На правах рукописи

Мнацаканян Аревик Васильевна

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИЙСКОЙ ФЕДЕРАЦИИ: УГОЛОВНО - ПРАВОВЫЕ АСПЕКТЫ

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

Автореферат диссертации на соискание учёной степени кандидата юридических наук

Москва – 2016

Диссертация выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университете имени М.В. Ломоносова», юридический факультет

Научный руководитель: доктор юридических наук, доцент **Серебренникова Анна Валерьевна.**

Официальные оппоненты: **Букалерова Людмила Александровна,** доктор юридических наук, профессор, Федеральное государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов», кафедра уголовного права, уголовного процесса и криминалистики, заведующий кафедрой.

Юрченко Ирина Александровна, кандидат юридических наук, доцент, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Московский государственный юридический университет им. О.Е. Кутафина», кафедра уголовного права, старший преподаватель.

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Сибирский федеральный университет».

Защита состоится 22 марта 2016 г. в 15 часов 00 минут на заседании диссертационного совета Д 501.001.73 на базе федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» по адресу: 119991, Москва, ГСП-1, Ленинские горы, д.1, строение13-14, 4-й учебный корпус, юридический факультет, ауд.535а.

С диссертацией можно ознакомиться в отделе диссертаций научной библиотеки федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» по адресу: Москва, 119992, Ломоносовский проспект, 27, Фундаментальная библиотека, сектор А, 8 этаж, комната 812 и на сайте www.istina.msu.ru

Автореферат разослан «__» _____ 2016 г.

Учёный секретарь
диссертационного совета **Анна Аветиковна Арутюнян**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования. Развитие системы уголовного права подтверждает, что в различные исторические периоды объектом правовой защиты становились лишь те общественные отношения, которые на данном историческом этапе являются значимыми для государства, общества и человека.

В настоящее время такими отношениями являются отношения по поводу создания, распространения и использования информации, которые развиваются в соответствии с развитием информационного общества – характерной чертой цивилизации XXI века.

Возникает понимание и огромной ценности информации, следствием чего становится появление объективной потребности в её защите. Данная проблема, а именно, проблема защиты информации и информационных систем сейчас является одной из самых актуальных в России и в мире. Новые возможности, которые предоставляют информационные технологии, их широкая распространённость и доступность делают эту область чрезвычайно привлекательной для представителей криминалитета, а динамичное развитие телекоммуникационных сетей, создание многочисленных информационных ресурсов и баз данных, разработка более совершенных устройств создают условия, облегчающие совершение преступлений в этой сфере, число которых в России увеличивается.

Об актуальности проблемы обеспечения информационной безопасности говорят объективные данные статистики, которая свидетельствует, что каждую секунду в мире жертвами преступников, специализирующихся на совершении противоправных деяний в сфере

информационной безопасности становятся 12 человек, и эта цифра с каждым годом растёт[1].

Что касается Российской Федерации, то в нашей стране также наблюдается тенденция к росту данного вида преступности. Статистика свидетельствует, что если в 2000 году в стране было зарегистрировано 800 преступлений, предусмотренных ст.ст. 272-274 УК РФ, то в 2013 году данный показатель составил уже 2564 преступлений, а в 2014 году этот показатель снизился – было зарегистрировано 1739 преступлений в сфере компьютерной информации. При этом по данным МВД, в России в 2013 году было зарегистрировано 11 тыс. преступлений в сфере телекоммуникаций и компьютерной информации, аналогичный показатель (11 тыс. преступлений) был зафиксирован и в прошлом 2014 году, при том, что в 2000 году аналогичный показатель составлял 1170 преступлений[2].

Следует указать на тот факт, что Президент Российской Федерации В.В. Путин, выступая на заседании коллегии ФСБ 26 марта 2015 года, заявил, что в 2014 году в ходе спецопераций ФСБ РФ пресекла деятельность 52 кадровых сотрудников и 209 агентов иностранных спецслужб. Президент считает, что сегодня особенно важно совершенствовать систему защиты сведений, представляющих государственную тайну, не допускать утечки информации о развитии военных организаций, мобилизационных планов промышленных и оборонных технологий.

По словам В.В. Путина, под особым контролем должны оставаться вопросы защиты национальных информационных ресурсов, поскольку количество кибератак на официальные сайты и информационные системы органов власти России не уменьшается. Только в прошлом году пресечено около 74 миллионов попыток помешать безопасному информационному обмену при том, что правоохранительные органы выявили свыше 25 тысяч

[1] Число компьютерных преступлений в РФ в 2013 году увеличилось на 8,6% [Электронный ресурс]. – Режим доступа: https://news.mail.ru/incident/16727249/

[2] Отчёт ФГКУ «Главный аналитический центр» МВД России о состоянии преступности в России за январь-декабрь 2014 года [Электронный ресурс]. – Режим доступа: http://mvd.ru/upload/site1/document_file/H8NGnfdiEy.pdf

интернет-ресурсов с публикациями, нарушающими закон, и прекратили работу более 1,5 тысяч экстремистских сайтов[3].

В то же время следует иметь в виду, что, как считают специалисты, статистика преступности в сфере компьютерной информации отражает факты не вполне корректного применения правоприменительными органами соответствующего законодательства, невнимательного отношения к толкованию элементов состава преступления, а также непонимание технических условий функционирования телекоммуникационных сервисов, что приводит к искажению статистических данных.

По нашему мнению, несовершенство отечественной статистики можно также объяснить недостаточным пониманием содержания понятия «преступление в сфере информационной безопасности», что приводит к статистическим искажениям как в качественном, так и в количественном аспекте.

В этой связи актуальной задачей уголовного законодательства становится обеспечение эффективной правовой защиты информационных систем и ресурсов, с целью пресечения наиболее общественно опасных посягательств на информацию, информационные системы и сети.

Надо отметить, что именно в указанной сфере российское уголовное право оказалось не вполне готовым к стремительному развитию компьютерной техники, информационных технологий, а также к тому, что современная информационная сфера стала полем информационной агрессии против России, осуществляемой странами запада и США с использованием различных противоправных форм информационного воздействия.

Таким образом, **объектом** диссертационного исследования являются правоотношения, складывающиеся в сфере уголовно-правового обеспечения информационной безопасности, противодействия преступлениям, направленным против информационной безопасности России, а также проблемы совершенствования норм закона, устанавливающего уголовную

[3] В. Путин. У нас есть адекватный ответ на все угрозы[Электронный ресурс]. – Режим доступа: http://news.rambler.ru/29758066/

ответственность за указанные преступления.

Предметом диссертационного исследования является нормативно-правовая база, определяющая уголовную ответственность за преступления в сфере информационной безопасности, совокупность преступлений, связанных с информационной безопасностью, зарубежный опыт, а также информационная среда, нуждающаяся в уголовно-правовой защите.

Цель и задачи исследования. Основная цель исследования состоит в анализе уголовно-правовой природы преступлений, посягающих на теоретические основы информационной безопасности, в совершенствовании норм уголовного законодательства и оценке возможностей обеспечения информационной безопасности Российской Федерации с помощью норм Уголовного кодекса.

Реализация указанной цели предполагает решение следующих конкретных задач:

1. Рассмотреть понятие информационной безопасности как системы общественных отношений и объекта правовой охраны.

2. Проанализировать нормативно-правовые аспекты обеспечения информационной безопасности и её уголовно-правовой защиты в международном праве и в зарубежных странах.

3. Рассмотреть содержание понятия «преступление против информационной безопасности», предложить классификацию преступлений, относящихся к данной группе противоправных деяний.

4. Выделить и проанализировать преступления против компьютерной безопасности как составную часть преступлений против информационной безопасности.

5. Охарактеризовать с уголовно-правовой точки зрения преступления, посягающие на тайную информацию, охраняемую законом.

6. Рассмотреть иные составы преступлений против информационной безопасности по уголовному праву Российской Федерации.

