Министерство образования и науки Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»

На правах рукописи

СЕЛИВАНОВА ТАТЬЯНА АНДРЕЕВНА

«Правовые механизмы обеспечения информационной безопасности личности в интернете»

направления подготовки 40.04.01 – «Юриспруденция»
юридического факультета СГУ им. Н.Г.Чернышевского

Автореферат магистерской работы

профессор, д-р юрид. наук,
профессор С.Е. Чаннов

заведующий, д-р социол. наук,
профессор О.Ю. Голуб

Саратов 2017

Актуальность исследуемой темы обусловлена тем, что с начала 2000 годов по настоящее время, государство ведет усиленную работу по обеспечению информационной безопасности личности в сети интернет.

В тех или иных масштабах актуальность проблемы информационной безопасности личности в Российской Федерации была и существует по сегодняшний день. На текущий момент данная проблема заслуживает особого подхода и изучения в связи с процессами интеграции и возможностью перемещения достаточных объемов информации через границы различных городов и государств. Информационные сети реализуют право граждан на обмен информацией, которое, в свою очередь, охраняется законами. Таким образом, обеспечение безопасности информации является одной из главных государственных задач. Для информационной безопасности личности в сети интернет у государства имеется необходимый комплекс мероприятий: законов, концепций, доктрин и иных ведомственных наставлений и положений. Однако, несмотря на богатую нормативную базу, существуют некоторые проблемы, которые необходимо решать.

В качестве **объекта** исследования выступают общественные отношения по исследуемой проблеме, которые возникают в связи с обеспечением информационной безопасности личности в Российской Федерации.

Предметом является информационное и гражданское законодательство Российской Федерации и зарубежных государств, а также отечественная доктрина информационного и гражданского права.

Целью магистерской работы является анализ информационной безопасности личности в сети интернет.

Для достижения поставленной цели разрешаются следующие **задачи**:

1. рассмотреть теоретико-правовые основы информационной безопасности личности в интернете;

2. раскрыть организационные особенности и проблемы системы информационной безопасности личности в интернете;

3. предложить решение текущих проблем.

Степень научной разработанности темы исследования. Данную проблему в своих научных трудах рассматривали следующие известные правоведы: Е.П. Бажанов, А.И. Горев, Р.И. Дремлюга, Е.А. Ерофеев, В.Н. Лопатин, И.Н. Панарин, А.А. Смирнов, В.П. Талимончик, Ю.С. Уфимцев, В.И. Ярочкин и другие. В работах перечисленных правоведов содержатся научно-обоснованные теоретические и практические тезисы. Однако определенные вопросы требуют дальнейшей научной выработки с учетом изменяющегося законодательства.

Методы. В магистерской работе для достижения основной цели, а также решения поставленных задач использовались такие методы научного познания: дедукция, синтез, универсальный диалектический метод, анализ сравнительно-правовой и исторический.

Научная апробация. Результаты исследования прошли апробацию и были доложены на 3 конференциях: 9 Международной научно-практической конференции: «Актуальные проблемы правового, социального и политического развития России» «21» апреля 2016 г.; 3 Всероссийской научно-практической конференции с международным участием: «Правовое регулирование медиакоммуникационной сферы в России: новое в законодательстве и проблемы правоприменения» «20» апреля 2016; 1 Международном фестивале науки «85 лет совершений и побед» СГЮА «18-20» апреля 2016 г., а также опубликованы в статье: «Некоторые особенности защиты персональных данных в сети интернет» (Сборник статей по материалам 9 международной научно-практической конференции студентов, магистрантов, аспирантов «Актуальные проблемы правового, социального и политического развития России», ISBN 978-5-91879-611-5).

Структура работы. Магистерская работа состоит из введения, двух глав, заключения и списка использованной литературы. В первой главе рассматриваются теоретико-правовые основы информационной безопасности личности в интернете. Вторая глава посвящена организационным особенностям и проблемам системы информационной безопасности.

Основное содержание работы

Глава 1 магистерской работы посвящена изучению теоретико-правовых основ информационной безопасности личности в интернете.

