МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

40.05.01 Правовое обеспечение национальной безопасности
(код и наименование направления подготовки / специальности)

Государственно-правовая
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему Правовая политика в сфере информационной безопасности

Обучающийся Е.А. Шевченко _____
(Инициалы Фамилия) (личная подпись)

Руководитель к.ю.н., доцент, А.А. Иванов
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Тема исследования «Правовая политика в сфере информационной безопасности».

Работа посвящена исследованию правовой политики в сфере информационной безопасности в российском государстве.

Актуальность исследования обуславливается тем обстоятельством, что государству необходимо пристально уделить внимание и направить все свои усилия в сторону предотвращения действий, которые направлены на возникновение и введение информационных войн против государства, которые дестабилизируют систему национальной безопасности. Для того, чтобы общество продолжало развиваться и стремительно прогрессировало, государству необходимо обеспечить кибербезопасность. Цель настоящей работы состоит в том, чтобы изучить теоретические основы, которые определяют место и роль государственного регулирования информационной безопасности Российской Федерации, определить проблемы в ходе осуществления государственного регулирования в этой сфере, определить пути решения выявленных проблем.

В соответствии с указанной целью были поставлены следующие задачи: изучить доктринальные основы информационной безопасности в современных условиях; проанализировать государственную политику в сфере информационной безопасности; проанализировать правовое регулирование информационной безопасности в Российской Федерации, а также в зарубежных странах; выявить и охарактеризовать органы государственной исполнительной власти в сфере информационной безопасности, а также методы государственного регулирования информационной безопасности.

Структурно работа состоит из введения, трех глав, включающих семь параграфов, заключения и списка используемой литературы и используемых источников.

Оглавление

Введение

Развитие личности, общества и государства в различные исторические периоды всегда проходило и проходит через стадию кризиса, проявляющегося в их разнообразных кризисах. В условиях развития компьютерных и информационно-телекоммуникационных технологий нахождение границы частного и публичного интересов становится с каждым разом все более затруднительным, особенно в свете недавно принятых законодательных мер противодействия терроризму и обеспечения общественной безопасности. Между тем кризис выступает не только орудием расшатывания сложившейся системы ценностей, в которой пребывает общество и человек, но переломным моментом в осмыслении того огромного значения, которое несет в себе неприкосновенность частной жизни для развития правосознания человека.

Обеспечение информационной безопасности является одним из центральных звеньев во внешней политике любого государства, всё это, безусловно, связано с глобальной информационной революцией. Одновременное развитие двух сфер – с одной стороны постоянный рост объема информации и его роли в жизни каждого, с другой стороны, постоянный процесс развития и совершенствования технологий накопления и распространений информации. Поэтому надёжная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для того чтобы обеспечить суверенитет государства.

Безусловно, ни одна сфера жизни на современном этапе развития общества не может функционировать без развитой информационной структуры. Именно, поэтому национальный информационный ресурс стал на сегодняшний момент одним из ключевых факторов, влияющих на все сферы, а основным из них является экономика, так как рост любого государства,

зависит от экономической составляющей, государство заинтересовано в тщательном регулирование данной сферы.

Государству необходимо пристально уделить внимание и направить все свои усилия в сторону предотвращения действий, которые направлены на возникновение и введение информационных войн против государства, которые дестабилизируют систему национальной безопасности. Для того, чтобы общество продолжало развиваться и стремительно прогрессировало, государству необходимо обеспечить кибербезопасность.

Проблемами государственного регулирования информационной безопасности в Российской Федерации занимались различные ученые, такие как: Ю.М. Батурин, О.А. Городов, И.Б. Григорьев, В.А. Копылов, В.Н. Лопатин, О.А. Степанов, А.А. Фатьянов, Д.Б Фролов, В.Д. Элькин. Также вызывают большой интерес, научно-исследовательские труды, следующих авторов: Х.А. Андриашин, Н.А. Антоненко, М.В. Ареева, Е.А. Артюшова, Р.М. Асланов, Ю.А. Белявская, Ю.В. Вовенда, С.А. Дементьев, В.М. Елин, А.Ю. Карась, А.А. Карцхия, Ю.В. Косов, Н.И. Костенко, Г.О. Крылов, Т.П. Кукса, В.М. Кулешов, Н.М. Курбатов, В.М. Лазарев, В.А. Мазуров, Р. Мардашина, А.С. Минзов, С.В. Михнева, И.П. Михнев, Н.В. Михайленко, И.О. Мельникова, Н.В. Морозов, А.А. Мурашкин, А.Э. Мысев, И.В. Плюгина, Е.А. Проценко, Д.Н. Садчикова, В.В. Середа, О.В. Столетов, А.В. Тарасенко, В.Н. Тихонов, Н.А. Трынченков, В.В. Филатов, Д.Н. Щедрин, А.Е. Любимов, А.А. Ефремов, Е.С. Зиновьева, А.П. Фисун, Д. Устинов.

Цель настоящей работы состоит в том, чтобы изучить теоретические основы, которые определяют место и роль государственного регулирования информационной безопасности Российской Федерации, определить проблемы в ходе осуществления государственного регулирования в этой сфере, определить пути решения выявленных проблем.

В соответствии с указанной целью были поставлены следующие задачи:

- изучить доктринальные основы информационной безопасности в современных условиях;
- проанализировать государственную политику в сфере информационной безопасности;
- проанализировать правовое регулирование информационной безопасности в Российской Федерации, а также в зарубежных странах;
- выявить и охарактеризовать органы государственной исполнительной власти в сфере информационной безопасности, а также методы государственного регулирования информационной безопасности.

Объектом исследования являются общественные отношения, которые возникают в процессе государственного регулирования информационной безопасности в Российской Федерации.

Предметом исследования являются нормативные акты и специальная литература, обеспечивающие государственное регулирование информационной безопасности в Российской Федерации.

В ходе работы применялись такие методы исследования как общенаучные, в частности, в данном случае можно выделить следующие методы: анализ, синтез, дедукция, индукция, системный и функциональный подходы, а также частно-научные методы, основными из которых были формально-юридический, сравнительно-правовой и социологический.

Теоретическую основу работы составили публикации таких ученых как Т.В. Александровой, Р.Ш. Закирова, А.К. Дубень, С.А. Куликовой и другие.

Нормативной и эмпирической основой работы являются Конституция Российской Федерации, Федеральные конституционные законы, Федеральные законы, подзаконные акты, постановления и определения Конституционного Суда Российской Федерации.

Новизна выпускной квалификационной работы состоит в том, что в ходе рассмотрения конституционных прав личности в их соотношении с

информационной безопасностью были выявлены проблемные аспекты как нормативно-правового регулирования обеспечения информационной безопасности, так и их практической реализации, в связи с чем, автором сформулированы предложения по устранению этих проблем.

Сфера информационной безопасности является весьма новым направлением в области обеспечения национальной безопасности государства, а само понятие национальной безопасности не является классическим для отечественной юриспруденции. Указанное обстоятельство обуславливает необходимость проведения соответствующих исследований, необходимость которых обусловлена в числе прочего и необходимостью обновлению и дополнению существующей юридической терминологии, внедрении новых дефиниций в юридический дискурс.

Теоретическая и практическая значимость выпускной квалификационной работы заключается в том, что основные положения и выводы исследования могут быть использованы в дальнейших научных исследованиях, а также в правотворческой деятельности по совершенствованию действующего законодательства, направленной на устранение выявленных в работе проблем.

Структура работы включает введение, три главы, разделенные на семь параграфов, заключение и список используемой литературы и используемых источников.

Глава 1 Доктринальные основы информационной безопасности в современных условиях

1.1 Понятие информационной безопасности

Информационная безопасность в XXI представляет собой большую значимость, учитывая тот факт, насколько быстро развиваются технологии обработки, хранения и передачи информации, применение информационных технологий. Происходят постоянные изменения, модификации, блокирование, копирование информационных ресурсов, которое приводит к нанесению ущерба не только отдельно взятому гражданину или организации, но и государству в целом.

Для того, чтобы дать полное определение «информационной безопасности», необходимо определится, что из себя представляет «информация» и «безопасность» как отдельные категории.

В научной литературе существует большое количество мнений о том, что же представляет собой понятие «информация». Так, согласно мнению А.А. Снытникова, «информация как благо нематериальное имеет множество разнообразных оттенков. В зависимости от тех или иных обстоятельств в повседневной жизни информация может быть актуальной и устаревшей, объективной и субъективной, основательной и безосновательной, многоплановой и однобокой, укрепляющей и компрометирующей и т.д.» [61, с. 22].

Достаточно интересное мнение у О.А. Городова, он считает, что «… информации только прагматика интересуется конкретными пользователями информационного продукта и той областью общественных отношений, участниками которых они выступают» [8, с. 19].

В словаре основных понятий книги, содержится следующее толкование информации.

Информация (в узком смысле) - это любые сведения об окружающем мире, которые человек получает с помощью органов чувств [14, с. 19].

Информация (в широком смысле) – это общенаучное понятие, включающее в себя обмен сведениями между людьми, обмен сигналами между живой и неживой природой, людьми и устройствами, между устройствами без участия человека [11, с. 42].

Информация - это сведения (сообщения, данные) независимо от формы их представления [29].

Теперь необходимо определится, что же собой представляет общее понятие «информационная безопасность». Так из Доктрины информационной безопасности Российской Федерации под ней понимается защищенность личности, общества и государства от информационных угроз извне и изнутри, обеспечивающее реализацию конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое социально-экономическое развитие Российской Федерации, оборону и безопасность государства.

Таким образом, под информационной безопасностью понимаются две составляющие:

В первую очередь, состояние (качество) определенного объекта (под объектом понимается, данные, информация, информационно-коммуникационные сети, ресурсы автоматизированных систем). Во вторую очередь, это деятельность, которая направлена на организацию обеспечения состояния защищенности объекта (в данную деятельность входят мероприятия правового, организационного, технического характера, которые направлены на предотвращение угроз информационной безопасности).

Но в научной литературе не сложилось единого взгляда на содержание понятия «информационная безопасность».

Понятие «информационная безопасность» тесно взаимосвязано с понятием «безопасность информации». Их достаточно часто используют в

качестве синонимов, но необходимо заметить, что существование «безопасности», без определения объекта понятия «безопасность» является неопределенным и бессмысленным (лишенном внутреннего смысла).

Понятие «информационная безопасность» приобретает тот или иной смысл в зависимости от объекта безопасности. В том случае, если объектом защиты будет выступать информация, то в таком случае, понятия «информационная безопасность» и «безопасность информации» будут выступать синонимами и их значение будет идентичное.

В том случае, если объектом будет выступать другой объект, например, участник информационных отношений, то в понятие «информационная безопасность» слово «информационная» указывает на направление деятельности, в таком случае трактуется как состояние защищенности данного объекта от угроз информационного характера.

В утратившем силу Федеральном законе Российской Федерации «Об участии в международном информационном обмене», под информационной безопасностью понимается состояние защищенности информационной среды общества, которая также обеспечивает формирование, использование и развитие в интересах граждан, организаций и государства».

В данном понятии защита информации и информационная инфраструктура является одним целым и представляет одно понятие «информационная безопасность». Важную сторону в этом понятии является техническая сторона [49, с. 289].

В последнее время, достаточно большое внимание уделяется к другому подходу, совершенно противоположному предшествующим определениям информационной безопасности.

Так, под информационной безопасностью понимается, защита от информации. Так одним из сторонников данного понимания определения «информационная безопасность» является С.П. Расторгуев, который высказывался по этому поводу следующим образом: «В результате проблема защиты информации, которая ранее была как никогда актуальна,

перевернулась подобно монете, что вызвало к жизни ее противоположность. Теперь уже саму информационную систему и, в первую очередь человека - необходимо защищать от поступающей «на вход» информации, потому что любая поступающая на вход самообучающейся системы информация неизбежно изменяет систему. Целенаправленное же деструктивное информационное воздействие может привести систему к необратимым изменениям и, при определенных условиях, к самоуничтожению» [59, с. 47].

Понятие «информационная безопасность» достаточно тесно взаимосвязано с понятием «безопасность информации» или «защита информации», они достаточно синонимичны. Но «безопасность» не может существовать сама по себе, безотносительно к объекту, «без внутреннего смысла» [62, с. 55].