7. Совершенствование уголовного законодательства.

Методология и методика. Методологической основой диссертационного исследования являются современные общенаучные методы познания, такие как системный подход, логический и диалектический методы познания, которые использовались в процессе выяснения правового содержания информационной безопасности. Метод классификации использовался в процессе систематизации преступлений, связанных с посягательствами на информационную безопасность, формулировка и обоснование теоретических положений, практических рекомендаций и выводов осуществлены с использованием метода обобщения, а также на основе использования метода анализа норм уголовного права.

Нормативную базу исследования составляют: Конституция Российской Федерации, УК РФ, российское федеральное законодательство, регламентирующее информационную безопасность, а также уголовное законодательство, регламентирующее информационную безопасность в зарубежных странах. Кроме того, значительную часть нормативной базы исследования составили международно-правовые нормы, содержащиеся в руководящих документах Организации Объединённых Наций, Совета Европы, Европейского Союза, Интерпола, Содружества Независимых Государств.

Эмпирическую основу работы составляют опубликованная судебная практика судов общей юрисдикции Российской Федерации по преступлениям, посягающим на информационную безопасность. Всего, автором данного исследования, проанализировано 105 уголовных дел по преступлениям в сфере информационной безопасности.

Степень научной разработанности темы. Анализ монографических исследований, диссертационных работ показывает, что проблемы информационной безопасности Российской Федерации в настоящее время изучены в недостаточной степени, большинство научных исследований посвящено правовому обеспечению информационной безопасности в сфере информационных технологий и компьютерной техники, не выходя своим

содержанием из данного проблемного круга.

Речь идёт о работах таких учёных как: Л.А. Букалерова, В.Б. Вехов, А.Г. Волеводз, О.А. Герасимова, Е.В. Громов, Ю.Гульбин, К.Н. Евдокимов, Л.Ю. Исмаилова, В. С. Карпов, В.С. Комиссаров, У.В. Зинина, М.А. Зубова, Д. А. Зыков, В.Д. Курушин, В.А. Минаев, И.А. Юрченкои т.д.

Что касается непосредственно проблем информационной безопасности, то данную проблему изучали А.Д. Калмыков [4], Н.И. Бусленко, В.Г. Шевченко, Н.В. Федотов, Г.Х. Архагов [5], А.В. Серебренникова [6], А.И. Смирнов[7], В.Г. Степанов-Егиянц[8], В.И. Ярочкин[9] и др.

Не смотря на то, что данные работы заложили научные основы для создания системы информационной безопасности в Российской Федерации, данная проблематика не утрачивает своей актуальности.

В тоже время, на сегодня Россия оказалась в состоянии информационной войны со странами, старающимися навязать нашей стране свои ценности, разрушить традиционные морально-нравственные устои российского общества. Развитие информационных технологий привело к тому, что информационная экспансия осуществляется системно, а преступления против информационной безопасности становятся все более изощрёнными и опасными.

В связи с этим, научная новизна диссертационного исследования заключается в получении новых знаний на основе рассмотрения информационной безопасности Российской Федерации, как широкого явления, имеющего отношение к различным сферам общественного бытия, гарантирующей государству, личности и обществу безопасное создание,

---

[4] Калмыков Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны : Дис. ... канд. юрид. наук : 12.00.08. – Ярославль, 2005. С. 219.

[5] Информационная безопасность России / В.Г. Шевченко, Н.В. Федотов, Г.Х. Архагов и др. – М., 2001. 623 с.

[6] Серебренникова А.В Уголовно-правовое обеспечение конституционных прав и свобод человека и гражданина по законодательству Российской Федерации и Германии / А.В. Серебренникова - М.: ЛексЭст, 2005. 304 с.

[7] Смирнов А.И. Информационная глобализация и Россия PDF. – Москва, 2005. 392 с.

[8] Степанов-Егиянц В.Г. Преступления в сфере безопасности обращения компьютерной информации: сравнительный анализ. Дис. … канд. юрид. наук: 12.00.08 / Степанов-Егиянц В.Г. - М., 2005. 168 с.

[9] Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Междунар. отношения, 2000. 400 с.

хранение и использование информации на основе правовой защиты информационных ресурсов, морали, нравственности и иных аспектов жизнедеятельности, связанных с информацией и информационным обменом.

Изучение российского и зарубежного уголовного законодательства, правоприменительной практики позволило автору сделать выводы о тенденциях и современных направлениях обеспечения информационной безопасности, о развитии положений уголовного права, регламентирующих ответственность за преступления в данной сфере.

Новизна исследования проявляется в совокупности авторских предложений, выводов и рекомендаций, направленных на совершенствование российского уголовного законодательства.

На защиту выносятся следующие положения и предлагаются выводы, которые имеют принципиальное значение для теории и практики уголовно-правового обеспечения информационной безопасности, борьбы с компьютерной преступностью в Российской Федерации:

1. Преступления против информационной безопасности следует рассматривать как широкий класс уголовно наказуемых деяний, посягающих на безопасность субъекта информационных отношений, как в социальной, так и в информационной среде. В исследовании предложена следующая классификация преступлений против информационной безопасности:

а) Преступления, посягающие на тайную (конфиденциальную) информацию, личную тайну, а также, преступления, направленные на распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 128.1 УК РФ, 137 УК РФ, ст. 138 УК РФ, ст. 138.1, ст. 146 УК РФ, ст. 155 УК РФ, ст. 183 УК РФ, ст. 170.1 УК РФ, ст. 183 УК РФ, ст. 283 УК РФ, ст. 283-1 УК РФ, ст. 310 УК РФ, ст. 311 УК РФ, ст. 320 УК РФ). Указанные преступления посягают на информацию, отнесённую законом к категории тайной, нарушают права участников информационных отношений на конфиденциальность информации.

б) Информационные преступления, направленные против безопасного обращения компьютерной информации, которые посягают на интересы личности и общества в сфере информационного обмена, создания, защиты, хранения и использования информации, хранящейся в компьютере. Речь идёт о преступлениях, обозначенных статьями 272 - 274 УК РФ, которые включённые в гл. 28 УК РФ, а также ст. 159. 6 УК РФ. Данная группа преступных посягательств нарушает права граждан на безопасное использование информации, находящейся на компьютерных носителях, в информационной сети.

в) Иные составы преступлений, направленные против прав граждан на получение информации, объектом преступных посягательств в данном случае являются законные конституционные права граждан на информацию (ст. 140 УК РФ, ст. 144 УК РФ, ст. 237 УК РФ).

2. Информационная безопасность представляет собой совокупность общественных отношений, которые регулируются системой правовых норм, направленных на обеспечение национальных интересов государства, интересов общества, на обеспечение законных интересов личности и субъектов хозяйствования в информационной сфере, гарантируют права человека и гражданина в информационной сфере, защиту информации от несанкционированного доступа, уничтожения, блокирования, модификации копирования, и неправомерного использования.

3. В отношении сбора информации в социальных сетях нецелесообразно говорить о целенаправленном сборе данной информации со стороны операторов социальных сетей, поскольку такая информация предоставляется пользователями добровольно. В этой связи следует говорить не о сборе информации, а о доступе к персональным данным, добровольно предоставляемыми пользователями социальных сетей, что не является преступлением. В тоже время раскрытие и распространение оператором персональных данных без согласия пользователя следует рассматривать как правонарушение, которое может повлечь за собой наступление уголовной

ответственности.

4. Анализ УК РФ и российской судебной практики по вопросам информационной безопасности позволил автору данного исследования предложить уточнить название ст. 137 УК РФ, изложив её в следующей редакции: «Незаконный доступ к сведениям, составляющим личную или семейную тайну».

5. Часть 1 ст. 159.6 УК РФ предлагается изложить в следующей редакции: «мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путём распространения с использованием информационных технологий ложной информации, ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей …(далее по тексту)».

