МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра конституционного и муниципального права

Обеспечение безопасности личности, общества и государства при применении информационных технологий

АВТОРЕФЕРАТ БАКАЛАВРСКОЙ РАБОТЫ

студента 512 группы
направления подготовки 40.03.01 «Юриспруденция»
юридического факультета

Кобы Никиты Владиславовича

Научный руководитель
доктор юрид. наук, доцент Куликова С.А.

Зав. кафедрой
доктор юрид. наук, профессор Комкова Г.Н.

Саратов 2022

Введение

Актуальность работы и обоснование ее выбора определены тем, что в условиях развития глобального информационного общества, открываются широкие возможности для интенсификации новейших вызовов и угроз, направленных на личность как уязвимый субъект информационных отношений, а также нарушения прав и интересов общества и государства в целом, что становится причиной обострения проблем национальной безопасности. Об актуальности обеспечения национальной безопасности России в информационной сфере свидетельствует утверждение Указом Президента России от 5 декабря 2016 года № 646 Доктрины информационной безопасности Российской Федерации (далее – Доктрина информационной безопасности) – системы официальных взглядов, определяющей национальные интересы как объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития. Масштабные преобразования в условиях развития информационно-телекоммуникационных технологий становятся причиной обострения проблем национальной безопасности, актуализируют современные тенденции реализации триады интересов личности, общества и государства при применении информационных технологий.

В условиях новых вызовов и угроз, трансграничности глобального информационного общества актуальность научных правовых проблем и выработка новых подходов к противодействию информационно-психологическому, деструктивному воздействию определяются значимыми задачами правового обеспечения информационной безопасности личности.

Все это обуславливает актуальность обеспечения безопасности личности, общества и государства при применении информационных технологий.

Объектом изучения являются регулируемые нормами права общественные отношения, возникающие и развивающиеся по поводу

обеспечения безопасности личности, общества и государства при применении информационных технологий.

Предметом изучения выступают нормы права, регламентирующие общественные отношения, возникающие и развивающиеся по поводу обеспечения безопасности личности, общества и государства при применении информационных технологий.

Цель работы состоит в разработке теоретического представления о сущности информационной безопасности личности, общества и государства, а также в анализе развития российского законодательства в сфере обеспечения безопасности личности, общества и государства при применении информационных технологий и обеспечения информационной безопасности личности, общества и государства в сети «Интернет».

Для достижения поставленной цели необходимо решить следующие **задачи**:

- изучить понятие информационной безопасности личности, общества и государства;

- проанализировать развитие российского законодательства в сфере обеспечения безопасности личности, общества и государства при применении информационных технологий;

- охарактеризовать обеспечение информационной безопасности личности в сети «Интернет»;

- изучить механизм ограничения доступа к распространяемой в сети «Интернет» информации, способной нанести вред обществу;

- рассмотреть государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы.

Основное содержание работы

Глава 1«Конституционно-правовые основы обеспечения безопасности личности, общества и государства при применении информационных технологий»включает в себя два параграфа.

В параграфе 1.1«Понятие информационной безопасности личности, общества и государства»рассмотрены конституционно-правовые основы обеспечения безопасности личности, общества и государства при применении информационных технологий.

Право на владение информацией выступает личным правом каждого человека, заключающееся в способности свободно воплощать в жизнь всевозможные операции, связанные с поиском, получением, созданием, распространением информации, без учета ее предназначения и содержания.

Информационная безопасность Российской Федерации — 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 государства

Существует несколько видов информационной безопасности.

Во-первых, информационная безопасность личности, которая характеризуется степенью ее защищенности. Данный вид информационной безопасности направлен на защиту личной информации человека от попыток вторжения, похищения, распространения и т. д.

Кроме того, существует информационная безопасность государства - защита конституционного строя, суверенитета; обеспечение законности и правопорядка. Обеспечение информационной безопасности государства неразрывно связано с обеспечением национальной безопасности.