Таким образом, учитывая всё вышесказанное информационная безопасность - это достаточно широкое понятие, которое включает в себя все, что взаимодействует с информацией. Было приведено достаточно большое количество понятии, которые содержатся, как в научной литературе, так и в некоторых правовых актах.

Но, достаточно большой интерес вызывает определение, данное А.И. Алексенцевым: «информационная безопасность - состояние информационной среды, обеспечивающее удовлетворение информационных потребностей субъектов информационных отношений, безопасность информации и защиты субъектов от негативного информационного воздействия» [2, с. 45].

В данном понятии, по нашему мнению, содержатся все необходимые признаки для характеристики информационной безопасности.

Можно прийти к выводу, что понятие информационной безопасности носит достаточно сложный: комплексный и системный характер, затрагивающий различные стороны отношений в обществе.

1.2 Государственная политика в сфере информационной безопасности

В России, как и в других государствах, наблюдается возрастание роли информационной сферы, увеличение значения информации как фактора жизни, непосредственно влияющие на национальную безопасность государства. Именно поэтому возникает потребность правовой оценки и регламентации информационных отношений.

Обеспечение информационной безопасности, как справедливо отмечает Р.Ш. Закиров, не может быть разовым мероприятием, а представляет собой непрерывный процесс, поддержание которого предполагает наличие соответствующего механизма [13, с. 38].

Обеспечивая информационную безопасность, государство предпринимает комплекс мер, включающих в себя выработку государственной политики в рассматриваемой сфере, на основе которой формируется законодательная база, регулирующая информационные отношения, определяются органы публичной власти, реализующие это законодательство и контролирующие его исполнение, разрабатывается система сертификации и лицензирования в области защиты информации, определяются приоритеты в разработки российских технологий по защите информации, обеспечивается повышение уровня информационной грамотности населения, предусматривается ответственность за нарушение законодательства в сфере информационной безопасности государства.

Государственная политика России в сфере информационной безопасности построена на основе соблюдения интересов личности, общества и государства в информационной сфере.

Государственная политика прежде всего определяет важнейшие направления деятельности федеральных органов государственной власти и органов государственной власти субъектов РФ в сфере обеспечения информационной безопасности, кроме того в нём закрепляется порядок

реализации их обязанностей, которые направлены на защиту интересов РФ в информационной среде.

Государственная политика в сфере безопасности информации отражается в Доктрине информационной безопасности Российской Федерации, развивающей положения Концепции национальной безопасности. Доктрина определяет национальные интересы России в информационной сфере, информационные угрозы, стратегические цели и направления, а также организационные основы обеспечения безопасности информации.

Данная доктрина содержит информацию не только обеспечивающую информационную безопасность в нашей стране на десятки лет вперед, но также в ней отражаются существующие недостатки мер, которые были предприняты в плане защиты информации ранее. В доктрине стало намного больше конкретики, а все те детерминанты, влияющие на ситуацию, которая связана с информационной безопасностью в России, охватили все сферы деятельности общества: кредитно-финансовую сферу, государственную и общественную безопасность.

Исходя из текста рассматриваемой Доктрины, можно сделать вывод о том, что главным направлением государственной политики в области информационной безопасности является защита государства от внешних (исходящих преимущественно от иностранных государств и террористических организаций) информационных угроз, обращенных к военно-промышленному комплексу, политическому устройству России, отношению граждан к действующей власти, а также кредитно-финансовому сектору.

На обеспечение государственной безопасности от внешних информационных угроз направлено ограничение деятельности СМИ с иностранным участием, которое Конституционный Суд признал не противоречащим Конституции Российской Федерации [55].

То, что основной упор в государственной политике России сделан на противостояние внешним угрозам, отчасти объясняет нежелание Российской Федерации присоединяться к Конвенции о преступности в сфере компьютерной информации, принятой в Будапеште 23 ноября 2001 года, так как Конвенция предусматривает сотрудничество спецслужб, подписавших ее государств по обмену информацией о киберпреступлениях, что, как считает Россия, несет угрозу ее государственному суверенитету.

Вместо этой Конвенции Российская Федерация предложила собственный вариант, усиливающий контроль каждым государством своего сегмента глобальной сети Интернет, что, по мнению стран развитой демократии (с чем можно полностью согласиться), во-первых, несовместимо с принципом свободы Интернета, во-вторых, в условиях глобализации и всеобщего проникновения информации неэффективно.

Одним из принципов обеспечения информационной безопасности России является законность, означающая, что весь механизм государственной безопасности в информационной сфере может работать только на основе норм права [25, с. 56].

Конституционно-правовое регулирование информационной безопасности в Российской Федерации показывает наличие большого объема законов и подзаконных актов в этой области. Но простого закрепления мер обеспечения информационной безопасности недостаточно. Необходима система претворения законов в жизнь, включающая деятельность органов публичной власти по реализации данного законодательства, контролю его исполнения и привлечения к ответственности нарушителей.

До настоящего времени основным концептуальным документом, определяющим политику Российской Федерации в информационной сфере, содержание национальных интересов и потребность государства в обеспечении их безопасности в настоящий момент является утвержденная Указом Президента от 9 мая 2019 г. № 203 новая Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы [45],

в которой были определены основные цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и телекоммуникационных технологий, направленных на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов.

В Стратегии предусмотрены следующие основные моменты для обеспечения безопасного и независимого функционирования сегмента сети Интернет:

- принять меры по обеспечения устойчивого функционирования российского сегмента сети Интернет;
- реализовывать государственную политику в части, касающейся государственного управления инфраструктурой российского сегмента сети Интернет;
- выработать технические и законодательные меры по предотвращению нарушений работы сети интернет и отдельных ее ресурсов на территории Российской Федерации в результате целенаправленных действий.

В современном мире киберпреступность достаточно острая проблема и борьба с ней не только становится одной из ключевых задач государства, но и даже приобретает мировой масштаб, так как атаки приобретают более глобальный характер. Она включает атаки на крупные корпорации, предприятия и государственные учреждения, данные атаки могут произойти, когда и где угодно. Поэтому для предотвращения данных атак недостаточно издание нормативных актов, которые направлены на борьбу с этими угрозами, но, а также инициатива должна исходить и от тех субъектов, кто заинтересован в защите информации. Только в этом случае нормативные акты, которые принимаются в государстве, а также на международном уровне будут приобретать какой-либо эффект.

Таким образом, всё вышеуказанное говорит о том, что государство активно ведёт работу, направленную на обеспечение информационной безопасности. И это положительный момент, так как развитие информационных технологий не остановится, изменения грядут во всех сферах жизни общества. Учитывая, что на сегодняшний момент активность пользователей сетью Интернет с каждым днём увеличивается, вопросы конфиденциальности пользователей, защита информации на пространства приобретает большое значение.

Государство, которое сможет правильно выстроить государственную политику для обеспечения информационной безопасности, сможет обеспечить достойную защиту прав граждан и предотвратить «информационную войну», сможет также добиться результатов не только в рамках обеспечения информационной безопасности, но и в рамках экономического развития государства, для формирования более развитого общества, обеспечив защищенное свободное информационное пространство.

1.3 Принципы и методы государственного регулирования информационной безопасности

Обеспечение информационной безопасности каждого государства требует, прежде всего, реализации некоторых задач. Когда государство определяет цели, задачи, принципы обеспечения информационной безопасности страны, это даст возможность для формирования определенных границ для достижения цели информационной безопасности и становится важным элементом данной системы.

Информационная безопасность должна является связующим звеном между политикой национальной безопасности и информационной безопасности, то есть важно проводить ее по единым принципам, общим и для национальной безопасности, и для информационной политики.

Определение базовых принципов в рамках государственного регулирования информационной безопасности является основополагающим началом, ввиду того что они способствуют развитию правовой системы государства, тем самым определяя основу правовой политики в сфере информационной безопасности.

Так, В.В. Лапаева в своей работе отмечает, что «в рамках такой трактовки правовой политики право представляет одновременно и как цель и как средство ее достижения» [53, с. 27].

А в свою очередь, В.С. Нерсесянц, утверждает следующее: «правовая политика – это государственная политика в области развития права (внутреннего и международного), стратегии и тактики правового пути развития общества, государства, страны, система идей, принципов, норм, форм и процедур признания, осуществления и развития начал и требований господства права в общественной и государственной жизни» [53, с. 23].

Если рассматривать принципы, непосредственно связанные с обеспечением информационной безопасности, с учётом представленных в Доктрине информационной безопасности РФ, а также с учетом выделенных принципов в учебной литературе, то можно указать на следующие основополагающие принципы информационной безопасности:

- принцип системности - основной, требующий учёта всех возможных угроз и рисков, хотя в полной мере учесть все невозможно. Поэтому необходимо абстрагирование от мелких деталей, но с учетом воздействия этих деталей на систему в целом;
- принцип комплексности предполагает согласование разнородных средств при построении целостной системы защиты, перекрывающей все каналы реализации угроз и не содержащий слабых мест на стыках ее компонентов;
- принцип непрерывности. Защита – непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла автоматизированных систем. Для

эффективного функционирования физических и технических средств защиты необходима постоянная организационная поддержка. Применение мер защиты – это, прежде всего, не разовое применение, а предполагает комплексное и непрерывное применение соответствующих мер;

- принцип разумной достаточности. Предполагает обеспечение лишь такого уровня информационной безопасности, при котором затраты, риск и размер возможного ущерба были бы приемлемы. Абсолютной защиты нет, или она стоит бесконечно много, либо система становится нефункциональной;
- принцип гибкости. Система создается в условиях неопределенности. Особенно важно, если защита устанавливается на уже работающую систему. Внешние условия постоянно меняются. Поскольку нельзя предвидеть будущее, необходимо иметь возможность относительно простого внесения изменений, настроек или дополнения новыми компонентами уже существующей системы защиты;
- принцип открытости механизмов и алгоритмов защиты. Защита не должна обеспечиваться исключительно за счет секретности структурной организации и алгоритмов функционирования. Знание алгоритмов и механизмов защиты не должно давать возможность ее преодоления. Но это не значит, что эта информация должна быть общедоступна;
- принцип простоты применения. Механизмы защиты должны быть понятны и просты в использовании. Не должно быть значительных дополнительных трудозатрат при обычной работе законных пользователей, должна быть минимизация дополнительных ручных операций. Чем проще и понятнее действия, тем меньше вероятность дополнительных действий, меньше желание уклониться от выполнения этих действий. Чем проще выполнение процедур

защиты, тем больше времени персонал сможет посвятить выполнению своих прямых обязанностей.

Также деятельность государственных органов по обеспечению информационной безопасности строится на основании принципов, указанных в Законе РФ «О безопасности», которые были переформулированы в основные принципы обеспечения безопасности. К таким принципам относятся: законность, соблюдение баланса жизненно важных интересов личности, общества и государства; взаимная ответственность личности, общества и государства по обеспечению безопасности; интеграция с международными системами безопасности.

Таким образом, под принципами, следует понимать, совокупность общих установлений, императивов, руководящих потенциалом для формирования такой модели информационных отношений, в рамках которой не будут нарушаться базовые и присущие конкретному обществу, его социокультурной программе информационные права и свободы. Инструментально принципы призваны решить проблему информационной агрессии, которая разрушает устои информационной безопасности человека. В целом можно отметить, что в совокупности таких принципов следует отнести принцип баланса информационных интересов как важную характеристику позитивной и неагрессивной информационной среды, принцип неуклонного соблюдения информационной свободы, принцип информационной ответственности и принцип социального информационного контроля.

Обеспечение информационной безопасности является одной из приоритетных задач государства. Целью защиты информационной инфраструктуры критически важных объектов сдержать кибератаку и не допустить несанкционированный доступ и т.п., при этом обеспечивается стабильная работа всей информационной инфраструктуры, что является гарантом безопасности России.

Важным направлением основного метода государственного регулирования в сфере информационной безопасности является правовое обеспечение. Нормативно-правовые акты регулируют вопросы обеспечения информационной безопасности, вопросы защиты информации, охраны государственной тайны, обеспечения защиты конфиденциальной информации, информационных ресурсов, направленные на реализацию положений Доктрины информационной безопасности. Политика информационной безопасности, а также безопасность информации в целом, разработаны с учетом методологии.