6. Часть 2 ст. 272 УК РФ изложить в следующей редакции «То же деяние, направленное на перехват информации, совершенное с корыстным мотивом и причинившее крупный ущерб ….(далее по тесту).

7. Часть 1 ст. 274 УК РФ предлагается изложить в следующей редакции: «нарушение правил, касающихся информационных ресурсов, а также эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб … (далее по тексту)».

8. Сравнительный анализ ст. 159 УК РФ и ст. 159.6 РФ позволил установить, что законодатель лояльно подходит к проблеме наказания за мошенничество в сфере компьютерной, предоставляет необоснованные льготы виновным лицам, совершающим мошеннические действия в сфере компьютерной информации. Сделан вывод, что наказания за эти

преступления, как минимум, должны быть соразмерными, соответственно имеется необходимость внести соответствующие изменения в нормы Уголовного кодекса РФ.

9. В п. 7 ст. 2 Закона РФ «Об информации, информационных технологиях и о защите информации» предлагается установить, что «конфиденциальность информации представляет собой обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя, а также в случае, если запрет на передачу такой информации установлен законом, иным нормативно-правовым актом и данный запрет не противоречит положениям Конституции РФ».

10. Предлагается дополнить ст. 63 УК РФ пунктом «с», указав в нем, что совершение преступления с помощью компьютерной техники, информационных и сетевых технологий, является обстоятельством, отягчающим наказание.

Теоретическая значимость результатов исследования состоит в развитии теории уголовного права в части, касающейся правового содержания понятия «информационная безопасность», научных предпосылок для совершенствования норм УК РФ, предусматривающих ответственность за преступления в сфере информационной безопасности. Положения данного исследования имеют существенное значение при проведении дальнейших научных исследований в сфере уголовно-правового регулирования информационной безопасности.

Практическое значение результатов исследования состоит в разработке рекомендаций по совершенствованию уголовного законодательства и практики его применения. Результаты диссертационного исследования могут быть учтены при совершенствовании норм УК РФ, подготовке разъяснений Пленума Верховного Суда РФ, в деятельности следственных и судебных органов при расследовании и разрешении уголовных дел, связанных с обеспечением информационной безопасности.

Положения диссертационного исследования могут использоваться при подготовке позиции Российской Федерации в международных организациях, а также для совершенствования учебных курсов уголовного и информационного права в образовательных учреждениях высшего профессионального образования РФ.

Степень достоверности результатов диссертационного исследования. Сформулированные в исследовании выводы и рекомендации логически обоснованы и имеют высокую степень достоверности, что подтверждается совокупностью следующих положений:

- использованы данные, полученные учёными в ходе исследования теоретических основ информационной безопасности уголовной ответственности за нарушение избирательных прав и права на участие в референдуме;

- эффективно применён комплекс общенаучных и частнонаучных методов познания, составивших методику исследования;

- осуществлён сравнительный анализ обширной нормативно-правовой базы, включающей международные правовые акты, российское и зарубежное уголовное законодательство, регламентирующее информационную безопасность.

Апробация результатов диссертационного исследования. Положения, выносимые на защиту, докладывались на научных и научно-практических конференциях, в том числе на 3-й Международной научно-практической конференции «Информационные ресурсы и системы в экономике, науке и образовании» (Пенза, 2013), Международной конференции «Ренессанс естественно-правового понимания права» (апрель 2014 г.).

Основные положения диссертационного исследования докладывались и получили одобрение на заседании кафедры уголовного права и криминологии юридического факультета МГУ имени М.В. Ломоносова. Они

нашли своё отражение в шести научных публикациях, в том числе в четырёх статьях, опубликованных в ведущих рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве образования и науки Российской Федерации.

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

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, определяются его цели и задачи, объект и предмет исследования, его методологическая и эмпирическая основы, раскрывается научная новизна исследования, формулируются основные положения, выносимые на защиту, указывается теоретическая и практическая значимость, степень достоверности результатов проведённого исследования, а также представлены сведения об апробации полученных результатов.

Глава первая «Информационная безопасность государсва, личности и общества как объект уголовно-правовой защиты» состоит из трех параграфов.

В *первом параграфе «Понятие информационной безопасности как системы общественных отношений и объекта правовой охраны»* рассматривается феномен информации, анализируется понятие «информационная безопасность», в том числе её конституционно-правовое регулирование.

Сегодня только начинает осознаваться проблема «человек в информационном обществе»[10], возникает понимание того, что интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на

[10] Бачило И.Л. История и проблемы становления законодательства в области информатизации // Информационное право. 2005. № 2. С. 7.

использование информации в интересах осуществления не запрещённой законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.[11] Информация приобретает новые свойства, определяющие как её социально-экономическую ценность, так и правовое содержание. В последние десятилетия информация приобретает свойства мощного средства воздействия на общественно-политические, идеологические и социально-экономические процессы, становится своего рода оружием, которое требует создания системы противодействия, защиты информационных ресурсов, принадлежащих государственным органам, составляющим государственную, врачебную, личную тайн[12].В этой связи актуализируется проблема правового регулирования процессов, в которых информация начинает выступать как основа общественных отношений, возникающих при реализации информационных потребностей государства, личности и общества. Сложность определения рассматриваемого понятия состоит в том, что каждая наука, имеющая дело с информацией, предлагает свою дефиницию. В связи с этим в работе рассматриваются разные подходы в понимании информации. Проанализировав информацию с философской, кибернетической, коммуникативной и правовой точки зрения, автор приходит к выводу, что рассматривать информацию в отрыве от сложного и разнообразного процесса её передачи и получения, практически невозможно. В статическом состоянии информация перестаёт обладать тем огромным массивом полезных качеств, которыми она наделена, будучи способной к передаче. В противном случае она и превращается в просто сведения или данные, чья ценность состоит лишь в содержании, которое они несут. Поэтому, представляется, что под информацией следует понимать совокупность сведений и данных, процесс их передачи и получения, а также их психическое восприятие и оценка. С правовой точки зрения автор

[11] Крат Ю.Г. Основы информационной безопасности: учебн. пособие / Ю.Г. Крат, И.Г. Шрамкова. – Хараровск, Изд-во ДВГУПС, 2008. 112 с.
[12] Информатика для юристов и экономистов / Под ред. С.В. Симоновича. – СПб.: Питер, 2002. С. 20.

предлагает определять информацию, как субстанцию, имеющую способность трансформироваться в фактические социально-правые отношения по поводу обладания, распространения, продажи и передачи сведений, которые подлежат правовой защите и охране.

Обращаясь к определению термина «информационная безопасность», следует признать, что в научной литературе отсутствует единое мнение относительно его содержания. В работе рассмотрены существующие определения информационной безопасности и предложено авторское понимание. В юридическом смысле информационная безопасность – совокупность общественных отношений, которые регулируются системой правовых норм, направленных на обеспечение национальных интересов государства, интересов общества, на обеспечение законных интересов личности и субъектов хозяйствования в информационной сфере, гарантируют права человека и гражданина в информационной сфере, защиту информации от несанкционированного доступа, уничтожения, блокирования, модификации, копирования и неправомерного использования.

В процессе исследования информационной безопасности возникает проблема разграничения данного вида безопасности и безопасности общественной, поскольку, поместив главу 28 УК РФ в раздел IX «Преступления против общественной безопасности и общественного порядка», законодатель определил родовой объект посягательства преступлений в сфере компьютерной информации как отношения общественной безопасности, что представляется достаточно спорным. Учёные, исследовавшие проблемы общественной безопасности и общественного порядка, не склонны относить преступления в сфере информационной безопасности к данному виду преступности[13]. По нашему

[13]Ковалев М.И. Преступления против общественной безопасности // Уголовное право. Особенная часть: Учебник / М.И. Ковалев, В.Н. Петрашев / Под ред. проф. В.Н. Петрашева. М., 1999. 303 с.; Боков А.В. Преступления против общественной безопасности // Уголовное право России. Практический курс: Учебно-практическое пособие / Под общ. ред. Р.А. 471 с.; Комиссаров В.С. Преступления против общественной безопасности // Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. Г.Н. Борзенкова и В.С. Комиссарова. – М., 2004. 331 с.; Зелинская Н.А. Преступления против общественной безопасности // Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. проф. Л.В.

