. – 0,27 п.л.

46. Ефремова, М.А. Некоторые проблемы квалификации мошенничества с использованием платежных карт / М.А. Ефремова // Материалы VII Международной научно-практической конференции «Судебная реформа в России: прошлое, настоящее, будущее» (Кутафинские чтения). – В 2 кн. – Кн. 2. – М., 2015. – С. 216-219. – 0,15 п.л.

47. Ефремова, М.А. Computer fraud / М.А. Ефремова // European science review. – 2015. – № 1–2. January-February. – С. 126-128. – 0,35 п.л.

48. Ефремова, М.А. Уголовная ответственность за подделку, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков / М.А. Ефремова // Вестник Казанского юридического института МВД России. – 2015. – № 2 (20). – С. 35-39. – 0,27 п.л.

49. Ефремова, М.А. К вопросу об уголовно-правовой охране служебной тайны в Российской Федерации / М.А. Ефремова // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы всероссийского круглого стола 20 марта 2015 г. – Иркутск, 2015. – С. 125-130. – 0,17 п.л.

50. Ефремова, М.А. Уголовно-правовая охрана информационной безопасности Российской Федерации в условиях глобализации / М.А. Ефремова // Уголовно-правовая охрана информационного пространства в условиях глобализации: Коллективная монография по материалам XII Международной научно-практической конференции, посвященной памяти М.И. Ковалева / отв. ред. И.Я. Козаченко. – Екатеринбург: Издательский дом Уральского государственного юридического университета, 2016. – С. 56-60. – 0,27 п.л.

51. Ефремова, М.А. Социально-криминологическая обусловленность уголовно-правовой охраны информационной безопасности / М.А. Ефремова // Уголовное законодательство: вчера, сегодня, завтра (памяти профессора С.Ф. Кравцова: материалы ежегодной всероссийской научно-практической конференции: в 2 ч. Ч. 1. – Спб., 2016. – С. 274-278. – 0,15 п.л.

52. Ефремова, М.А. Social conditionality of information security protection by criminal law in the Russian Federation / М.А. Ефремова // European Journal of Law and Political Sciences. – 2016. – № 4. – С. 53-59. – 0,35 п.л.

53. Ефремова, М.А. К вопросу о понятии интернет-преступности / М.А Ефремова // Стратегия национального развития и задачи юридической науки: сборник докладов Международной научно-практической конференции 24 ноября-3 декабря 2016 г. – М.: Проспект, 2016. – С. 112-116. – 0,13 п.л.

Общий объем опубликованных работ составил 62,12 п.л.