«Информационная безопасность и её составляющие рассматриваются сквозь призму функционального подхода в качестве объекта управления. Существующие концепции по видам опасностей, в том числе в информационной сфере, получили определенное нормативно-правовое закрепление в рамках парадигмы «безопасность является защитой от угроз»» [26, с. 131]. Эта парадигма нашла отражение в Стратегии национальной безопасности Российской Федерации [44].

На сегодняшний день пути, который выбрала Россия в рамках осуществления информационной безопасности, недостаточно эффективны, необходимо введение функционального подхода. На данный момент, когда осуществляется борьба в этой сфере, меры защиты вводит тот орган, в чьи компетенции это входит. Но следовало бы провести корректировку в составляющих защиту элементах и когда осуществляется информационная безопасность – борьбу с угрозами должны осуществлять органы совместно, сообща, ведь только в рамках совместной работы министерств, ведомств и других органов можно добиться национальной безопасности в этой сфере. Только в рамках функционального подхода можно установить взаимодействие всех министерств и ведомств, а также скоординировать их деятельность, обеспечив организационными, материально-техническими возможностями.

Т.М. Нинциева достаточно ярко выразилась по этому поводу в своей работе «Обеспечение информационной безопасности государства правовыми методами регулирования». Она утверждает, что «содержательную сущность информационной безопасности в упрощенном виде можно изложить как комплекс превентивных действий, направленных на обеспечение права на информацию и свободу информационной деятельности, на защиту информации и права собственности на информацию, на защиту от информации и от информационных воздействий. Методология формирования системы обеспечения информационной безопасности и практическое решение этих проблем свидетельствуют о том, что эффективность любой подсистемы будет напрямую зависеть от эффективного функционирования системы, в которую эта подсистема встроена. Иными словами, основой для совершенствования системы обеспечения информационной безопасности в процессе расширения межгосударственного сотрудничества должна быть эффективно действующая общая система обеспечения информационной безопасности как важная составляющая национальной безопасности РФ» [26, с. 131].

Следует также отметить, некоторых авторов, которые в своих работах предложили некоторые методы совершенствования защиты информации от различных угроз, для более лучшего достижения цели информационной безопасности.

В.Е. Новичков и И.Г. Пыхтин в работе «Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» проводят исследование «о необходимости введения уголовной ответственности за преступления в сфере информационной безопасности. Обосновывается необходимость таких мер, тем, что по данным статистики количество компьютерных преступлений в последние годы значительно возросло. Учитывая это, а также действующее законодательство Российской

Федерации, авторы делают выводы об актуальности и необходимости введения уголовной ответственности за данные правонарушения» [27, с. 27].

Г.А. Остапенко, Д.Г. Плотников, А.С. Рогозина в работе «Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов» рассматривают параметры функции риска для элементов критической информационной инфраструктуры на основе параметров рисков и их компонентов. Авторами предлагаются способы расчета риска для сложных многокомпонентных систем, учитывающих как синхронные, так и асинхронные атаки. «Предложенные формулы дают возможность оценки риска совместного и несовместного воздействия дестабилизирующих факторов, а также жизнестойкости системы, что, как следствие, позволяют адекватно классифицировать степень защищенности инфраструктуры и точнее прогнозировать ущерб от потери работоспособности данных объектов» [48, с. 361].

Для государства одним из важных методов воздействия на информационную безопасность является нормативно-правовое регулирование Российской Федерации в этой сфере. В текущих нормативных правовых актах существует некоторые проблемы, начиная от понимания определенных категорий до регулирования функционирования тех или иных органов. Учитывая это, государству следует усилить и продолжить совершенствовать правовое регулирование в области информационной безопасности, так как это его исключительная прерогатива.

В то же время, человек не может находиться в правовой неопределенности, не ведая какие именно деяния являются преступными, а какие нет. В данном контексте можно провести аналогию с презумпцией знания закона, согласно которой незнание закона не освобождает от ответственности. В соответствии с частью 3 статьи 15 Конституции Российской Федерации неопубликованные законы не подлежат применению. То есть все законы доводятся до всеобщего сведения, с тем, чтобы каждый

желающий мог ознакомиться с их содержанием и в случае нарушения закона не смог оправдаться незнанием его требований. В случае с государственной тайной, закон перечисляет только то, в какой области сведения могут быть засекречены, а какие не подлежат засекречиванию, но конкретные сведения, составляющие государственную тайну, не публикуются (иначе они перестанут быть тайной). Следовательно, человек не может знать того, что какая-либо конкретная информация является секретной. Такими знаниями обладают только лица, имеющие допуск к государственной тайне. По этой причине, все граждане, не имеющие соответствующего допуска, не могут привлекаться к уголовной ответственности за разглашение государственной тайны, даже если они действительно случайно стали ее носителями и разгласили. В таком случае ответственность должны нести должностные лица, ответственные за сохранность тайны, по чьей вине информация стала доступна третьим лицам, а не сами эти третьи лица.

Формулировка статьи 275 Уголовного кодекса Российской Федерации, помимо открытого перечня деяний, подпадающих под государственную измену, дающего правоприменителю возможность неоправданно широко трактовать эту статью (на что нами обращалось внимание во втором параграфе первой главы), не содержит различий по субъектам преступления [66]. То есть обвинение в государственной измене может быть предъявлено любому человеку, который даже не имеет доступа к государственной тайне. На практике это приводит к тому, что человек, не имея допуска к государственной тайне и не зная о том, что данная конкретная информация является секретной, разглашает ее, становясь при этом преступником, даже не подозревая об этом.

Таким образом, нормы статьи 275 Уголовного кодекса Российской Федерации содержат в себе существенные дефекты, как с точки зрения правового регулирования, так и с точки зрения государственно-правового механизма обеспечения информационной безопасности. В этой связи, нами предлагается внести изменения в статью 275 Уголовного кодекса Российской

Федерации, которыми должен определяться исчерпывающий перечень деяний, подпадающих под государственную измену вообще и под шпионаж в частности, путем изъятия таких формулировок как «в иных случаях» и «иной помощи». Также нами предлагается закрепить норму о том, что наказание за шпионаж и разглашение государственной тайны может распространяться только на лиц, имеющих соответствующий допуск к государственной тайне.

Помимо явного смещения законодательного регулирования и последующей правоприменительной практики с защиты прав человека в сторону обеспечения государственного интереса в области охраняемой законом тайны, имеет место проблема ограничений на распространение информации, не являющейся секретной. Закрепленная статьей 29 Конституции Российской Федерации свобода слова не является абсолютной, но ограничения этой свободы должны быть минимальны и только в той мере, в какой это необходимо для достижения конституционно значимых целей. Сама Конституция Российской Федерации, частью 2 статьи 29 запрещает пропаганду, разжигающую ненависть, вражду, языковое, национальное, религиозное или социальное превосходство. Такое ограничение обоснованно и соразмерно конституционным целям, так как направлено на сохранение общественного согласия и мира [24, с. 137]. Однако текущее законодательство неоправданно расширяет перечень высказываний, запрещенных под угрозой наказания.

В частности, статья 205.2 Уголовного кодекса Российской Федерации предусматривает наказание не только за призывы к террористической деятельности, но и за оправдание терроризма. Терроризм является одной из самых серьезных угроз современного мира и призывы к совершению терактов, несомненно, должны наказываться, так как они имеют побудительную направленность. Но оправдание терроризма, при всей морально-нравственной недопустимости, все же является оценочным суждением, отражающим личное отношение человека к тому или иному явлению, а не побуждающим к совершению преступления [51, с. 99].

Человек, разделяющий даже человеконенавистнические взгляды, но при этом никому не причиняющий вреда и не призывающий к насилию, с формально-юридической точки зрения не является преступником. Так, нельзя подвергать уголовному наказанию гражданина, оправдывающего красный или белый террор во время гражданской войны, либо сталинизм, унесший жизни миллионов людей. По этой причине для привлечения лица к ответственности, одного только оправдания чего-либо, без последующих призывов или действий недостаточно, в противном случае это вступает в противоречие с частью 3 статьи 29 Конституции Российской Федерации, согласно которой никто не может принуждаться к отказу от своих мнений и убеждений. То есть Конституция Российской Федерации проводит четкую границу между высказыванием мнения (которое не может подвергаться запрету) и призывами (которые, в силу их потенциальной опасности подлежат законодательному регулированию).

Кроме того, Российская Федерация подписала Конвенцию Совета Европы о предупреждении терроризма, которая, содержа понятие «подстрекательство к терроризму» не упоминает «оправдание терроризма» [18]. Подстрекательство по смыслу близко к призывам, но не к оправданию. Оправдание чего-либо, будучи оценочным суждением, является частью идеологии, которая, как справедливо указывает Л.Р. Гасанова, не обладает необходимой для уголовного законодательства определенностью [7, с. 129].

Терроризм во всех его проявлениях является злом, на борьбу с которым должны быть направлены все силы государства и общества. Однако, норма статьи 205.2 Уголовного кодекса Российской Федерации об оправдании терроризма, в том виде, в каком она есть сейчас, как показывает правоприменительная практика, не выполняет охранительную функцию, а напротив, может использоваться в отношении людей, вносящих вклад в борьбу с терроризмом. Так, летом 2020 года по части 2 статьи 205.2 Уголовного кодекса Российской Федерации была осуждена псковская журналистка Светлана Прокопьева, проанализировавшая в своей статье

причины подрыва террориста в архангельском УФСБ. Текст журналистской статьи по отношению к терроризму имел явно негативную коннотацию, но попытка анализа возможных мотивов действий террориста позволила следствию возбудить уголовное дело, а суду вынести обвинительный приговор.

Для недопущения подобного в будущем и исходя из вышеизложенного, нами предлагается заменить в статье 205.2 Уголовного кодекса Российской Федерации словосочетание «оправдание терроризма» на «пропаганда терроризма», что с одной стороны сохранит правовой механизм защиты от террористической угрозы, с другой стороны снимет противоречие с частью 3 статьи 29 Конституции Российской Федерации.

Схожая проблема и со статьей 354.1 Уголовного кодекса Российской Федерации, предусматривающей наказание за распространение ложных сведений о деятельности СССР в период Второй мировой войны. Помимо несовместимости с частью 3 статьи 29 Конституции Российской Федерации, данная норма Уголовного кодекса содержит потенциал принуждения к единомыслию, что противоречит частям 1 и 2 статьи 13 Конституции Российской Федерации. В данном случае, нами предлагается полностью изъять эту статью из Уголовного кодекса Российской Федерации, так как любое заблуждение человека (неосознанное или осознаваемое) не может быть уголовно наказуемо.

Таким образом, с точки зрения информационной безопасности, ограничению должно подвергаться распространение информации, которая побуждает к общественно опасным действиям, но запрет на высказывание собственного мнения и оценочных суждений (даже идущих в разрез с общепринятыми) выходит за конституционно очерченные рамки и является недопустимым.

Отметим, что государственно-правовой механизм обеспечения информационной безопасности должен сохранять разумный баланс между интересами государства и правом каждого на распространение информации.

Анализ действующего законодательства и практики его применения показывает, что отдельные законодательные нормы и основанные на них властные решения в некоторых случаях имеют вектор излишнего ограничения прав человека в пользу государственного интереса. Полагаем, что предложенные нами меры по совершенствованию действующего законодательства позволят устранить этот дисбаланс без ущерба государственной безопасности.

Стремительный прогресс современных технологий во всех сферах общественной жизни приводит ко все большей цифровизации общества, открывая для него новые, ранее недоступные возможности. Посредством сети Интернет граждане получают государственные услуги, осуществляют товарооборот, а информационные и коммуникационные технологии прочно укоренились в управленческих системах. Развитие телекоммуникационных сетей сделало Интернет основным источником информации для многих людей, вытесняющим из информационного пространства печатные и телевизионные СМИ. Появление мобильного Интернета позволило гражданам обмениваться информацией даже в отсутствие доступа к стационарному компьютеру.