мнению, информационная безопасность в отдельных случаях обеспечивает безопасные условия при производстве различного рода работ, также посягательство на информационную безопасность оказывает влияние на безопасные условия жизни общества, однако, данная форма безопасности выходит за рамки производственного аспекта безопасности, сам компьютер едва ли следует рассматривать как источник повышенной опасности, хотя как и каждое преступление, данный вид преступности посягает на безопасные условия общественной жизни. Однако, соглашаясь с К.С. Бельским, и признавая, что общественная безопасность наряду с государственной, экономической, военной, политической, экологической, информационной, является разновидностью национальной безопасности[14], мы, таким образом, фактически ставим знак равенства между общественной и информационной безопасностью в смысле их юридической значимости. Т.е. информационная безопасность не рассматривается нами как элемент общественной безопасности, а получает целиком самостоятельную регламентацию.

Если обратиться к Доктрине информационной безопасности РФ[15], в которой под информационной безопасностью Российской Федерации понимается состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства, то можно сделать вывод, что основным вектором политики государства по обеспечению информационной безопасности является соблюдение конституционных прав и свобод человека в информационной сфере. Анализ норм Конституции позволяет выделить ряд статей, провозглашающих права и свободы человека, которые так или иначе связаны с информацией (ч. 4 ст. 29, ч. 5 ст. 29, ч. 1 ст. 23, ст. 33 ст. 42). В то

Иногамовой-Хегай, проф. А.И. Рарога, А.И. Чучаева. – М., 2004. С. 340 - 342.; Малков В.П. Преступления против общественной безопасности // Уголовное право России. Часть Особенная: Учебник для вузов / Отв. ред. Л.Л. Кругликов. 3-е изд., перераб. и доп. – М., 2005. С. 405 - 406.

[14] Бельский К. С. Полицейское право. Лекционный курс. – М.: «Дело и Сервис», 2004. – Режим доступа: http://www.pravo.vuzlib.su/book_z1044_page_44.html

[15] Доктрине информационной безопасности Российской Федерации (утв. Президентом РФ 09.09.2000 N Пр-1895) [Электронный ресурс]. – Режим доступа: http://www.rg.ru/oficial/doc/min_and_vedom/mim_bezop/doctr.shtm

же время Конституция РФ устанавливает и ряд принципиальных положений, касающихся гарантий информационной безопасности (ч. 1 ст. 46, ч. 1 ст. 21, ч. 1 ст. 23, ч. 1 ст. 24, ч. 1 ст. 46, ч. 2- 4 ст. 29, ст. 44, ст. 56).

Таким образом, информационная безопасность представляет собой сложную конституционно - правовую конструкцию, что определяется её социальной и правовой природой, основанной на многообразии информационных отношений в обществе; на дифференциации субъектов информационных отношений, имеющих свои интересы, права и обязанности в данной сфере; на объективном характере информационных отношений, которые в начале XXI века определяют развитие мировой цивилизации и системы международного права.

Второй параграф «Нормативно-правовые аспекты обеспечения информационной безопасности и её уголовно-правовой защиты в международном праве и в зарубежных странах» посвящён международно-правовому регулированию информационной безопасности, осуществляемому Организацией Объединённых Наций, Советом Европы, Европейским Союзом, Интерполом, Содружеством Независимых Государств, а также рассмотрению преступлений против информационной безопасности, в том или ином виде включённых в уголовное законодательство зарубежных стран.

Международно-правовой анализ в работе начинается со Всеобщей декларации прав человека, провозглашающей в ст. 19 право каждого «искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ».[16]

Учитывая, что в международном праве до сих пор не удалось создать единого подхода к определению информационной безопасности, в работе рассматриваются две полярные концепции относительно регулирования общественных отношений, касающихся проблем информационной безопасности. Сторонники первой концепции, которой придерживается и

[16]Всеобщая декларация прав человека Принята *резолюцией 217 А (III)* Генеральной Ассамблеи ООН от 10 декабря 1948 года. – Режим доступа: http://www.un.org/ru/documents/decl_conv/declarations/declhr

Россия, базируют свою позицию на широком понимании проблематики международной информационной безопасности. В её основу положены принципы неделимости безопасности и ответственности государств за своё информационное пространство. Согласно такому пониманию решения вопросов, касающихся поддержания информационной безопасности, противодействие угрозам военного (военно-политического), террористического и криминального характера с использованием ИКТ, должно осуществляться системно. Соответственно, международно-правовое регулирование должно быть распространено на все указанные структурные элементы, и ради достижения этого предложено принятие международного соглашения на универсальном уровне. Таким образом, начиная с 1998 г. на ежегодных сессиях ГА ООН был принят ряд резолюций, посвящённых проблемам информационной безопасности. По результатам работы ГА ООН участники пришли к пониманию того, что «информационные компьютерные технологии могут использоваться в целях, несовместимых с задачами обеспечения международной стабильности и безопасности, а также негативно воздействовать на целостность инфраструктуры внутри отдельных государств, нарушая их безопасность, как в гражданской, так и в военной сфере»[17].

В рамках данной концепции особое место уделяется вопросу регулирования структурных элементов международной информационной безопасности. В связи с этим в работе рассмотрены два основных направления международно-правового регулирования использования ИКТ: информационный («содержательный») и коммуникационный («технический»), которые в доктрине определяются как функциональные. В международно-правовой проблематике информационной безопасности данные элементы рассматриваются с позиций противодействия использования ИКТ, направленного на вред основным правам и свободам

[17] Международное сотрудничество в области информационной безопасности (справочная информация). [Электронный ресурс]. – Режим доступа: http://www.ln.mid.ru/ns-dvbr.nsf/0/4c86fcb9f8dc1b41c3256e320029b1ef?OpenDocument

человека и критически важным структурам государств. В случае с информационным («содержательным») направлением – это противодействие трансграничному распространению посредством ИКТ информации, что противоречит принципам и нормам международного права, разжигает межнациональную, межрасовую и межконфессиональную вражду, распространяет расистские, ксенофобские письменные материалы, изображения или любую демонстрацию идей или теорий, которые пропагандируют, подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц. В случае с коммуникационным («техническим») направлением – это противодействие использованию коммуникационных систем, процессов и ресурсов против коммуникационных сетей и критически важных структур других государств, что наносит ущерб функционированию финансовой, политической, экономической и социальной системам.

В рамках данных направлений автор рассматривает такие международно-правовые акты, как Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г.[18], Конвенции о киберпреступности от 23 ноября 2001 г.[19] и Дополнительный протокол к Конвенции о киберпреступности, который касается криминализации действий расистского и ксенофобского характера, совершенных через компьютерные системы от 28.01.2003 г.[20], что были приняты в рамках Совета Европы, Соглашения между правительствами

[18] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. Ратифицировано Федеральным законом РФ от 1 октября 2008 года N 164-ФЗ. – Режим доступа: http://docs.cntd.ru/document/902140948

[19] Конвенция о киберпреступности [Электронный ресурс].– Режим доступа: http://conventions.coe.int/Treaty/RUS/ Treaties/Html/185.htm

[20] Дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и ксенофобского характера, осуществляемых при помощи компьютерных систем, г. Страсбург, 28 января 2003 года [Электронный ресурс].– Режим доступа:http://mvd.gov.by/ru/main.aspx?guid=4593

государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. [21].