Общие вопросы гражданской безопасности сформировались с давних пор. В первобытном периоде человек самостоятельно противостоял различным жизненным угрозам. Однако в дальнейшем люди постигли очевидную истину: вопрос обеспечения безопасности - это задача целого сообщества, а не отдельных граждан.

Исторически сложились три уровня безопасности: государственный, общественный и личностный. В связи с процессами мировой интеграции на сегодняшний момент сформировался еще один уровень - международной всеобщей безопасности.

Сфера информационной безопасности является составной частью национальной безопасности. При этом в информационной сфере, представленную область гражданских правоотношений необходимо рассматривать на самостоятельном уровне, а также на уровне взаимодействия с социальными, экономическими, политическим процессами в стране и мире, которые не способны существовать вне информационной сферы деятельности.

Согласно правовой доктрине Российской Федерации «информационная безопасность - это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государств»[1].

Проблема отсутствия единообразного правового понятия «информационная безопасность» существует в международной практике, так

[1] Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

как у правоведов отсутствует единство во взглядах.

Автором были исследованы важнейшие нормативно-правовые акты, которые действуют в нашем государстве и зарубежом, с точки зрения их значения была дана правовая оценка.

Информационная безопасность в Российской Федерации регулируется правовыми актами национального законодательства и ратифицированными международно-правовыми актами. Выработанная государством нормативно-правовая база позволяет решить задачу обеспечения информационной безопасности личности в интернете.

В Российской Федерации существуют более 50 законов и множество инструкций и нормативных актов Правительства РФ и Президента РФ.

Согласно Конституции Российской Федерации[2] в нашей стране признаются и гарантируются основные права и свободы человека и гражданина. В том числе основным законом регламентируются информационные права: право свободно искать, получать, передавать, производить и распространять информацию любым законным способом; право на свободу слова и мысли; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений; право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, и другие права.

Для регулирования правоотношений, которые возникают: при применении в Российской Федерации информационных технологий; при реализации прав на получение, поиск, производство, передачу и распространение информации, а также при обеспечении защиты информации в 2006 году был разработан и принят Федеральный Закон «Об информации,

[2] Конституция Российской Федерации от 12 дек. 1993 г. (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ) // "Собрание законодательства РФ", 04.08.2014, N 31, ст. 4398.

информационных технологиях и защите информации»[3].

В целях ограничения детей от определенного вида специфичной информации в 2010 году был разработан и принят Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию»[4].

Также в целях реализации информационной безопасности личности в интернете был закреплен единый реестр запрещенных сайтов. Автором было выявлено отсутствие полного списка запрещенных сайтов, что является противоречащим принципам открытости и прозрачности.

В начале 2004 года вступил в силу Федеральный закон от 07.07.2003 № 126-ФЗ «О связи»[5], который призван урегулировать некоторые вопросы, в том числе по услуге в предоставлении свободного доступа к передаче данных, а также по предоставлению доступа к телекоммуникационному интерфейсу сети Интернет.

Вступивший в силу 9 апреля 1992 года Закон Российской Федерации «О защите прав потребителей»[6] аналогичным образом регулирует правоотношения, которые возникают при реализации товаров через интернет-сеть.

Гражданское законодательство Российской Федерации включает в себя правовые нормы относительно результатов интеллектуальной деятельности и интеллектуальных прав, которые защищены законом.

Уголовное законодательство Российской Федерации фиксирует санкции за преступления в компьютерной сфере, в том числе его нормы закрепляют ответственность за такой вид преступления как мошенничество, совершенное

---

[3] Об информации, информационных технологиях и защите информации: Федеральный закон от 27 июля 2006 г. (ред. от 06.07.2016) № 149-ФЗ // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

[4] О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29 декабря 2013 г. (ред. от 29.06.2015) № 436-ФЗ // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

[5] О связи: Федеральный закон от 07.07.2003 (ред. от 06.07.2016) № 126-ФЗ // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

[6] О защите прав потребителей: Закон Российской Федерации от 7 февраля 1992 г. (ред. от 03.07.2016 г.) № 2300-1 // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

при использовании компьютера.

Административное законодательство Российской Федерации закрепляет ответственность за нарушение правил обращения с информацией, в том числе в непредставлении информации по запросу в установленный срок.