Однако, цифровизация общества, помимо несомненных благ, таит в себе множество угроз и вызовов. Цифровые информационные технологии могут использоваться как инструмент негативного воздействия на людей, что обуславливает необходимость принятия мер по защите прав человека в информационной сфере, которая посредством развития телекоммуникационных сетей приобрела всеохватывающий характер [52, с. 168]. Можно согласиться с Т.А. Поляковой и И.С. Бойченко в том, что существующие в цифровом мире угрозы, объективно вынуждают государство формировать систему обеспечения безопасности граждан в этой области [54, с. 98].

Таким образом, в условиях глобальной цифровизации общества большое значение приобретает информационная безопасность граждан в

Интернет-пространстве. Вместе с тем, повышение уровня безопасности неизбежно влечет расширение ограничений и запретов, что, по мнению Н.Н. Ковалевой и О.Л. Солдаткиной, приводит к размыванию границы между ограничением на распространение информации и цензурой, а также возникновению технических и правовых проблем, связанных с блокировкой сайтов [16, с. 27]. При этом, некоторые авторы допускают введение цензуры, как необходимого инструмента обеспечения информационной безопасности личности [50, с. 103].

С последней точкой зрения мы не можем согласиться по следующим причинам. Как нами указывалось во втором параграфе первой главы, Конституция Российской Федерации частью 5 статьи 29 запрещает цензуру. Исходя из императивной формулировки конституционной нормы, не допускающей ее ограничительного толкования, можно сделать вывод об абсолютном запрете цензуры, при котором не может быть никаких исключений. Закон Российской Федерации «О средствах массовой информации» статьей 3 дает определение цензуры, под которой понимается обязанность СМИ согласовывать сообщения и иные материалы с органами власти и иными субъектами права, а равно запрет на публикацию тех или иных материалов. Верховный Суд Российской Федерации, в Постановлении от 2010 года № 16 подчеркнул неправомерный характер требования от редакций СМИ согласовывать с кем-либо выпускаемые материалы [56]. На недопустимость цензуры указал и Конституционный Суд Российской Федерации в сформулированной им правовой позиции, относительно этого вопроса [57].

Кроме того, право на распространение информации, закрепленное частью 4 статьи 29 Конституции Российской Федерации, согласно части 3 статьи 55 Конституции Российской Федерации может быть ограничено только федеральным законом и только для достижения конституционно значимых целей. То есть ограничение на распространение тех или иных материалов может устанавливать только законодатель, при условии, что эти

ограничения соразмерны конституционно значимым целям. Передача же полномочий по решению вопроса, что можно публиковать, а что нельзя цензору, имеющему собственные представления о безопасности информации, является недопустимой. Только закон, а не какое-либо должностное лицо вправе ограничивать распространение информации. По этой причине нами дифференцируются понятия «ограничение на распространение информации», возможное для обеспечения информационной безопасности и «цензура», являющаяся недопустимой.

Защищая права и свободы личности в информационной сфере, законодатель вводит ограничения на доступ к персональным данным в сети Интернет [63, с. 399]. Так, в 2015 году были внесены изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации», согласно которым по требованию гражданина операторы поисковых систем обязаны прекратить предоставление сведений о страницах сайтов, через которые возможен доступ к данным об этом гражданине, если они являются неактуальными, недостоверными или размещенными с нарушением закона. Исключение составляют сведения о совершенных гражданином преступлениях, по которым не истекли сроки давности [38]. Данное законоположение нами оценивается положительно, так как оно защищает человека от неограниченного по времени вторжения в его частную жизнь со стороны третьих лиц.

Развитие системы электронной почты актуализирует защиту прав личности на неприкосновенность переписки, осуществляемой посредством почтовых серверов. Тайна переписки, исходя из части 2 статьи 23 Конституции Российской Федерации, имеет ту же природу, что и тайна телефонных переговоров. Согласно Определению Конституционного Суда Российской Федерации, право на тайну телефонных переговоров включает в себя комплекс мер по защите информации, передаваемой по каналам связи, вне зависимости от ее полноты, содержания и времени передачи. При этом доступ к передаваемым сведениям возможен исключительно по судебному

решению [47]. Исходя из этой правовой позиции, а также единой конституционно-правовой природы тайны телефонных переговоров и тайны переписки, электронная почта гражданина должна обладать той же неприкосновенностью что и телефонная связь, так как защите подлежит тайна самих сообщений, независимо от того, каким способом эти сообщения передаются (по телефону или через электронную почту).

Таким образом, доступ к электронным сообщениям имеет только обладатель информации, которым, в соответствии с законодательством, является лицо, создавшее информацию, а также получившее в силу закона, либо договора право ограничивать или разрешать доступ к соответствующей информации. Законодательное определение понятия «обладатель информации», по нашему мнению, необходимо, так как оно позволяет очертить круг субъектов, обладающих правом распоряжаться информацией. Ведь наличие у конкретного лица доступа к информации еще не делает его обладателем этой информации в том смысле, в котором это позволило бы ему свободно распространять данную информацию.

Обладатели Интернет-сервиса, при помощи которого осуществляется передача электронных сообщений, оказывают услуги не по предоставлению доступа к сети Интернет, являющегося каналом связи, который предоставляет провайдер, а оказывают услуги по предоставлению возможности пользования программным обеспечением, позволяющим передавать электронные сообщения. Поскольку отсутствует специальное правовое регулирование, обязывающее обладателей соответствующего Интернет-сервиса обеспечивать тайну переписки, возникает неопределенность в вопросе наличия у него такой обязанности. С одной стороны, от субъекта права нельзя требовать выполнения обязанностей, не обусловленных законодательством. С другой стороны, услуги обладателей Интернет-сервисов, посредством которых осуществляется электронная переписка, аналогичны услугам операторов телефонной связи, на которых

пунктом 2 статьи 63 Федерального закона «О связи» возложена прямая обязанность обеспечить тайну телефонных переговоров [37].

Данная правовая неопределенность была снята Конституционным Судом Российской Федерации, который своим Постановлением от 26 октября 2017 г. указал, что в силу частей 1 и 2 статьи 15 Конституции Российской Федерации, часть 2 статьи 23 Конституции Российской Федерации, гарантирующая тайну переписки и телефонных переговоров, является нормой прямого действия, обязательной для всех субъектов права. Следовательно, отсутствие прямого законодательного обязывания обладателя Интернет-сервиса обеспечить тайну переписки не может расцениваться как отсутствие у него такой обязанности [58]. Таким образом, исходя из конституционного права каждого на тайну переписки, обладатель Интернет-сервиса, при помощи которого осуществляется передача электронных сообщений, не может иметь доступа к содержанию передаваемых через его ресурс электронным письмам.

Помимо положительных аспектов государственных мер по защите прав и свобод личности в информационной сфере, эти меры (прежде всего законодательные) имеют и ряд недостатков, связанных как с пробельностью, так и с чрезмерным правовым регулированием.

Пробелы права нами видятся в следующем. Доступ ко многим цифровым услугам сопровождается установкой соответствующих приложений, которая предваряется согласим гражданина с условиями пользовательского соглашения. В большинстве случаев условием такого соглашения является неограниченный доступ оператора к данным камеры устройства, контактов, галереи, местоположения и иным персональным данным, а также возможность передачи этих данных третьим лицам (как правило – рекламодателю). В соответствии с законами «О персональных данных» и «О связи» такие сведения являются информацией ограниченного доступа и без согласия абонента не могут передаваться третьим лицам.

Однако, гражданин, не желающий предоставлять доступ к этим данным, лишается возможности получения услуги, так как соответствующее приложение без требуемого согласия абонента не установится. Таким образом, операторы, по сути, вынуждают граждан соглашаться с передачей их персональных данных, формально не нарушая закон [6, с. 5]. Конечно, человека никто не заставляет устанавливать приложение, но находясь в цифровом обществе, он не может не пользоваться электронными устройствами, многие функции которых без приложений не поддерживаются. В этой связи необходимо законодательное регулирование данного вопроса, напрямую запрещающее операторам связи ставить предоставление услуги и установку соответствующего приложения в зависимость от согласия гражданина на доступ третьих лиц к его персональным данным.

Чрезмерное правовое регулирование в информационной сфере нами видится в неоправданном ограничении прав граждан на распространение информации в сети Интернет, подрывающем саму основу свободы Интернет-пространства. Так, Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» [40] при всей правильности своего названия содержит ряд норм, имеющих цензурную направленность. Закон содержит много расплывчатых и оценочных формулировок, таких как «побуждающие», «вызывающие страх», «способные вызвать» и др., что предоставляет правоприменителю неоправданную широту усмотрений при применении данного закона. Предусматриваемы законодательные ограничения на передачу информации в сети Интернет, распространяются на места, доступные для детей, следовательно, к таким местам могут относиться дома и квартиры, в которых живут дети со своими родителями. То есть, ограничительные меры охватывают практически все жизненное пространство людей, а значит, неизбежно касаются не только детей, но и взрослых [4, с. 143].

Так же, как справедливо отмечают В.М. Филиппов, В.В. Насонкин и Ч. Папачараламбоус, перечень видов информации, оборот которой может причинить вред несовершеннолетним, не отвечает потребностям настоящего дня [71, с. 368]. Все это позволяет в правоприменительной практике ограничивать распространение информации и доступ к ней не только в отношении детей, но и взрослых граждан, притом, что каждый совершеннолетний человек имеет право сам решать какая информация для него полезна, а какая вредна, в противном случае он лишается субъектности и, по сути, приравнивается к несовершеннолетнему.

Также в марте 2019 года был принят закон, предусматривающий ответственность за распространение в сети Интернет общественно значимой информации, которая является недостоверной [39]. Так, если в сети Интернет размещается недостоверная информация под видом достоверной, то может последовать ограничение доступа к сетевому изданию, распространившему такую информацию во внесудебном порядке. Согласно статье 15.1 Федерального закона «Об информации, информационных технологиях и о защите информации» на основании решения Роскомнадзора нежелательная информация включается в специальный реестр. Если речь идет о сведениях, касающихся чести, достоинства и деловой репутации, то основанием для включения в реестр является решение суда или пристава-исполнителя. После этого ограничивается доступ к сайтам, разместившим информацию, попавшую в данный реестр. Таким образом, Роскомнадзор, обладая правом признавать практически любую информацию нежелательной, посредством включения ее в соответствующий реестр, является органом, по сути, осуществляющим внесудебную блокировку сайтов. Такое полномочие Роскомнадзора делает его цензурирующим органом, решающим, какую информацию граждане могут получать, а к какой следует ограничить доступ, что несовместимо с конституционными принципами свободы получения и передачи информации, ограничение которой может осуществляться только законом или судебным решением. При этом, законодательное ограничение

распространения информации предполагает указание в законе конкретных сведений, подлежащих запрету, а не делегирование органу исполнительной власти права самому определять эти сведения.

Отметим, что недостоверная информация под видом достоверной является основой розыгрыша или пародии, суть которых как раз в том, чтобы выдать фейк за истину. Так, в Уссурийске снимаются и выкладываются в сети Интернет шуточные ролики про вымышленного чиновника Виталия Наливкина (являющегося собирательным образом), который «решает» проблемы горожан. Никакой общественной опасности эти ролики не представляют, но в соответствии с действующим законодательством они могут подпасть под запрет, что нами расценивается как несоразмерное конституционно значимым целям ограничение права на производство и распространение информации.

Все изложенное позволяет говорить о том, что в настоящее время в сфере регулирования информационной сферы в нашем государстве существуют проблемы разнообразного рода: связанные как с зарегулированностью соответствующих общественных отношений, так и с их недостаточным регулированием в настоящее время. Во многом это можно объяснить как «молодостью» отрасли информационного прав Российской Федерации, так и наличием множества нововведений в информационной сфере, возникновение которых обуславливается развитием технического прогресса и за чем законодатель часто по объективным причинам не успевает.

В завершении параграфа можем сделать следующие выводы. Нахождение человека в цифровом обществе помимо расширения возможностей влечет появление новых вызовов и угроз его информационной безопасности, что обуславливает необходимость принятия государственных мер по защите прав и свобод личности в информационной сфере.

Анализ действующего законодательства, регулирующего пользование телекоммуникационными сетями и практики его применения, показывает,

что они имеют как положительные, так и отрицательные стороны. Положительными сторонами является защита персональных данных, в том числе и посредством удаления данных о гражданине по его просьбе, а также распространение тайны сообщений на электронные письма.