Сторонники второй, «узкой» концепции, настаивают на том, что основу международной информационной безопасности составляет только один элемент – борьба с уголовными преступлениями в сфере информационно-коммуникационных технологий. Реализуя данную концепцию в практическом плане, Совет Европы разработал Конвенцию о киберпреступности, которая вступила в силу 1 июля 2004 г. В рамках этой концепции, в связи с тем, что её сторонники не рассматривают террористический и военный элементы как составные элементы международной информационной безопасности, вопрос о регулировании функциональных элементов (информационного и коммуникационного) не рассматривается как перспективный для международно-правового разрешения.

В целом, можно утверждать, что информационная безопасность в её международно-правовых основах представляет собой широкий перечень документов, который является основой для конструирований аналогичного понятия в российской национальной доктрине информационной безопасности, а также для её понимания в уголовно-правовом смысле.

Основываясь на проведённом в работе анализе международных документов и научной литературе, которая касается комплекса вопросов информационной безопасности человека, учреждения, общества и государств[22], мы можем рекомендовать включить в будущий международный нормативный акт в сфере информационной безопасности (создание которого

[21] Соглашения между правительствами государств-членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. [Электронный ресурс].– Режим доступа: http://www.worklib.ru/law/96355/

с[22]Калмыков Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны: Дис. ... канд. юрид. наук : 12.00.08. – Ярославль, 2005. С. 219, Информационная безопасность России / В.Г. Шевченко, Н.В. Федотов, Г.Х. Архагов и др. – М., 2001.623 с., Смирнов А.И. Информационная глобализация и Россия PDF. – Москва,2005. 392 с., Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Междунар. отношения,2000. 400с., Петров В. К. От информационных войн к управляемой конфронтации и сотрудничеству / В. К. Петров, И. И. Рабинович // Власть. 2001. № 1. С. 21.

предусмотрено многочисленными Резолюциями ГА ООН) такие виды международной информационной безопасности, как глобальная информационная безопасность (т.е. безопасность международного сообщества); информационная безопасность отдельных государств в международном информационном пространстве; информационная безопасность учреждений в международном информационном пространстве; информационная безопасность личности в глобальной информационной среде.

Дальнейшее изучение нормативно-правовых аспектов обеспечения информационной безопасности сводится к рассмотрению преступлений против информационной безопасности, включённых в Уголовные кодексы Нидерландов, ФРГ, Франции, Испании, Республики Узбекистан, Республики Молдова, Республики Армения.

В *третьем параграфе «Содержание понятия «преступление против информационной безопасности» и их классификация»* рассматриваются статистические тенденции развития в России преступлений, посягающих на основы информационной безопасности, даётся характеристика и классификация таких преступлений.

Важность исследования данных проблем велика, поскольку на сегодня рассматриваемый вид преступности, во-первых, вышел за рамки традиционной компьютерной преступности, а во-вторых, стал самостоятельным криминальным явлением, динамично развивающимся под воздействием мировых процессов глобализации и информатизации, а также под непосредственным воздействием постоянных атак на информационное пространство России.

В связи со сложностью выделения единого объекта данных преступлений, множественностью предметов преступного посягательства с точки зрения их уголовно-правовой охраны, в научной литературе предлагаются совершенно разные подходы в классификации преступлений в сфере информационной безопасности. В диссертационной работе

рассмотрены классификации экспертов международных организаций, в том числе подробный кодификатор компьютерных преступлений Генерального Секретариата Интерпола, а также классификации, предложенные такими учёными, как Ю.М. Батурин и А.М. Жодзишский, С.С. Шахрай, А.Г. Волеводз.

Опираясь на данные исследования, автором предлагается классификация преступлений в сфере информационной безопасности, в основе которой лежит принципиальное положение Доктрины информационной безопасности Российской Федерации относительно того, что под информационной безопасностью Российской Федерации следует понимать состояние защищённости её национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Определив в качестве общего объекта рассматриваемых преступлений правоотношения в сфере информационного обмена, создания, защиты, хранения и использования информации, родового объекта — интересы государства, экономические интересы субъектов хозяйствования, интересы личности в информационной сфере и, выбрав в качестве единого критерия предлагаемой классификации непосредственный объект преступлений, — права владельцев информации на её неприкосновенность, безопасное использование и распространение, автором предлагается разделить преступления против информационной безопасности на следующие группы:

1. Преступления, посягающие на тайную (конфиденциальную) информацию, личную тайну, а также, преступления, направленные на распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию. В данном случае речь идёт о преступных деяниях касающихся личной тайны, которая охраняется статьями ст. 128.1 УК РФ, 137 УК РФ, ст. 138 УК РФ, ст. 138.1, ст. 146 УК РФ, ст. 155 УК РФ, ст. 183 УК РФ, а также преступления, направленные на фальсификацию информации: ст. 170.1 УК РФ; коммерческой, налоговой и

банковской тайны – ст. 183 УК РФ, государственной тайны – ст. 283 УК РФ, ст. 283-1 УК РФ, тайны предварительного следствия – ст. 310 УК РФ, сведений о мерах безопасности в отношении судьи и участников уголовного процесса – ст. 311 УК РФ, сведений о мерах безопасности, применяемых в отношении должностного лица правоохранительного или контролирующего органа – ст. 320 УК РФ.

Указанные преступления посягают на информацию, отнесённую законом к категории тайной, нарушают права участников информационных отношений на конфиденциальность информации.

2. Информационные преступления, посягающие на безопасное обращение компьютерной информации, на интересы личности и общества в сфере информационного обмена, на информацию, хранящуюся на различных информационных носителях, в компьютере. Речь идёт о преступлениях, обозначенных статьями 272 – 274 УК РФ, которые включены в гл. 28 УК РФ, а также ст. 159.6 УК РФ.

Данная группа преступных посягательств нарушает права граждан на безопасное использование информации, находящейся на компьютерных носителях, в информационной сети.

3. Иные составы преступлений, направленные против прав граждан на получение информации, объектом преступных посягательств в данном случае являются законные конституционные права граждан на информацию, речь идёт о преступлениях, обозначенных ст. 140 УК РФ, ст. 144 УК РФ, ст. 237 УК РФ.

Как представляется, перечень данных преступлений должен быть открытым, поскольку постоянно совершенствующаяся компьютерная техника, информационные и сетевые технологии создают новые угрозы информационной безопасности и соответственно уже в ближайшем будущем, возможно ожидать появление новых форм преступности в информационном пространстве Российской Федерации.

Автором также делается обоснованное в работе предложение

дополнить ст. 63 УК РФ пунктом «с» и отнести к обстоятельствам, отягчающим наказание, совершение преступления с помощью компьютерной техники, информационных и сетевых технологий.

Глава вторая «Правовая характеристика преступлений против информационной безопасности по уголовному праву Российской Федерации» состоит из трёх параграфов.

В *первом параграфе* «*Преступления против компьютерной безопасности как составная часть преступлений против информационной безопасности»* анализируются преступления, входящие в гл. 28 УК РФ.

В научной юридической литературе, изучающей проблемы информационной безопасности, понятие «компьютерное преступление» является центральным, однако окончательно не определённым. По нашему мнению, компьютерными преступлениями следует признать общественно опасные деяния, которые направлены на причинение вреда (либо создающие угрозу причинения вреда) общественным отношениям в сфере законного пользования компьютерной информацией, что влечёт за собой привлечение к уголовной ответственности.

Система компьютерных преступлений в российском законодательстве регулируется главой 28 УК РФ, где предусмотрена уголовная ответственность за неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Анализ норм УК РФ показывает, что данные преступления направлены на уничтожение, блокирование, модификацию либо копирование компьютерной информации, а также в отдельных случаях на нейтрализацию средств защиты компьютерной информации[23], хотя при этом по юридическим признакам

[23]Уголовное право России. Особенная часть./ Под ред. В.Н. Кудрявцева, А.В. Наумова. -3-е изд., перераб. и доп. – М.: Юристъ, 2005. С. 350.