Для достижения поставленной цели повышении эффективности взаимодействия информационных технологий, в том числе обеспечении информационной безопасности граждан 17 марта 2008 года был подписан Указ Президента Российской Федерации № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»[7], а также разработано и принято Постановление Правительства Российской Федерации «О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов»[8].

Немаловажный интерес вызывает принятая в 2016 году Доктрина информационной безопасности Российской Федерации[9], которая является важным документом, регулирующим информационную безопасность личности в интернете. В вышеуказанном документе содержатся основные тезисы относительно государственных интересов в информационной сфере, сформулированы внутренние и внешние источники угроз информационной безопасности, стратегические цели и способы организационного обеспечения информационной безопасности и т.д.

---

[7] О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента РФ от 17.03.2008 (ред. от 22.05.2015) № 351 // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

[8] О координации мероприятий по использованию информационно-коммуникационных технологий в деятельности государственных органов: Постановление Правительства РФ от 24.05.2010 г. (ред. от 05.05.2016) № 365 // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

[9] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 19.12.2016 г.

Стратегия развития информационного общества в Российской Федерации[10] была утверждена президентом Российской Федерации В.В. Путиным 7 февраля 2008 года. В указанной стратегии сформулированы: задачи и цели, основные направления национальной политики в сфере развития и использования информационных технологий, образования, науки и культуры для дальнейшего укрепления и продвижения России на пути развития и формирования информационного сообщества.

Автором были отмечены недостатки в законодательном закреплении некоторых правовых норм. Так за прошедшее время по настоящий момент принципиальных изменений в развитии правового обеспечения информационной безопасности в России не предпринималось. Также унифицированная законодательная система регулирующая вопросы информационной безопасности личности в интернете отсутствует.

Глава 2 магистерской работы посвящена исследованию организационных особенностей и проблем системы информационной безопасности личности в интернете.

Бурный научно-технический прорыв породил большое количество угроз безопасности в информационной сфере. Автором были выявлены следующие угрозы безопасности личности в интернете:

- распространение вредоносного программного обеспечения;
- кибератаки на государственные сайты, учреждения и предприятия;
- мошенничество;
- взлом почтовых сервисов и персональных банковских данных;
- распространение противоправной и потенциально опасной для граждан информации.

В качестве обеспечения информационной безопасности граждан в интернет-сфере автором предложен дополнительный комплекс мер:

- повышение уровня гражданской грамотности в вопросе

[10] Стратегия развития информационного общества в Российской Федерации: Приказ Президента РФ от 17.03.2008 № 351 (ред. от 22.05.2015) // [Электронный ресурс]. – Режим доступа: СПС КонсультантПлюс. – Дата обращения 11.09.2016 г.

информационной безопасности (использование антивирусов, фаэрволов, лицензионных программ, фильмов и музыки);

- установление правового режима для использования новых (разработанных) информационных технологий;

- усовершенствование имеющейся нормативной базы в сфере обеспечения безопасной передачи и обработки информации, а именно: поиск, анализ, сохранение, сбор, использование и распространение информации;

- обеспечение баланса интересов между защитой законных прав граждан и внедрением современных технологий обработки информации;

- усовершенствование алгоритмов обработки данных;

- осуществление обработки данных российскими серверами с использованием сетей связи российских операторов;

- государственная координация и регулирование информационных ресурсов созданных на территории Российской Федерации;

- усовершенствование оперативно-розыскных мероприятий направленных на расследование информационных преступлений.