Недостатками являются все еще существующие пробелы права, неоправданно широкий перечень сведений, распространение которых ограничено в сети Интернет и избыточная широта полномочий Роскомнадзора по внесудебной блокировке сайтов. Подобного рода широта полномочий организации, осуществляющей функции по контролю и надзору в сфере распространения информации, неоднозначным образом воспринимается в обществе, обуславливают наличие различного рода критических высказываний, разнообразных предложений по совершенствованию указанной сферы общественных отношений. Наличие данных недостатков свидетельствует о векторе государственной политике в сторону повышения информационной безопасности в ущерб свободе слова. Однако без свободы мысли и слова общественный прогресс становится невозможным и чем меньше у людей информационной свободы, тем медленнее происходит общественное развитие. В этой связи необходим поиск баланса между обеспечением безопасности и сохранением права на получение и распространение информации. Устранение выявленных нами недостатков правового регулирования обмена информацией в телекоммуникационной сети Интернет может поспособствовать установлению этого баланса.

Глава 2 Организационно-правовое обеспечение информационной безопасности

2.1 Правовое регулирование информационной безопасности в Российской Федерации

Информационная безопасность, будучи сложной и всеохватывающей категорией, непосредственно затрагивает права и свободы человека, так как обеспечение безопасности информации неизбежно сопряжено с определенным ограничением прав и свобод в сфере распространения информации. Для избегания произвола правоприменителя и недопущения избыточного ограничения права граждан на распространение информации необходимы законодательные пределы такого ограничения. В этой связи огромное значение приобретает правовое регулирование информационной безопасности.

Конституция Российской Федерации напрямую не закрепляет информационную безопасность, однако ряд ее норм непосредственно с ней связанны и составляют конституционно-правовую базу для текущего законодательства в этой области. Так, например статья 23 Конституция Российской Федерации закрепляет неприкосновенность частной жизни, включая тайну переписки, телефонных переговоров и иных сообщений. Важной гарантией информационной безопасности личности выступает положение о том, что ограничение этого права возможно только на основании решения суда. При этом суд не может давать разрешение на ограничение тайны переписки в отношении неопределенного круга лиц. Каждое, связанное с ограничением данного права дело, должно рассматриваться индивидуально. Статье 23 корреспондирует часть 1 статьи 24 Конституция Российской Федерации, запрещающая сбор, хранение и распространение информации о личной жизни человека без его согласия [21].

На основе этих конституционных положений получило развитие текущее законодательство в сфере неприкосновенности частной жизни. Так, Федеральный закон «О персональных данных» закрепляет основные принципы обработки персональных данных, согласно которым обработка персональных данных должна ограничиваться только конкретными целями, обрабатываемые данные не должны быть избыточными, а хранение данных должно быть ограничено по времени, в соответствии с целями обработки персональных данных [33].

Части 4 и 5 статьи 29 Конституции Российской Федерации закрепляют право каждого свободно искать, производить и распространять информацию, гарантируют свободу массовой информации и запрещают цензуру. Однако, свобода передачи информации не является абсолютной. В соответствии с частью 2 статьи 29 Конституция Российской Федерации запрещается агитация, возбуждающая религиозную, национальную, социальную и иную вражду. Также, по смыслу части 4 статьи 29 Конституция Российской Федерации определенные сведения могут составлять государственную тайну и как следствие исключаться из публичного оборота.

Базовым законом в этой сфере является Федеральный закон «Об информации, информационных технологиях и о защите информации». Данный закон содержит общие принципы регулирования правоотношений в области использования телекоммуникационных сетей, устанавливает основные способы защиты права на получение информации, а также защиты самой информации. В зависимости от формы доступа к определенным сведениям, информация делится на общедоступную и информацию ограниченного доступа. Большое внимание законодатель уделит порядку ограничения доступа к информации, распространяемой в сети Интернет [34].

Упомянутый нами в предыдущем параграфе Закон Российской Федерации «О государственной тайне» закрепляет перечень сведений, составляющих государственную тайну, а также сведений, которые не могут быть отнесены к государственной тайне, что направлено на предупреждение

произвольного засекречивания любых данных, влекущего нарушение конституционного права каждого на доступ к информации. При этом, засекречивание тех или иных сведений допустимо не только при условии их законодательного отнесения к перечню сведений, составляющих государственную тайну, но и при условии обоснованности такого засекречивания. Гарантией от волюнтаризма должностного лица, принимающего решение о засекречивании данных, является то, что определение обоснованности засекречивания не находится в его компетенции, а осуществляется посредством экспертной оценки целесообразности такого засекречивания на основе сохранения баланса прав граждан на информацию и интересов государственной безопасности.

Раскрывая положения части 5 статьи 29 Конституции Российской Федерации, Закон Российской Федерации «О средствах массовой информации» закрепляет запрет на злоупотребление свободой массовой информации, с одной стороны и недопустимость цензуры – с другой. Статья 3 этого закона дает легальную дефиницию понятия «цензура», под которой понимается обязанность редакций согласовывать с кем-либо материалы и сообщения, а также запрет на распространение этих материалов и сообщений [41]. Вместе с тем, пунктом 15 статьи 7 Федерального конституционного закона «О военном положении» закрепляется возможность введения военной цензуры за сообщениями и почтовыми отправлениями, контроль телефонных переговоров, а также создание органов цензуры [28]. Данное законоположение противоречит части 5 статьи 29 Конституции Российской Федерации запрещающей цензуру. Конституционная норма о запрете цензуры является императивной и не предусматривает каких-либо исключений из этого запрета. Соответственно, включение возможности введения цензуры в законодательство является неконституционным и нуждается в пересмотре.

Для правового регулирования информационной безопасности важное значение имеет закрепление ответственности за нарушение безопасности

информации и связанных с нею прав граждан и интересов государства. Конституция Российской Федерации не содержит и не может содержать норм, закрепляющих конкретные формы ответственности за нарушение информационной безопасности. Однако она предусматривает необходимость правового закрепления такой ответственности, отсылая к текущему законодательству. Так, часть 3 статьи 41 Конституции Российской Федерации содержит отсылочную норму, согласно которой сокрытие должностным лицом сведений, влияющих на безопасность граждан, влечет ответственность в соответствии с законом. В зависимости от тяжести и степени общественной опасности правонарушений в области информационной безопасности текущее законодательство предусматривает уголовную, административную и дисциплинарную ответственность.

Так, Уголовный кодекс Российской Федерации содержит ряд статей, предусматривающих наказание за нарушение тайны переписки (статья 138), отказ в предоставлении информации (статья 140), разглашение сведений, составляющих коммерческую тайну (статья 183), совершение государственной измены (статья 275), разглашение государственной тайны (статья 283) и др. Развитие цифровых технологий предопределяет необходимость закрепления ответственности в этой сфере отдельной главой Уголовного кодекса Российской Федерации. Глава 28 «Преступления в сфере компьютерной информации» предусматривает наказания за неправомерный доступ к компьютерной информации (статья 272), использование вирусных программ (статья 273), нарушение правил обработки компьютерной информации (статья 274), воздействие на информационную структуру государства (статья 274.1) [66].

Также Кодекс Российской Федерации об административных правонарушениях предусматривает административную ответственность за нарушение правил защиты информации (статья 13.12), незаконную деятельность в сфере защиты информации (статья 13.13), разглашение

сведений, имеющих ограниченный доступ (статья 13.14), воспрепятствование распространению информации (статья 13.16) и др. [17].

Если уголовная и административная ответственность распространяется на всех, то дисциплинарная ответственность в сфере информационной безопасности касается только тех субъектов права, которые находятся на службе и встроены в систему должностного подчинения. В зависимости от характера службы различаются и виды дисциплинарной ответственности, установленной различными законами. Так, нарушение информационной безопасности, ставшее следствием ненадлежащего исполнения должностных обязанностей государственным гражданским служащим влечет наложение дисциплинарной ответственности в соответствии с Федеральным законом «О государственной гражданской службе Российской Федерации» [34]. Дисциплинарный проступок в рассматриваемой сфере сотрудником полиции влечет привлечение к дисциплинарной ответственности в соответствии с Федеральным законом «О полиции» [35]. Аналогично этому дисциплинарная ответственность военнослужащих, прокурорских работников, сотрудников Росгвардии, Федеральной службы безопасности и иных служащих предусматривается специальными законами, регулирующими прохождение их службы [65, с. 104].

Закрепление словосочетаний «в иных случаях» и «иной помощи» делает перечень обстоятельств и деяний, подпадающих под государственную измену открытым, что позволяет правоприменителю произвольно включать в него практически любые действия подозреваемого, создавая для него правовую неопределенность в вопросе какие именно деяния могут стать основанием для привлечения к уголовной ответственности. На практике известно несколько уголовных дел, демонстрирующих несовершенство статьи 275 Уголовного кодекса Российской Федерации. Так, в 2015 году в отношении С.В. Давыдовой было возбуждено уголовное дело по статьи 275 Уголовного кодекса Российской Федерации за то, что она позвонила в посольство Украины и сообщила о переброске российских военнослужащих

на территорию Украины. Ввиду большого общественного резонанса, а также абсурдности обвинения, уголовное дело было закрыто, но формулировка закона, позволяющая возбуждать подобные уголовные дела, так и не была изменена, что сохранило почву для дальнейших обвинений в государственной измене, как ученых, поддерживающих международные контакты, так и лиц, даже не имеющих допуска к государственной тайне. Таким образом, объективная потребность обеспечения государственной безопасности, вытекающей из национальной безопасности не должна порождать правовую неопределенность для граждан, из чего следует необходимость корректировки рассматриваемых правовых норм.

Основные принципы обеспечения национальной безопасности российского общества и государства закреплены в ФЗ «О безопасности», согласно которому для обеспечения безопасности необходима системность и комплексность правовых, политических, организационных, информационных и других мер, на основе законности и соблюдения прав и свобод личности [30]. Регулируя вопросы безопасности в самом общем виде, этот закон выступает основой для принятия подзаконных актов, дающих более подробную регламентацию государственных мер по отдельным направлениям обеспечения безопасности [68, с. 173].

В исследуемой нами сфере принята Доктрина информационной безопасности, являющаяся актом стратегического планирования [43]. Доктрина информационной безопасности, будучи подзаконным актом, по своей важности не уступает законам, так как находится в основе формирования государственной политики в области информационной безопасности. Ориентируясь на эту Доктрину, законодатель принимает соответствующие законы, что делает необходимым более подробное рассмотрение положений самой Доктрины информационной безопасности.

В качестве основных информационных угроз Доктриной указываются использование информации для террористических, экстремистских, криминальных и других противозаконных целей, оказание зарубежными

странами информационно-технического воздействия на российские государственные органы и военно-промышленный комплекс, информационно-политическое вмешательство иностранных государств во внутренние дела России с целью дестабилизации политической и социальной ситуации, размывание российских традиционных нравственных ценностей, информационное воздействие на население с целью создания социальной напряженности, компьютерная преступность, преимущественно в финансовой области и др.

Основными направлениями сохранения информационной безопасности России, согласно рассматриваемой Доктрине, выступают развитие системы информационного противоборства в Вооруженных силах, прогнозирование и обнаружение информационных угроз, противостояние информационному воздействию, подрывающему патриотизм и исторические основы, развитие российских информационных технологий, развитие системы управления российским сегментом сети Интернет и др.

Реализация Доктрины в части сохранении информационной безопасности в России может наталкиваться на определенные трудности, вызванные разнонаправленностью правового регулирования этой сферы [69, с. 30]. С одной стороны, необходимость защиты информации порождает принятие законодательных ограничительных и запретительных мер, а также установление юридической ответственности за нарушение существующих ограничений и запретов. С другой стороны, развитие российских информационных технологий, являющееся одним из направлений сохранения информационной безопасности, возможно только в ситуации максимальной свободы, без которой творческое начало и инициатива людей угасают. Установление большого количества ограничений в информационной сфере создает препятствия для свободного обмена информацией (в том числе и с иностранными специалистами), креативного мышления, разработки и воплощения в жизнь творческих идей и внедрению новых технологий. Уголовное преследование ученых, обвиняемых в

государственной измене, наличие элементов цензуры, размытость законодательных формулировок, предусматривающих ответственность в сфере информационной безопасности, безусловно, тормозят развитие российских информационных технологий [15, с. 120]. По этой причине необходимо выявить баланс между ограничительными мерами государства (являющимися важной составляющей информационной безопасности) и конституционными правами и свободами граждан, которые важны не только как самоценность (что вытекает из статьи 2 Конституции Российской Федерации), но и как условие развития российских информационных технологий, которые тоже являются составляющей информационной безопасности России.