между данными преступными деяниями имеется существенная разница. В первую очередь, как представляется автору данной работы, внимание следует уделить вопросам, касающимся разграничения неправомерного доступа к компьютерной информации (ст. 272 УК РФ) и созданием, использованием и распространением вредоносных компьютерных программ (ст. 273 УК РФ).

Проанализировав ст. 272 УК РФ, неправомерный доступ к компьютерной информации следует квалифицировать как деяние, направленное на незаконное вмешательство в информационную систему, компьютер, которое нарушает права собственника информации и наносит ему вред в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. Таким образом, данный состав имеет материальный характер, преступное деяние обязательно влечёт за собой наступление указанных выше последствий, а субъектом данного преступления является любое вменяемое физическое лицо, достигшее 16-летнего возраста.

Вместе с тем ст. 272 УК РФ, устанавливая уголовную ответственность за неправомерный доступ к компьютерной информации, не рассматривает возможностей её похищения, хотя сам термин «хищение» в отношении информации присутствует в научных исследованиях. Например, в работах конца XX – начала XXI века данный термин весьма активно использовался для обозначения преступных деяний, связанных с незаконным доступом к информации[24]. По нашему мнению, ориентируясь на родовое понятие «хищения», похищением компьютерной информации следовало бы понимать как противоправное безвозмездное изъятие информации, программного обеспечения, совершенное с корыстной целью, причинившие ущерб собственнику или иному владельцу данной информации либо программного

---

[24] Максимов В.Ю. Компьютерные преступления (вирусный аспект). –Ставрополь: Книжное издательство, 1999. 112 с.; Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. – М.: МЦНМО, 2002. 296 с.; Юсупов Р.М. Научно-методологические основы информатизации / Р.М. Юсупов, В.П. Заболотский. – СПб.: Наука, 2000. 455 с.

обсечения. Тем не менее понятие «похищение» в сфере компьютерной безопасности, как правило, не используется, вместо него используется термин «перехват», т.е. неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, приём и обработку информативных сигналов[25].

Однако, ч. 1 ст. 272 УК РФ в качестве уголовно наказуемых действий предусматривает лишь уничтожение, блокирование, модификацию либо копирование компьютерной информации, а в ч. 2 данной статьи указывается, что данное деяние может причинить крупный ущерб и быть совершенным с корыстным умыслом, т. е. ч. 2 ст. 272 фактически описывает состав хищения. В этой связи, по нашему мнению, ч. 2 ст. 272 УК РФ нуждается в уточнении и рекомендуется её изложить в следующей редакции: «То же деяние, направленное на перехват информации, совершенное из корыстной заинтересованности и причинившее крупный ущерб… (далее по тесту).

Рассматривая состав преступления, описанного ст. 273 УК РФ, следует указать на то, что объектом данного состава преступления является совокупность общественных отношений, которые обеспечивают законное и безопасное использование информации, а его объективную сторону составляет создание компьютерной программы (вирус, компьютерный червь, программа-сканер, программа-эмулятор, программа-патчер и т. д.), которая изначально предназначена для уничтожения, блокирования, модификации, копирования компьютерной информации, имеет функцию нейтрализации средств защиты информации. Способ совершения указанного преступления представляет собой действие, которое выражается в форме целенаправленной работы над созданием вредоносных компьютерных программ, а также действий, направленных на их использование, распространение. Таким образом, данный состав можно определить как формальный, необходимо особо подчеркнуть тот факт, что согласно содержанию ч. 1 ст. 273 УК РФ для того, чтобы деяние было признано

[25] Бытко С.Ю. Некоторые проблемы уголовной ответственности за преступления, совершенные с использованием компьютерных технологий: Дис. ... канд. юрид. наук: 12.00.08. – Саратов, 2002. С. 34.

преступным не требуется фактического наступления последствий в виде уничтожения, блокирования, модификации либо копирования информации. Что касается субъективной стороны преступления, которое предусмотрено ч. 1 ст. 273 УК РФ, то она характеризуется прямым умыслом, который выражается в создании вредоносной программы (например, программы-вируса) с целью уничтожения, блокирования, модификации, копирования информации, а также с целью нарушения работы информационно-телекоммуникационных сетей и использовании компьютерных программ (т. е. действия, направленные на ввод таких программ в хозяйственный оборот), распространении программ (т. е. предоставления доступа к таким программам), субъектом данного преступления, также является любое вменяемое физическое лицо, достигшее 16-летнего возраста. При этом, анализируя содержание ст. 273 УК РФ, можно утверждать, что данное деяние может быть совершено и с косвенным умыслом.

Как представляется автору данной работы, «использование» и «распространение» вредоносных программ по объёму вредоносных последствий не является одинаковым, распространение всегда провоцирует использование, и в этой связи, уголовная ответственность за распространение вредоносных программ должна быть более суровой, нежели за их использование.

Таким образом, можно констатировать, что различия между неправомерным доступом к компьютерной информации и созданием, использованием и распространением вредоносных программ заключаются в юридических признаках предмета преступного посягательства, в содержании общественно опасных деяний, которые приводят к вредным последствиям, в субъективной стороне преступления, которое даёт представления об отношении лица к совершенному деянию, а также к его последствиям.

Что касается ст. 274 УК, то она устанавливает уголовную ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо

информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб (ч. 1 ст. 274 УК РФ), в том числе, когда такие деяния имеют тяжкие последствия или создало угрозу их наступления (ч. 2 ст. 274 УК РФ). Таким образом, объективной стороной данного преступления следует считать нарушения правил эксплуатации компьютеров, информационно-телекоммуникационных сетей, которые повлекли за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Данный состав является материальным, а его необходимым признаком следует считать причинение крупного ущерба, причём, между правонарушением и наступлением ущерба должна быть причинная связь. При этом негативные последствия должны являться следствием именно нарушения правил эксплуатации, а не ошибкой работы программы, либо следствием действий, уголовная ответственность предусмотрена статьями ст. 272 УК, 273 УК РФ.

Для данной статьи важным отличительным фактором является то, что в данном случае признак неправомерного доступа к компьютерной информации отсутствует, отсутствует и возможность наступления последствия в виде несанкционированного копирования информации. Виновное лицо в силу своего служебного положения, выполняя функциональные обязанности, пользуется информацией на законных основаниях, соответственно в отличие от ст. 272 УК РФ субъектом данного преступления следует признать законного пользователя информации, который осуществляя то или иное деяние, не имеет прямого умысла нанести ущерб. Следует также указать и на то, что деяния, предусмотренные ст. 272 УК и 273 УК РФ, являются следствием совершения активных действий, в то время как ст. 274 УК предусматривает уголовную ответственность за деяния, которые совершены, в том числе и путём

бездействия.

Кроме того существенным признаком объективной стороны преступных деяний, предусмотренных главой 28 УК РФ, являются общественно опасные последствия, хотя следует признать, что их нельзя считать равнозначными как по внутреннему содержанию, так и по объёму.

Уголовная ответственность, согласно норме, изложенной в ст. 274 УК РФ, предусмотрена только за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации. Как представляется автору данной работы, существенным пробелом такой формулировки является то, что данная статья обходит проблему нарушения правил создания информации. Например, разработчики информационных ресурсов, несущих в себе конфиденциальную информацию, должны позаботиться о создании средств её защиты. Если же таковые изначально не созданы, то это может свидетельствовать о преступной халатности, которая может повлечь за собой наступление тяжких последствий (угрозу их наступления). В связи с этим, автором предлагается ввести соответствующие изменения в текст ч. 1 ст. 274 УК РФ, которую необходимо изложить в следующей редакции: «нарушение правил создания информационных ресурсов, а также эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб … (далее по тексту)».

В целом можно говорить, что компьютерная преступность является составной частью преступлений против информационной безопасности, представляя собой, при этом, тот вид преступности, который нашёл отражение в нормах Уголовного кодекса Российской Федерации. В то же время с развитием компьютерных технологий вполне возможно появление

новых составов преступлений, требующих адекватного ответа государства, их включения в действующий Уголовный кодекс.