Третьим видом является информационная безопасность общества - защита экономических, социальных, международных ценностей с использованием информационных средств от внешних и внутренних угроз. Она обеспечивается его защищенностью от вредных информационных воздействий в ходе информационной войны против страны.

Конституционная поправка п. «м» ст. 71 Конституции объективирована высокой степенью важности законодательной регламентации, а также масштабностью потенциальных угроз в сфере информационной безопасности.

Обеспечение безопасности при применении информационных технологий, обороте цифровых данных - самостоятельный правовой институт, который объединяет частную, общественную и публичную сферы. Он носит междисциплинарный характер и регулируется нормами международного, конституционного, административного, уголовного, информационного права.

Применение информационных технологий не должно создавать угрозу пренебрежения конституционными правами и свободами человека и гражданина, снижения уровня жизни и социально-экономического развития, суверенитету государства.

В целях реализации конституционных норм, Стратегия общественной безопасности должна быть дополнена новой угрозой - угроза безопасности общества в цифровой среде.

Современный этап развития нормативной базы в области обеспечения информационной безопасности характеризуется как минимум двумя обстоятельствами. С одной стороны, базовые основы для реализации конституционной нормы получили реальное воплощение в нормативных актах. Однако, очевидно, что действующее законодательство в области информационной безопасности отличается низкой систематизацией и декларативностью. Существенная часть отношений в сфере обеспечения безопасного применения информационных технологий регулируется

стратегиями, доктринами, которые хоть и являются системой официальных руководящих принципов, представлений государства, но выступают подзаконными нормативными актами.

В параграфе 1.2«Развитие российского законодательства в сфере обеспечения безопасности личности, общества и государства при применении информационных технологий» рассматривается конституционная реформа, ознаменованная внесением 206 поправок в Конституцию Российской Федерации и масштабным обновлением национального законодательства, коснулась большинства стратегических сфер государственной и общественной жизни. Одной из самых важных поправок стала статья 71 гл. 3 Конституция Российской Федерации. Новым предметом федерального ведения - «обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных.

Также был сделан вывод, что для цифровых технологий уже не существует границ, а мир превращается в глобально связанное информационное общество. Формирующаяся тенденция исторически значима, подтверждает, что вопросы безопасности обрели повышенную актуальность и требует серьезного внимания, ответственности государства.

В заключении данной главы рассматривается угроза опасности обществу в информационном пространстве пресекается в законодательстве об информационных технологиях. Так, Закон об информации устанавливает запрет на распространение информации, которая «оскорбляет общественную нравственность, выражается в явном неуважении к обществу» (п. 5 ч. 1 ст. 10.6, ч. 1 ст. 15.1).

В силу нашего представления о нравственности определенные признаки конструкции общественной нравственности можно увидеть в п. 22 Стратегии национальной безопасности, где идет речь о сохранении российской самобытности, культуры, традиционных российских духовно-нравственных ценностей и патриотическое воспитание граждан будут

способствовать дальнейшему развитию демократического устройства Российской Федерации и ее открытости миру.

Как указывает А.И. Овчинников, оскорбление общественной нравственности можно нанести не только весьма ограниченным кругом средств, но и многими другими (культурными провокациями, фотографиями, пародиями, высказываниями о ментальности народа). Разделяя мнение автора, следует добавить, что в сети нанести подобный вред гораздо быстрее и масштабнее.

Правовые установки Стратегии национальной безопасности и Доктрины информационной безопасности обозначают приоритеты в области безопасности государства и вытекающие из них потенциальные информационные угрозы.

Глава 2 «Обеспечение информационной безопасности личности, общества и государства в сети «Интернет»включает в себя три параграфа.

В параграфе 2.1 «Обеспечение информационной безопасности личности в сети «Интернет» принято считать, что отношения в сети Интернет всегда представляли и еще долго будут представлять проблему для законодателя. Сложность правового регулирования данных отношений определяется особенностью общественных отношений, складывающихся в виртуальной среде.