В завершении параграфа можем сделать следующие выводы. Будучи сложной категорией, информационная безопасность обуславливает наличие сложного многоуровневого конституционно-правового регулирования этой разновидности безопасности. В основе данного регулирования лежат нормы Конституции Российской Федерации о свободе поиска, производства, передачи и распространения информации, которая, однако, не является абсолютной. Раскрытие положений Конституции Российской Федерации осуществляется большим массивом федеральных законов, а также подзаконных актов, содержащих как регулятивные, так и охранительные нормы. Цифровизация многих сфер общественной жизни, по нашему мнению, делает развитие российских информационных технологий (которые могут развиваться только в условиях свободы) одной из важнейших составляющих сохранения информационной безопасности. По этой причине, поддержание максимальной свободы граждан в информационной сфере не только не противоречит информационной безопасности, но и является одним из условий ее сохранения.

2.2 Органы государственной исполнительной власти в сфере информационной безопасности

Когда в отношении России проявились международные санкционные меры со стороны других государств, это стало толчком для принятия определенных решений и проведения изменений в различных сферах: в здравоохранении, науки, транспорта, различных финансовых секторов и других областях, но ключевую роль занимает информационная безопасность.

В обеспечении информационной безопасности задействована вся система органов государственной власти, что обусловлено как всеохватывающим характером информационной среды, проникающей во все сферы социальной активности, подверженной правовому регулированию, так и необходимостью поддержания механизма сдержек и противовесов в самой власти.

На законодательном уровне контроль защиты информации обеспечивают комитет Государственной Думы по безопасности и противодействию коррупции, а также комитет Совета Федерации по обороне и безопасности. Кроме того, согласно Федеральному закону «О парламентском контроле» контрольные полномочия, в том числе и в области безопасности информации, принадлежат палатам Федерального Собрания, их иным комитетам и создаваемым палатами парламента специальным комиссиям [31]. На уровне исполнительной власти информационная безопасность обеспечивается Федеральной службой по техническому и экспортному контролю, Министерством обороны, Министерством внутренних дел, Федеральной службой безопасности, Федеральной службой охраны, Службой внешней разведки. Контроль и надзор за деятельностью средств массовой информации, а также в сфере массовых коммуникаций, информационных технологий и связи осуществляет Роскомнадзор.

Важную роль в обеспечении информационной безопасности играют суды, проверяющие законность и обоснованность действий субъектов

информационных отношений, а также назначающие наказания за нарушения законодательства в области безопасности информации.

Среди органов государственной власти с особым статусом следует отметить Прокуратуру, осуществляющую общий надзор за состоянием законности и Совет безопасности – конституционный совещательный орган, готовящий решения Президента Российской Федерации по вопросам безопасности (в том числе и информационной). Формирует и возглавляет Совет безопасности Президент Российской Федерации, который своим Указом утверждает Положение об этом органе [42].

Так как государственно-правовой механизм обеспечения информационной безопасности основывается на сочетании правотворческой, правоохранительной, правоприменительной, контрольной, судебной и иных форм деятельности органов власти, невозможно создание единого органа, сосредоточившего в себе все полномочия в области информационной защиты государства.

Таким образом, вся организационная система обеспечения информационной безопасности строится на основе разделения полномочий между разными органами государственной власти с учетом предметов ведения каждого из них.

Вместе с тем, исходя из выявленных нами приоритетов государственной политики в исследуемой сфере, главенствующее место занимает противостояние внешним угрозам, что существенно усиливает роль таких органов как Служба внешней разведки и Федеральная служба безопасности, следящие за сохранением государственной тайны и в частности, противостоящие шпионажу.

Во всех странах мира, включая и Россию, существуют подразделения, занимающиеся разведкой и противодействующие шпионажу (осуществляющие контрразведку). Как и в любом направлении деятельности по обеспечению информационной безопасности, разведывательная деятельность России имеет правовые основы, содержащиеся в Федеральном

законе «О внешней разведке» [32]. Подобные законы существуют и в других странах. То есть все государства официально признают за собой право осуществлять шпионскую деятельность в отношении других государств, но при этом борются со шпионажем в отношении себя. Такая дихотомия вызвана объективной невозможностью отказаться от разведки в одностороннем порядке, так как государство, не занимающееся шпионажем, становится более уязвимым по отношению к странам, продолжающим разведку, при том, что договориться всем о прекращении шпионажа априори невозможно. К тому же, такие государства как Саудовская Аравия, Северная Корея или Туркменистан, либо террористические образования, подобные Исламскому государству ни в какие соглашения входить не будут, а если и войдут, то с большой долей вероятности не станут их соблюдать. Необходимость шпионажа в отношении этих стран очевидна, так как она позволяет получать информацию о готовящихся в них терактах против других стран, о разработке запрещенных видов вооружения и иную информацию от которой зависит безопасность мирового сообщества.

Федеральный закон № 187-ФЗ от 01.01.2018 г. «О безопасности критической инфраструктуры» [36] увеличил полномочия федеральных органов власти. Так с произошедшими изменениями, которые были внесены вышеуказанным федеральным законом, в число полномочии ФСБ России дополнили следующими: создание и функционирование государственной системы обнаружения, предотвращения и ликвидации компьютерных атак и образование Национального координационного центра по компьютерным инцидентам, цель которого заключается в координировании мероприятий по реагированию на компьютерные инциденты и непосредственное участие в таких мероприятиях, организация и осуществление обмена информацией о компьютерных инцидентах между субъектами информационной безопасности, а также между субъектами и уполномоченными органами иностранных государств, международными организациями.

По сфере деятельности выделяют 2 группы федеральных органов, осуществляющие обеспечение информационной безопасности. Первый орган - это Федеральная служба безопасности (ФСБ), он осуществляет функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Второй орган - Федеральный орган по техническому и экспертному контролю (ФСТЭК) в его полномочия входит обеспечение безопасности критической информационной инфраструктуры.

Правовое положение Федерального органа по техническому и экспертному контролю предусматривает собой, то, что данный орган несет ответственность за ведение реестра объектов КИИ, а также осуществляет проверочную деятельность за правильностью категорирования объектов критической информационной инфраструктуры. В свою очередь, правовое положение ФСБ устанавливает полномочия данного органа, связанные с порядком реагирования на компьютерные инциденты, осуществляет разработку требований к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Государственное регулирование информационной безопасности осуществляется путем установления конкретных требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Так согласно, Федеральному закону РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» защита информации «представляет собой принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение

конфиденциальности информации ограниченного доступа; реализация права на доступ к информации» [29].

Проблема обеспечения информационной безопасности достаточно актуальна на сегодняшний день и активно развивается. Но мы не можем говорить о том, что современное состояние государственного и общественного обеспечения информационной безопасности на должном уровне, как и развитие информационных технологий. Анализируя тенденции изменения положений нормативно-правовых актов, можно выделить следующие направления деятельности государственного аппарата в информационной сфере. Так Президент РФ осуществляет разработку основ государственной политики в сфере информационной безопасности, в свою очередь органы законодательной власти определяют нормативную основу политики государства в этой сфере, законодательно закрепляют правовое положение основных субъектов критической информационной инфраструктуры, их права, обязанности и ответственность; а исполнительная власть определяет ключевые исполнительные органы, отвечающие за информационную безопасность, и обеспечивает непосредственно сам процесс защиты значимых объектов критической информационной инфраструктуры и ликвидации компьютерных атак.

Таким образом, можно прийти к выводу, что всем субъектам информационной инфраструктуры нужно провести массу продолжительных по времени мероприятий для того, чтобы создать эффективную системы безопасности. Создаваемые системы национальных органов в рамках осуществления информационной безопасности, организациям и должностным лицам, должны предъявляться требования: компетентности, независимости, беспристрастности.

Глава 3 Содержание государственного регулирования информационной безопасности

3.1 Правовое регулирование информационной безопасности в зарубежных странах

На мировой арене политика информационной безопасности в том или ином государстве, обеспечивается путем принятия стратегий кибербезопасности [70, с. 69] и других актов, а также основными законами страны [73, с. 134].

Следует рассмотреть несколько ведущих стран, которые выстраивают свою политику информационной безопасности.

Начнем подобное рассмотрение с Германии, как федеративного государства, чья правовая система имеет много общего с Российской Федерацией..

Законодательство об информационной безопасности Германии состоит из ряда актов, которые регламентируются отдельные аспекты защиты информационных интересов государства и общества. Основными из них являются: Федеральный закон «О вещательной деятельности (Телемедиа)», Федеральный Закон «Об охране персональных данных», Федеральный Закон «О порядке доступа к информации деятельности государственных органов и органов местного самоуправления», Федеральный Закон «О связи».

Согласно германской стратегии кибербезопасности на федеральное правительство возлагается принятие мер на основе созданных структур, которые соответствуют определенным уровням угроз по стратегическим направлениям, в число которых входит международное сотрудничество, эффективная борьба с преступностью в киберпространстве. Происходит стремительное усиление возможностей правоохранительных органов, Федеральной службы безопасности в сфере ИТ и экономики в контексте преодоления ИКТ- преступности.

В рамках Национальной стратегии кибербезопасности 2016 г. указывается, что «с учетом глобальных технологий, международное сотрудничество, сконцентрированное на аспектах международной политики и безопасности, носит обязательный характер» [74].

Следующей, рассматриваемой страной является Великобритания. Информационная политика Великобритании основана на технологической нейтральности законов; «активизация международного сотрудничества в сфере защиты информации; поддержка и защита интересов пользователей компьютерных и телекоммуникационных систем; развитие электронной коммерции во всех сферах хозяйствования; развитие автоматизированных систем обмена научно-технической информацией. Подобная ориентация политики ориентация политики информационной безопасности позволяет согласовать общегосударственный и местный уровни защиты интересов государства в информационной сфере, поскольку возрастает функциональность механизмов информационной безопасности» [70, с. 69].

Далее рассмотрим правовое регулирование информационной безопасности в США. Одной из самых первых стран, начавших осуществление стратегического планирования в сфере кибербезопасности, является Соединенные Штаты Америки. «Первая национальная доктринальная инициатива, которая определила необходимость координации различных ведомств государства в сфере национальной защиты информационного пространства, утвержденная в США в феврале 2003 г.» [22] International Strategy for cyberspace (Prosperity, Security and a Networked World) [75] (Международная стратегия по действиям в киберпространстве) которая раскрывает видение будущего киберпространства и план сотрудничества между странами и народами с целью его реализации.

International Strategy for cyberspace это документ, который определяет, что в США планируется противостояние тем, кто пытается разрушить сети и системы, также содержаться нормы о сдерживание злоумышленников, при

которых сохраняются важные информационные активы необходимыми и адекватными методами.

Основная сущность стратегии США заключается в том, что она призывает другие государства присоединится к ней, для того чтобы реализовать совместные цели, а именно реализовать идеи процветания, безопасности и открытости не только в США, но и во всем мире.

Большой интерес вызывает норма International Strategy for cyberspace обеспечивающая открытость и безопасность киберпространства и те средства, которые использует США для достижения своих целей.

Согласно этой норме США может применять для обеспечения безопасности не только экономические, дипломатические и информационные средства, но и также возможно вмешательство вооруженных сил США.

Кроме того, в законодательстве Соединенных Штатах Америки содержатся другие нормативно-правовые акты, регламентирующие правоотношения в сфере информационной безопасности [72, с. 62].