Во *втором параграфе «Уголовно-правовая характеристика преступлений, посягающих на тайную информацию, охраняемую законом»* рассматриваются проблемные вопросы, связанные с уголовно-правовым регулированием информации ограниченного доступа.

Отдельное внимание в работе уделяется проблемам правовой защиты информации в социальных сетях. Состояние, связанное с оборотом информации в социальных сетях, которые сегодня практически находятся вне правового регулирования и контроля со стороны общества и государства, должно рассматриваться как одна из угроз национальной безопасности России. В этой связи обеспечение контроля над обработкой персональных данных в социальных сетях и их защита приобретает первостепенное значение. В целом, по нашему мнению, применительно к социальным сетям сложно говорить о целенаправленном сборе информации, поскольку в большинстве случаев пользователи данных сетей самостоятельно и осознано доверяют информацию о себе операторам этих сетей.

Таким образом, мы можем констатировать, что доступ оператора к персональным данным не является правонарушением, в то время как раскрытие и их распространение, без согласия субъекта персональных данных, влечёт за собой юридическую ответственность, поскольку в данном случае имеет место нарушение закона.

В целом, проведённый анализ позволяет утверждать, что в настоявшее время отсутствует единый закреплённый перечень видов информации, относимой законом к тайне, что порождает неоднозначность и сложность в реализации механизмов обращения с такой информацией, очевидно и то, что предложенные нормативно-правовыми актами классификации не совпадают в полной мере.

Рассматривая существующие в научной литературе определения межотраслевого понятия «тайна», автор предлагает следующую дефиницию:

тайна – режим ограниченного доступа к информации, имеющей как материальную, так и иную ценность для принимающего меры по её охране правообладателя, нарушение конфиденциальности которой влечёт определяемые законом юридические последствия.

Представляется, что наиболее значимыми основаниями, по которым та или иная информация становится предметом тайны, являются следующие:

– охрана неприкосновенности частной жизни.

– охрана безопасности российской федерации.

– охрана профессиональной, служебной и коммерческой деятельности.

– охрана предварительного следствия судопроизводства.

– охрана института выборов.

В работе рассмотрены различные деления информации конфиденциального характера, предложенные А. В Серебренниковой, С.Д. Бражником, Б.В. Веховым, И.В. Смольковой, И.В. Бондарь, Д.В. Огородовым, С.В. Кузьминым, С.И. Сусловой, С.М. Паршиным.

По мнению автора, Уголовным кодексом Российской Федерации должны защищаться четыре вида тайн:

1) тайны личности, к которым относятся тайна частной жизни (личная и семейная), тайна переписки, тайна телефонных переговоров, почтовых, телеграфных и иных сообщений, тайна голосования, тайна усыновления (удочерения);

2) тайны, связанные с экономической деятельностью хозяйствующих субъектов – коммерческая, налоговая и банковская тайны;

3) государственная тайна;

4) тайны, обеспечивающие функционирование государственной власти, среди которых выделяются тайны правосудия (тайна предварительного расследования и тайна мер безопасности участников уголовного процесса) и тайну мер безопасности должностного лица или правоохранительного или

контролирующего органа[26].

Анализ предложенных разновидностей тайн начинается в работе с информации, составляющую личную тайну. Конституционные положения, гарантирующие право на доступ к информации, неприкосновенность частной жизни, тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, санкционируются главой 19 Уголовного кодекса Российской Федерации. Закреплённое в ст. 22 Конституции РФ право на неприкосновенность частной жизни, находит своё уголовно-правовое отражение в ст. 137 УК РФ «нарушение неприкосновенности частной жизни», предусматривающую ответственность за «незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации». Оценочный характер данных категорий, как известно, затрудняет криминализацию. Сложность составляет в первую очередь то, что в каждом индивидуальном случае схожие по характеру сведения могут как относится к тайным, так и являться доступными для третьих лиц. Вопрос о том, относится ли информация к личной или семейной тайне, решается лицом, а относительно семейной тайны, двумя или более лицами, которым эта информация принадлежит. То есть, к категории тайны информация здесь относится исходя не из объективных, а субъективных критериев, только по усмотрению самого лица.

Отметим, что диспозиция статьи 137 УК РФ устанавливает ответственность за незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, в то время как статья 24 Конституции Российской Федерации, как уже было отмечено в данном исследовании запрещает сбор, хранение, использование и распространение информации о частной жизни лица. Таким образом, при сравнении норм, очевидно, что Конституцией закреплён более широкий

[26]Паршин С.М. Тайна в уголовном законодательстве (теоретико-прикладное исследование): Дисс. ... канд. юрид. наук. – Н.Новгород, 2006. С. 58.

перечень недопустимых действий и именно данные перечень действий целесообразно закрепить в ст. 137 УК РФ.

В качестве формы нарушения тайны частной жизни в ч. 3 ст. 137 выделено распространение сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Позиция законодателя по поводу отграничения распространения вообще от публичного распространения была бы ясна, если бы большая общественная опасность последнего подтверждалась перемещением такого способа в часть вторую статьи. Публичность, то есть придание огласке информации, предпочитаемой сохранить в тайне, действительно повышает в разы вред, способный причинить лицу, в связи с чем, помещение разных по общественной опасности способов на один уровень, а тем самым установление одинаковый санкции, нельзя считать верным.

Следует сказать, что анализ ст. 137 УК РФ приводит к выводу о необходимости её уточнения, исходя из буквы закона. Именно через понятие «неприкосновенность частной жизни» определены пределы уголовно-правовой защиты, хотя в отдельных случаях информация относительно частной жизни гражданина подлежит обнародованию не зависимо от его желания. Из выше сказанного следует, что круг отношений, входящих в сферу частной жизни, но не относящихся к личной или семейной тайне, не подлежит уголовно-правовой охране. В этой связи, название ст. 137 УК РФ предлагается сформулировать следующим образом – «Незаконный доступ к сведениям, составляющим личную или семейную тайну», и уточнить ч. 1 ст. 137, изложив её в следующей редакции: сбор, хранение, использование и распространение информации о частной жизни лица, составляющих его личную или семейную тайну, без его согласия, либо без оснований, прямо указанных в Законе, а также распространение этих сведений в публичном выступлении, в публично демонстрирующемся произведении или средствах массовой информации (далее по тексту).

Следующей по значимости уголовно-правовой нормой, охраняющей

исследуемое нами явление «тайна», является ст. 138 Уголовного Кодекса Российской Федерации. В ст. 138 УК РФ говорится о переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях, которые все по своей сути являются способами обмена информацией, сообщениями между людьми. Под нарушением тайны переписки и иных сообщений граждан понимается незаконное ознакомление с содержанием письменных, телеграфных сообщений или полученных компьютерными системами связи, а также прослушивание телефонных переговоров. К последним следует относить также переговоры, ведущиеся по радиосетям связи[27].На наш взгляд, ст. 138 УК РФ должна устанавливать ответственность не только за незаконное нарушение тайны сообщений, но и тайны связи. Такое дополнение позволит решить проблемные вопросы с уничтожением корреспонденции любого вида, её утерей, в особенности случаи, когда потерянное письмо или иное сообщение становится доступным третьим лицам. В таких случаях письмо, утрачивая принадлежность определённому лицу, приобретает статус бесхозного, т.е. нарушается право на тайну переписки не конкретного лица, а тайна связи вообще.

Следует отметить, что и ФЗ «Об информации, информационных технологиях и о защите информации», и Указ Президента №188, среди разновидностей тайн выделяют коммерческую тайну, как сведения конфиденциального характера, связанные с коммерческой деятельностью. Уголовный кодекс объединяет в одной ст. 183 три предмета правовой охраны: коммерческую, налоговую и банковскую тайну. Две последние разновидности относятся в указанных перечнях к сведениям, связанным с профессиональной деятельностью. Помещение ст. 183 в раздел 8 «Преступления в сфере экономики» главы 22 «Преступления в сфере экономической деятельности» объясняется тем, что посягая на информационные отношения, эти преступления при этом относятся к

[27] Устинова Т.Д.Уголовная ответственность за нарушение тайны переписки, телефонных и иных сообщений граждан // Ваш адвокат. – М.: Интел- Синтез, 1998, №3. С. 38.