Автором предлагаются следующие изменения в законопроект «О мерах по обеспечению информационной безопасности Российской Федерации»:

1. Замена действующего иностранного программного обеспечения на аналогичное по параметрам программное обеспечение российского производства на государственном и муниципальном уровне. Данное предложение повысит конкурентоспособность отечественного программного продукта, позволит сэкономить на государственных закупках, а также создаст качественно новый уровень защиты информационной безопасности;

2. Активное внедрение средств электронной цифровой подписи и доступное обеспечение системы аутентификации гражданина в сети интернет – данное предложение позволит обеспечить идентификацию и безопасность гражданина при подписании и подаче заявлений в государственные органы исполнительной власти через интернет-портал государственных услуг;

3. Разработка и создание системы сверхзашифрованного государственного «облачного» сервера, в котором хранятся личные данные граждан: свидетельства о рождении, заключении брака, смерти, паспортные данные, ИНН, СНИЛС, трудовая книжка и т.д. Данная инициатива улучшит взаимодействие граждан с государством, а также обеспечит безопасность граждан в части возможной фальсификации персональных документов со стороны третьих лиц;

4. Пропаганда безопасной информационной коммуникации в сети интернет. Вышеназванная мера заключается в обязательном «предустановленном» оснащении компьютеров и смартфонов бесплатным антивирусом и межсетевым экраном (файрвол или брандмауэр). Подобная инициатива позволит обезопасить все группы пользователей интернета от информационных преступлений.

5. Профилактика информационных преступлений. Управлению «К» МВД РФ и отделам «К» региональных управлений внутренних дел, входящих в состав Бюро специальных технических мероприятий МВД РФ, необходимо осуществлять профилактическую работу с обществом начиная с детских садов и школ. Подобная профилактика является важным элементом противодействия информационным преступлениям с участием представителей различных возрастных групп.

Предусмотренные меры ответственности за нарушение информационной безопасности в интернет-сфере должны быть одновременно реализованы на всех уровнях.

В Российской Федерации зафиксирована административная и уголовная ответственность виновных лиц за противозаконные деяния, которые совершаются в интернет среде. В целях успешного взаимодействия по розыску, изобличению и задержанию киберпреступников национальное уголовное законодательство нуждается в процессе унификации норм, так как подобные преступления часто носят трансграничный характер.

Заключение магистерской работы в целом отражает авторские выводы,

которые были сделаны в ходе всего выпускного исследования.

Осуществляя меры государственного контроля в Российской Федерации, необходимо соблюдать баланс между законными ограничениями, принимаемыми в целях безопасности информационной сферы, и правами и свободами человека и гражданина относительно свободного выражения своих мыслей.

В качестве перспектив развития правового регулирования информационной безопасности граждан в России следует отметить Доктрину информационной безопасности России 2016 г. , стратегию развития информационного общества в Российской Федерации, государственную программу информационное общество на 2011-2020 гг.

Доктриной предусмотрен комплекс мер, для дальнейшего противостояния перечисленным информационным угрозам. Обеспечение информационной безопасности государства осуществляется на основе сочетания правоохранительной, контрольной, судебной, правоприменительной, законодательной и других форм деятельности органов государства во взаимодействии с органами местного самоуправления, гражданами и организациями.

Целью представленных стратегий и программ является установление такой инфраструктуры, которая способна обеспечить защиту и информационную безопасность государству, гражданам и субъектам хозяйственной деятельности.

Преступления, связанные с нарушением закона в области информационной безопасности интернет сети, рассматривают национальные и международные судебные органы. Интерес для национальной судебной системы вызывают правовые позиции и аргументации судей Европейского суда по правам человека и гражданина, так как подобные правовые мнения учитываются судебной системой Российской Федерации при рассмотрении аналогичных дел.

Национальное законодательство в сфере борьбы с информационными

преступлениями несовершенно, так как не охватывает общий массив деяний, совершаемых в интернете. Текущие правовые нормы о компьютерных преступлениях сложно и редко применяются на практике, так как требуется законодательная доработка. На территории России противодействие преступлениям в области информационных технологий занимается Управление «К» МВД РФ, а также отделы «К» региональных управлений внутренних дел, которые входят в состав Бюро специальных технических мероприятий МВД РФ.

Существует административная и уголовная ответственность за правонарушения и преступления в информационной сфере.

Были выделены основные проблемы, влияющие на эффективность обеспечения информационной безопасности:

- распространение вредоносного программного обеспечения;
- кибератаки на государственные сайты, учреждения и предприятия;
- мошенничество;
- взлом почтовых сервисов и персональных банковских данных;
- распространение противоправной и потенциально опасной для граждан информации.

Предложены варианты решения выявленных проблем.