Одним из основных законов США в сфере информационной безопасности является закон Electronic Communications Privacy Act of 1986 (Электронный Закон о конфиденциальности электронных коммуникаций 1986 года, ECPA) [76]. Данный закон содержит три раздела. Первый раздел закона ECPA, включает в себя нормы, защищающие данные в процессе, а также устанавливает требования по производству обысков. Второй же раздел ECPA содержит в себе другой нормативный акт the Stored Communications Act of 1986 (Закон о хранении контактов), который целенаправлен на сохранение коммуникаций, базы информации, сообщений, находящиеся в компьютерах. Раздел третий ECPA включает в себя запрет на использования записей и регистрационных данных, устройства трассировки, маршрутизации, адресации и передачи сигнальной информации, без постановления суда.

Stored Communications Act of 19862 (Закон о хранении контактов (SCA)) о данном законе говорилось выше, SCA планирует добровольного

процедуру или раскрытия хранящихся проводных и электронных сообщений и транзакционных записей, являющиеся собственностью провайдеров интернетуслуг (ISP). SCA определяет возможности Правительства США по предупреждению к раскрытию информации, а также предусматривает две категории услуг:

– Electronic communication service (услуга электронной коммуникации);
– Remote computing service (дистанционное компьютерное обслуживание).

Также закон Stored Communications Act of 1986 регламентирует деятельность в тех случаях, когда электронные данные сохраняются за пределами границ, оказывающиеся под юрисдикцию США, в связи с тем, что многие Интернет-провайдеры имеют распространенные по всему миру центры и сервера обработки данных [67, с. 131].

Интересен факт применения закона SCA на практике. Так, рассматривалось дело Microsoft Corporation vs United States of America, в связи с тем, что государственные органы 4 декабря 2013 года получили ордер на розыск определенной учетной записи электронной почты, регулируемой и поддерживаемой Microsoft Corporation. Представитель Microsoft указал, что требуемое данные хранятся на сервере в Ирландии, в связи с чем Microsoft подала ходатайство об аннулировании ордера, в связи с его административно-территориальным применением. Однако ходатайство было отклонено судом и на основании SCA, предписание было объяснено как коллизия, которая выполняется как повестка в суд. Апелляционный суд 14 июля 2016 года второго округа США было вынесено решение в пользу Microsoft, поскольку положения SCA не могут использоваться экстерриториально [77].

Другой прецедент «Robbins vs. Lower Merion School District связан с тем, что в 2010 году средние школы Филадельфии шпионили за учащимися путем скрытной и удаленной активации веб-камер, встроенных в ноутбуки

учащихся школы, которые те использовали у себя дома, тем самым нарушалось право на частную жизнь учащихся. Школы признали виновными в осуществлении более 66000 вебшотов и скриншотов, в том числе в спальнях учащихся» [78].

Таким образом, рассмотренные страны имеют свои специфические особенности правового регулирования информационной безопасности. И каждая страна, рассмотренная выше достойна внимания, в каждой концепции правового регулирования информационной безопасности имеются положительные и отрицательные стороны. Можно прийти к выводу, что необходимо учесть опыт развития различных стран в данной сфере для недопущения ошибок, как в государственной политике, так и правовом регулирование информационной безопасности своей страны. Государство должно разрабатывать политику, направленную на обеспечении информационной безопасности, также издавать нормативно-правовые акты для ускорения совершенствования этой сферы.

3.2 Международно-правовое регулирование информационной безопасности

В соответствии с частью 4 статьи 15 Конституции Российской Федерации общепризнанные принципы и нормы международного права, а также международные договоры России являются не только неотъемлемой частью ее правовой системы, но и в иерархии нормативных правовых актов имеют более высокую юридическую силу, чем законы.

Важность приоритета международных договоров перед национальным законодательством обусловлена тем, что в России, как правовом демократическом государстве могут приниматься только правовые законы, то есть законы, не противоречащие основополагающим принципам, признаваемым мировым сообществом.

Если предположить принятие закона, отменяющего или умаляющего права человека, то он неизбежно вступит в противоречие с международным правом, закрепляющим фундаментальные права личности и, исходя из части 4 статьи 15 Конституции Российской Федерации, его положения не будут применяться. То есть приоритет международного права является важнейшей конституционной гарантией прав и свобод граждан, защищающей их от возможного произвола законодателя.

Кроме того, развитие телекоммуникационных сетей, связывающих весь мир в единое информационное пространство, на основе которых возникло глобальное мировое информационное сообщество, выводит проблемы информационной безопасности с национального уровня на международный. Россия является частью мирового сообщества, следовательно, угрозы и вызовы, существующие в глобальном мире, непосредственно касаются и нашей страны [64, с. 56].

Ввиду этих обстоятельств становится необходимым рассмотрение не только внутригосударственного, но и международно-правового закрепления информационной безопасности. При этом, полагаем, что следует заострить внимание не только на актах, направленных на обеспечение информационной безопасности, но и на неразрывно с ними связанных актах, способствующих расширению обмена информацией.

Одним из первых актов в рассматриваемой области была принятая в июле 1968 года Европейская конвенция об информации относительно иностранного законодательства, обязывающая государств-участников этой Конвенции сообщать о любых изменениях в своей правовой и судебной системе [12]. Конвенция не только повысила информированность подписавших ее государств о состоянии законодательства в каждом из них, но и существенно облегчила разрешение судебных споров с иностранным участием, сняв информационные препятствия для взаимной правовой помощи.

В январе 1981 года Совет Европы принял Конвенцию о защите физических лиц при автоматизированной обработке персональных данных [20], ставшую важной международной гарантией права каждого (вне зависимости от его гражданства и места жительства) на неприкосновенность частной жизни. Конвенция обязывает государства создавать системы, предотвращающие уничтожение или потерю данных о человеке, а также не допускающие противоправный доступ к ним. Согласно статье 8 Конвенции каждый имеет право знать о существовании касающихся его персональных данных файлов, целях их создания, получать доступ к ним, требовать их уничтожения, если данные файлы обрабатываются в нарушение закона [23, с. 198].

Россия ратифицировала эту Конвенцию в 2005 году, сделав оговорку о том, что может ограничивать право лица, чьи персональные данные собираются, на доступ к собираемым данным, если это продиктовано требованиями государственной безопасности. Полагаем, что такая оговорка не совместима с частью 2 статьи 24 Конституции Российской Федерации, так как ставит возможность получения человеком информации о самом себе в зависимость от усмотрения должностного лица, принимающего соответствующее решение от имени государства. При этом, каждый человек имеет право знать какую информацию о нем собирает государство и это знание априори не может подрывать государственную безопасность, в то время как сокрытие такой информации создает очевидные препятствия для защиты своих прав в случаях, к примеру, уголовного преследования этого человека.

В июне 2000 года была принята Окинавская Хартия глобального информационного общества [46], в развитие положений которой Генеральной Ассамблеей ООН был вынесен ряд резолюций, касающихся международной информационной безопасности. В декабре 2003 года на всемирном саммите на высшем уровне в Женеве была принята Декларация принципов [9], изложившая основополагающие принципы всемирного

информационного общества. На основе этих принципов в ноябре 2005 года была подписана Тунисская программа для информационного общества, сосредоточившая основное внимание на механизмах преодоления цифрового разрыва и управлении пользованием Интернетом.

Рассматривая возможность инкорпорации названных актов в российскую правовую систему С.И. Бочков, Г.И. Макаренко и А.В. Федичев отмечают, что саммиты Большой восьмерки (на которой принимались Окинавская Хартия, а также Женевские и Тунисские принципы) представляют собой клубы по интересам, декларации которых не представляют собой документы, имеющие важное значение с формально-юридической точки зрения [5, с. 7].

Можем не согласиться с таким заявлением, так как сам формат встреч глав государств предполагает достижение конструктивных договоренностей, имеющих смысл только в том случае, когда договаривающиеся стороны берут на себя обязательство по их выполнению. По этой причине разработанная в России Стратегия развития информационного общества на 2017-2030 годы пунктом 5 опирается на международные принципы, определенные Окинавской Хартией, Женевской Декларацией принципов и Планом действий Тунисского обязательства [45].

Если Окинавская Хартия практически не затрагивает вопросы пользования Интернетом, а Женевская Декларация принципов содержит декларативные нормы, то Тунисская программа для информационного общества, также называемая Планом действий Тунисского обязательства имеет ряд положений, реализация которых может оказать существенное влияние на развитие информационной среды и обеспечение ее безопасности в области телекоммуникационных технологий.

В частности, в Плане действий Тунисского обязательства подчеркивается, что Интернет является эффективным средством достижения мировой сплоченности, развития демократии, преодоления разрыва в информированности населения разных стран. Вместе с тем, Интернет-

технологии могут использоваться в противоправных целях, что указывает на важность недопущения злоупотребления информационными технологиями в преступных целях. Для преодоления цифрового разрыва правительства должны создавать государственные системы информации, развивать сети коллективного доступа к Интернету, а также вырабатывать стратегии долгосрочного хранения информации в цифровом виде.

Отметим, что, несмотря на имеющийся план действий, цифровое разделение между большими группами людей еще не преодолено. Можем согласиться с Т.Ю. Сидоровой в том, что, для преодоления цифрового разделения имеющегося Плана действий явно недостаточно и для решения проблемы необходимо дальнейшее правовое регулирование этого вопроса на основе общей стратегии международных институтов [60, с. 99]. При этом, цифровое неравенство имеет всеохватывающий характер и касается не только глобального мира, но и как отмечает ряд исследователей, отдельных регионов Российской Федерации [1, с. 10; 10, с. 109].

Развитие Интернета, открывая новые возможности для удаленных друг от друга контрагентов, с каждым годом увеличивает долю электронного способа коммуникации во всех сферах, включая и коммерческую. Однако неопределенность правового значения электронных сообщений при заключении международных коммерческих договоров, обусловила необходимость урегулирования этого вопроса, ввиду чего в ноябре 2005 года Генеральная Ассамблея ООН приняла Конвенцию об использовании электронных сообщений в международных договорах [19]. Россия присоединилась к этой Конвенции, но также как и в случае с Конвенцией о защите физических лиц при автоматизированной обработке персональных данных, с некоторыми оговорками. В частности, Россия отказывается применять Конвенцию в отношении сделок требующих государственную регистрацию, либо заключение которых требует нотариального удостоверения.

Как нами ранее упоминалось, международно-правовое закрепление расширения информационного обмена (прежде всего посредством компьютерных технологий) неразрывно связано с необходимостью обеспечения компьютерной безопасности. В этой связи следует отметить Конвенцию о преступности в сфере компьютерной информации, принятую в Будапеште 23 ноября 2001 года. В соответствии этой Конвенцией государства-участники обязуются на взаимной основе оказывать друг другу правовую помощь в расследовании преступлений, связанных с компьютерными технологиями. Также, страны, подписавшие Конвенцию должны принимать законодательные меры, направленные на недопущение противоправного доступа, перехвата, воздействия на данные, незаконного использования устройств, мошенничества с использованием компьютера, нарушения авторских прав. Не смотря на важность Конвенции для обеспечения информационной безопасности, Россия не является ее участником. Думается, что для повышения компьютерной безопасности внутри страны, приведения национального законодательства в соответствие с мировыми стандартами, а также укрепления мирового сотрудничества в этой сфере (что также повысит эффективность противостояния информационным угрозам), Россия должна присоединиться к данной Конвенции.

Чрезвычайная сложность обеспечения компьютерной безопасности (являющейся существенным сегментом информационной безопасности) обусловлена тем, что для предотвращения преступлений в компьютерной сфере невозможно установить тотальный государственный контроль Интернета и тем более отключиться от него. Развитие цифровой экономики (позволяющее совершать электронные транзакции на международном, государственном, корпоративном и бытовом уровнях), получение государственных услуг, обмен информацией и др., стали возможными только благодаря беспрецедентному развитию Интернета, которое в свою очередь, имеет в своей основе свободу, базирующуюся на анонимности, трансграничности и саморазвитии. Подавление свободы Интернет-

пространства неизбежно приведет к его деградации, что негативно скажется на всех сферах жизни общества (от затруднения банковских операций до сбоев в работе предприятий, транспорта и иных систем жизнеобеспечения). Для поддержания информационной безопасности необходим сбалансированный, признаваемый мировым сообществом подход к регулированию Интернет-пространства.