экономическим, что говорит о том, что данная норма защищает информационно-экономическую безопасность.

В работе рассматривается уголовно-правовое регулирование коммерческой, налоговой и банковской тайны, а также проблема правовой трансформации одних и тех же по содержанию экономических сведений из одной тайны в другую.

В диссертационном исследовании также освещён вопрос оснований уголовной ответственности за распространение сведений, содержащих врачебную и адвокатскую тайну.

В *третьем параграфе «Иные составы преступлений против информационной безопасности по уголовному праву Российской Федерации»* рассматриваются деяния, ответственность за которые предусмотрена статьями159.6, 170-1 и 237 УК РФ.

Ст. 159.6 УК РФ устанавливает ответственность за мошенничество в сфере компьютерной информации предусмотрено, где оно трактуется как «хищение имущества или приобретение права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации или иного вмешательства в функционирование средств хранения, обработки и передачи информации или информационно-телекоммуникационных сетей».Соответственно, поскольку мошенничество в сфере компьютерной информации наносит ущерб законным интересам участниками правоотношений посредством использования информационных технологий, то данные преступления целесообразно отнести к информационным. Следует признать, что в данном случае информационная безопасность может выступать лишь дополнительным объектом преступного посягательства, в то время как основным объектом преступления являются отношения собственности в сфере компьютерной информации, владения имуществом, то есть совокупности вещей, которые находятся в собственности лица (включая деньги и ценные бумаги), а также имущественных прав на получение вещей или имущественного удовлетворения от других лиц.

Приобретение права на чужое имущество в рассматриваемом случае является следствием мошеннических действий именно в компьютерно-информационной среде, когда происходит ввод информации, способствующей хищению, возникновению права на имущество, иные активы, удаления информации, с целью совершения хищения, её блокирования с целью недопущения доступа к информации, либо её модификации, ведущей к искажению информации, вследствие чего возникают условия для совершения мошенничества.

Следует обратить внимание на то, что хищение денежных средств, находящихся на счёте в банке, с помощью «взлома» защищённой компьютерной информации не может расцениваться как мошенничество, поскольку в данном случае отсутствует факт обмана, так как отсутствует физическое лицо, введённое в заблуждение злоумышленником. Для того, чтобы правильно квалифицировать содеянное как мошенничество в сфере компьютерной информации, необходимо наличие признака явно выраженного обмана физического лица, а также в определённых случаях неправомерного доступа к защищённой информации с намерением ввести лицо в заблуждение с целью получить чужое имущество или право на имущество (что-либо ценное).

Содержание статьи 159.6 УК РФ позволяет говорить о том, что в основе большинства мошеннических действий лежит использование возможностей Интернета, мобильной связи, в связи с чем, возможно, целесообразно внести изменения в название данной статьи Уголовного кодекса, назвав её «Мошенничество с использованием информационных технологий».

Не совсем понятна логика законодателя, предусматривающего различные санкции за простое (ст. 159 УК) и квалифицированное мошенничество (ст. 159.6 УК РФ). По мнению автора данной работы наказания за эти преступления, как минимум, должны быть соразмерными,

соответственно имеется необходимость внести необходимые изменения в нормы Уголовного кодекса.

Кроме проанализированного выше состава преступления Уголовный кодекс предусматривает также уголовную ответственность за фальсификацию и сбор информации с использованием компьютерных технологий. Например, в ст. 170-1 УК РФ речь идёт о фальсификации единого государственного реестра юридических лиц, реестра владельцев ценных бумаг или системы депозитарного учёта. В практическом плане, сущностью данного преступного деяния является внесение в реестр владельцев ценных бумаг, в систему депозитарного учёта, ведущихся, как правило, в электронном виде, заведомо ложных данных путём неправомерного доступа к реестру либо к системе депозитарного учёта. С практической точки зрения это означает, что данные действия включают в себя уничтожение истинной информации и внесение заведомо ложных сведений в указанные информационные базы данных.

Как представляется, данное преступное деяние следует рассматривать как один из этапов преступной деятельности, поскольку вслед за фальсификацией должно последовать дальнейшее действие, например попытка завладения имуществом, либо иных выгод для лица, совершившего фальсификацию. Если же данное преступление остаётся неоконченным в силу различных причин, то уже сам факт видоизменения данных служит основанием для того, чтобы данное деяние квалифицировать как попытку совершения преступления.

УК РФ относить к уголовно-наказуемым деяниям и сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей (ст. 237 УК РФ). Обязательным условием для наступления уголовной ответственности в данном случае является наступление опасности для жизни и здоровья населения именно как следствие сокрытия информации.

Безусловно, что данными деяниями не ограничивается весь широкий

спектр составов, которые могут включать в себя использование компьютерных и информационных технологий, о чем уже шла речь в данном исследовании.

В этой связи, ведётся полемика относительно включения новых составов преступлений, посягающих на информационную безопасность, в Уголовный кодекс. Оправданным представляется внесение в ряд статей Уголовного кодекса квалифицирующего признака «применение информационных технологий». Как представляется автору данной работы введение указанного квалифицирующего признака способно, в определённой мере, облегчить квалификацию преступлений, связанных с информационной безопасностью и совершаемых с использованием компьютерных технологий.

Таким образом, современный этап развития информационных технологий обуславливает необходимость принятия мер по совершенствованию уголовного законодательства, в части противодействия преступности, связанной с использованием информационных технологий. Кроме того, по мнению автора данной работы, речь идёт о необходимости постоянного мониторинга состояния преступности в данной сфере с целью системного совершенствования уголовного законодательства, направленного на борьбу с преступлениями в информационной сфере.

В **заключении** подведены итоги исследования, сформулированы выводы, основные рекомендации и перспективы дальнейшей разработки темы исследования по совершенствованию уголовно-правового законодательства, посвящённого регулированию информационной безопасности в Российской Федерации.

Список опубликованных научных работ по теме диссертационного исследования.

Статьи, опубликованные в ведущих рецензируемых журналах и изданиях, указанных в перечне ВАК Министерства образования и науки Российской Федерации:

1. Мнацаканян А.В. Преступления в сфере безопасности компьютерной информации как элемент системы особенной части УК РФ // Пробелы в российском законодательстве.2012. № 3. С. 158 – 161. (0,14 п.л.)

2. Мнацаканян А.В. Использование технических устройств и информационных технологий в преступных целях как обстоятельство, отягчающее уголовную ответственность // Пробелы в российском законодательстве. 2014. № 3. С. 159-162. (0,14 п.л.)

3. Мнацаканян А.В. Классификация преступлений против информационной безопасности РФ с точки зрения текущей общественно-политической ситуации // Бизнес в законе. 2014. №2. С. 270-273. (0,14 п.л.)

4. Мнацаканян А.В. Тайна как предмет уголовно-правовой охраны // Социально-политические науки. 2015. №1. С. 84-87. (0,14 п.л.)

Статьи, опубликованные в иных изданиях:

5. Мнацаканян А.В. Информационные ресурсы и системы в жизни общества // Развитие информационного законодательства в РФ: сборник статей III Международной научно-практической конференции // Пенза: Приволжский Дом знаний. 2013. С. 3-5. (0,09 п.л.)

6. Мнацаканян А.В. Сущность понятия и особенности классификации компьютерных преступлений и компьютерной информации как объекта противоправных посягательств // Ренессанс естественно-правового понимания права: международная конференция // Санкт-Петербург: Фонд развития юридической науки. 2014. С. 119-123. (0,19 п.л.)