В первую очередь это определяется трансграничностью сети и невозможностью зачастую привязать события в сети Интернет к определенным географическим границам. Пользователь может легко оказаться на сайте, расположенном в другом городе, государстве или на другом континенте. Более того, как правило, пользователи даже и не имеют представления о том, где расположен тот или иной сайт. Такая возможность порождает множество правовых проблем: защиты личной информации о пользователе, защиты интеллектуальной собственности, регулирования содержания предоставляемой информационным посредником пользователю информации. Архитектура сети Интернет, а именно ее децентрализованный

характер, выражающийся в отсутствии единого центра, контролирующего все информационные процессы, происходящие в Интернете, является одной из основных причин невозможности их эффективного унифицированного правового регулирования.

Законодатель сталкивается с проблемой идентификации пользователей сети Интернет. Сам по себе IP-адрес, которым обладает каждое из устройств, подсоединенных к сети Интернет, позволяет лишь идентифицировать в сети Интернет такое устройство, но не позволяет произвести идентификацию лица, которое его использует.

В параграфе 2.2 «Механизмы ограничения доступа к распространяемой в сети «Интернет» информации, способной нанести вред обществу» рассматриваются причины и методы ограничения к информации, содержащих незаконные и опасные Интернет-ресурсы. Согласно ч. 6 ст. 10 Закона об информации в Российской Федерации запрещено распространять информацию, если:

1) она направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды;

2) за публичное оскорбление, в том числе в интернете;

3) незаконное распространение информации о несовершеннолетнем, пострадавшем в результате противоправных действий;

4)распространение заведомо недостоверной информации под видом достоверных сообщений об обстоятельствах, которые представляют угрозу жизни и безопасности граждан.

Существующий судебный порядок признания информации, запрещенной к распространению на территории Российской Федерации, затруднителен и неактуален, так как характеризуется длительностью его процедуры, перегрузкой судебной системы, неспособностью органов прокуратуры своевременно предотвращать размещение на вновь созданных интернет-страницах аналогичной противозаконной информации.

На основании изложенного, а также учитывая ее разноплановый и вредоносный характер, назрела необходимость вводить дополнительную ответственность за ее размещение, например, административную.

У административной ответственности необходимо привлекать не только инициаторов разработки таких интернет-страниц, но и технических посредников (провайдеры хостинга, операторы связи, администраторы доменных имен), роль которых заключается в предоставлении технических возможностей для размещения информации в сети Интернет. Далее после принятия решения о незаконности данной информации его копия направляется в Роскомнадзор. Затем следует процедура блокировки сайта. Роскомнадзор направляет запрос к провайдеру для того, чтобы со стороны хостинг провайдера был незамедлительно заблокирован запрещенный ресурс.

В параграфе 2.3«Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы» по итогам рассмотрения государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы отмечено, что модель построения ГосСОПКА призвана объединить специалистов реагирования и расследования компьютерных инцидентов в единое экспертное сообщество, обменивающегося обезличенной, но технически ценной информацией об угрозах безопасности. Это позволит эффективно реагировать на сложные и динамически развивающиеся атаки, предотвращать похожие атаки, эффективно координировать субъекты критической информационной инфраструктуры по вопросам информационной безопасности, в кратчайшие сроки ликвидировать последствия компьютерных инцидентов.

Заключение. В целом информационная безопасность Российской Федерации - 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 государства. Из этого определение видно, что составными части информационной безопасности страны является информационная безопасность личности, общества и государства.

В условиях цифровизации информационно-коммуникационной среды российского общества требуется установление баланса интересов личности, общества и государства в обеспечении информационной безопасности. Обеспечение персональной информационной безопасности, как составляющей политики национальной безопасности государства, общества и личности, должно осуществляться на основе следующих требований к балансу интересов: распределение ответственности, установлении равноправия интересов, определении целесообразности реализации интересов, соблюдении соразмерности интересов государства, общества и самой личности. Государственная информационная политика должна исходить из принципа соблюдения баланса интересов личности и государства и не выходить за пределы гарантированного конституцией права на неприкосновенность частной жизни.