В 2011 году ООН приняла резолюцию, в которой подчеркивается приверженность максимальной свободе распространения информации в Интернете, за исключением случаев попыток несанкционированного доступа к данным. В 2016 году ООН своей резолюцией также подтвердила право каждого на свободу высказываний в Интернете, одновременно с этим осудив государства, осуществляющие слежку за гражданами и блокирующие сайты [3, с. 65].

Эти резолюции подтверждают тезис о невозможности противостояния информационным угрозам посредством подавления свободы, однако и решения проблем безопасности не предлагают. Еще в 2011 году Российская Федерация внесла в ООН проект Конвенции об обеспечении международной информационной безопасности вместо Будапештской Конвенции о преступности в сфере компьютерной информации от 2001 года, подписанной США, Японией, Австралией, Израилем и всеми членами Совета Европы кроме России. В российском варианте Конвенции предлагалось усиление государственного контроля над национальным сегментом Интернета, что оказалось несовместимым с принципом свободы распространения информации и стало причиной отклонения проекта этой Конвенции. В 2017 году Российская Федерация подготовила еще один проект Конвенции о сотрудничестве в сфере противодействия информационной преступности. Данный проект (концепция) был представлен странам БРИКС, но дальнейшего развития не получил.

Таким образом, анализ международно-правового закрепления информационной безопасности показывает, что, не смотря на наличие ряда

международных актов в исследуемой сфере, некоторые проблемы остаются неразрешенными. Особенно остро проблемы стоят в области Интернет-пространства, чье развитие опережает не успевающее за ним правовое регулирование. Отсутствие взаимопонимания между Россией и странами развитой демократии по вопросам борьбы с компьютерными преступлениями свидетельствует о разном понимании как ценности свободы информации, так и самой сущности Интернета и соответственно о допустимых способах противостояния Интернет-угрозам.

Вместе с тем, существующие международные акты в области информационной безопасности имеют большое значение для обеспечения данной безопасности внутри России. Информация и связанные с ней угрозы пронизывают все мировое пространство, включая и Российскую Федерацию, следовательно, отказ от мирового сотрудничества не снимает этих угроз, но лишает возможности пользования инструментами, предусмотренными международными актами. По этой причине нами вносится предложение по присоединению Российской Федерации к Будапештской Конвенции о преступности в сфере компьютерной информации от 2001 года. При этом, участие России в рассмотренных международных актах не только повышает эффективность ее противостояния глобальным информационным угрозам, но и налагает обязательство по приведению национального законодательства в соответствие с мировыми стандартами в области прав человека, что имеет ключевое значение для сохранения баланса между правами граждан и интересами государства.

Заключение

В заключение исследования можем сделать следующие обобщения и выводы.

Информационная безопасность является составной частью системы национальной безопасности Российской Федерации, имеет собственное содержание и представляет собой сложную, многоаспектную категорию.

Под информационной безопасностью понимаются две составляющие. В первую очередь, это состояние (качество) определенного объекта (под объектом понимается, данные, информация, информационно-коммуникационные сети, ресурсы автоматизированных систем). Во вторую очередь, это деятельность, которая направлена на организацию обеспечения состояния защищенности объекта (в данную деятельность входят мероприятия правового, организационного, технического характера, которые направлены на предотвращение угроз информационной безопасности).

Будучи сложной категорией, информационная безопасность обуславливает наличие сложного многоуровневого конституционно-правового регулирования этой безопасности. В основе данного регулирования лежат нормы Конституции Российской Федерации о свободе поиска, производства, передачи и распространения информации, которая, однако, не является абсолютной. Раскрытие положений Конституции Российской Федерации осуществляется большим массивом федеральных законов, а также подзаконных актов, содержащих как регулятивные, так и охранительные нормы. Цифровизация многих сфер общественной жизни, по нашему мнению, делает развитие российских информационных технологий (которые могут развиваться только в условиях свободы) одной из важнейших составляющих сохранения информационной безопасности. По этой причине, поддержание максимальной свободы граждан в информационной сфере не только не противоречит информационной безопасности, но и является одним из условий ее сохранения.

Анализ международно-правового закрепления информационной безопасности показывает, что, не смотря на наличие ряда международных актов в исследуемой сфере, некоторые проблемы остаются неразрешенными. Особенно остро проблемы стоят в области Интернет-пространства, чье развитие опережает не успевающее за ним правовое регулирование. Отсутствие взаимопонимания между Россией и странами развитой демократии по вопросам борьбы с компьютерными преступлениями свидетельствует о разном понимании как ценности свободы информации, так и самой сущности Интернета и соответственно о допустимых способах противостояния Интернет-угрозам.

Вместе с тем, существующие международные акты в области информационной безопасности имеют большое значение для обеспечения данной безопасности внутри России. Информация и связанные с ней угрозы пронизывают все мировое пространство, включая и Российскую Федерацию, следовательно, отказ от мирового сотрудничества не снимает этих угроз, но лишает возможности пользования инструментами, предусмотренными международными актами. По этой причине нами вносится предложение по присоединению Российской Федерации к Будапештской Конвенции о преступности в сфере компьютерной информации от 2001 года. При этом, участие России в рассмотренных международных актах не только повышает эффективность ее противостояния глобальным информационным угрозам, но и налагает обязательство по приведению национального законодательства в соответствие с мировыми стандартами в области прав человека, что имеет ключевое значение для сохранения баланса между правами граждан и интересами государства. Ведь конституционные права личности, в соответствии со статьей 2 Конституции Российской Федерации являются первичными по отношению к государственному интересу и их ограничение в целях обеспечения информационной безопасности допустимы только для достижения конституционно значимых целей, детерминированных правами других людей.

Ограничительные меры, обусловленные соображениями информационной безопасности государства, также должны иметь конечной целью защиту прав человека, ведь государство призвано обслуживать людей, следовательно, система государственной информационной безопасности необходима лишь постольку, поскольку она позволяет поддерживать институт государства в работоспособном состоянии, без чего государство не сможет эффективно защищать права личности.

Анализ действующего законодательства и правоприменительной практики показывает наличие как положительных моментов, так и ряда недостатков, выражающихся в том, что отдельные законодательные нормы и основанные на них властные решения в некоторых случаях имеют вектор излишнего ограничения прав человека в пользу государственного интереса.

Для устранения этих недостатков нами предлагается внести изменения в статью 275 Уголовного кодекса Российской Федерации, которыми должен определяться исчерпывающий перечень деяний, подпадающих под государственную измену вообще и под шпионаж в частности, путем изъятия таких формулировок как «в иных случаях» и «иной помощи». Кроме того, необходимо закрепить норму о том, что наказание за шпионаж и разглашение государственной тайны может распространяться только на лиц, имеющих соответствующий допуск к государственной тайне.

Также нами предлагается заменить в статье 205.2 Уголовного кодекса Российской Федерации словосочетание «оправдание терроризма» на «пропаганда терроризма», что с одной стороны сохранит правовой механизм защиты от террористической угрозы, с другой стороны снимет противоречие с частью 3 статьи 29 Конституции Российской Федерации.

Помимо этого нами предлагается внести изменения в Федеральный закон «Об информации, информационных технологиях и о защите информации» в части отмены ответственности за распространение в сети Интернет любой недостоверной информации (запретив только общественно опасную информацию) и лишения Роскомнадзора полномочия по

внесудебной блокировке сайтов, так как в случае выявления в сети Интернет вредоносной информации вопрос о блокировке сайтов, разместивших такую информацию должен решаться исключительно в суде.

Также необходимо дополнение законодательства нормами, напрямую запрещающими операторам связи ставить предоставление услуги и установку соответствующего приложения в зависимость от согласия гражданина на доступ третьих лиц к его персональным данным.

Полагаем, что предложенные нами меры по совершенствованию действующего законодательства позволят устранить дисбаланс между интересами государства по обеспечению безопасности через максимальный контроль информационной среды и конституционным правом личности на свободное получение и распространение информации без ущерба информационной безопасности.

Список используемой литературы и используемых источников

1. Александрова Т.В. Цифровое неравенство регионов России: причины, оценка, способы преодоления // Экономика и бизнес: теория и практика. 2019. № 8. С. 9-12.
2. Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. С. 44-47.
3. Арчаков В.Ю. Актуальные проблемы правового обеспечения международной информационной безопасности // Динамика институтов информационной безопасности. Правовые проблемы: сборник научных трудов. -М.: Изд-во «Канон+» РООИ «Реабилитация», 2018. С. 61-73.
4. Боброва В.В., Бобров Ф.А. Правовые проблемы обеспечения информационной безопасности несовершеннолетних // Наука, Мысль: электронный периодический журнал. 2016. № 12. С. 141-145.
5. Бочков С.И., Макаренко Г.И., Федичев А.В. Об Окинавской Хартии глобального информационного общества и задачах развития российских систем коммуникации // Правовая информатика, 2018. № 1. С. 4-13.
6. Брылева Е.А. Неприкосновенность частной жизни: частные и публичные интересы // Информационное право. 2018. № 4. С. 4-7.
7. Гасанова Л.Р. О некоторых вопросах соответствия ст. 205.1 УК РФ предписаниям Конвенции Совета Европы о предупреждении терроризма // Пробелы в российском законодательстве. 2015. № 3. С. 129-132.
8. Городов О.А. Информационного права России. Учебное пособие // СПб.: Юридический центр Пресс, 2003. 303 с.
9. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» от 10-12 декабря 2003 г. (Женева) // Библиотековедение, 2005. № 2. С. 80-89.

10. Добринская Д.Е., Мартыненко Т.С. Перспективы российского информационного общества: уровни цифрового разрыва // Вестник РУДН. 2019. № 1. С. 108-120.

11. Дубень А.К. Информационная безопасность как составная часть национальной безопасности Российской Федерации // The Scientific Heritage. 2021. № 74-4 (74). С. 41-45.

12. Европейская конвенция об информации относительно иностранного законодательства от 7 июня 1968 г. № 062 (Лондон) // Бюллетень международных договоров. № 1, январь 2000 г.

13. Закиров Р.Ш. Информационная безопасность: конспект лекций. Челябинск, Изд. ЮУрГУ, 2014. 73 с.

14. Информационная безопасность и защита информации: учеб. пособие для направления подготовки 40.03.01 – Юриспруденция, специальности 40.05.02 – Правоохранительная деятельность, специальности 37.05.02 – Психология служебной деятельности, очной и заочной форм обучения / О. А. Панфилова и др.; Федер. служба исполн. наказаний; Вологод. ин-т права и экономики. – Вологда: ВИПЭ ФСИН России, 2018. 59 с.

15. Кашапова Е.С. Некоторые аспекты уголовно-правовой политики противодействия преступности в сфере высоких технологий // Закон и право. 2018. № 9. С. 119-123.

16. Ковалева Н.Н., Солдаткина О.Л. Запреты в информационном праве // Информационное право. 2019. № 1. С. 26-30.

17. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации от 7 января 2002 г. № 1 (часть 1), ст. 1.

18. Конвенция Совета Европы о предупреждении терроризма от 16 мая 2005 г. (Варшава) // Собрание законодательства Российской Федерации от 18 мая 2009 г. № 20, ст. 2393.

19. Конвенция ООН об использовании электронных сообщений в международных договорах от 23 ноября 2005 г. (Нью-Йорк) // Бюллетень международных договоров № 6, июнь 2018 г.

20. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 г. (Страсбург) // Бюллетень международных договоров. № 4, апрель 2014 г.

21. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) Поправки, внесенные Законом РФ о поправке к Конституции РФ от 14.03.2020 № 1-ФКЗ, вступили в силу 4 июля 2020 года (Указ Президента РФ от 03.07.2020 № 445) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 04.07.2020.

22. Корсаков Г.Б. Информационное оружие супердержавы: кибервойна и «управляемые кризисы» // Военно-политическое образование [Электронный ресурс] http://www.belvpo.com/ru/10497.html (дата обращения: 26.07.2022).

23. Костенко Н.И. Право международной информационной безопасности (становление, тенденции и проблемы развития): монография - М.: Юрлитинформ, 2019. 464 с.

24. Куликова С.А. Конституционный запрет цензуры в России: монография под ред. Г.Н. Комковой. М.: Проспект, 2016. 256 с.

25. Морозов А.В. Полякова Т.А. Организационно-правовое обеспечение информационной безопасности: монография. М., 2013. 276 с.

26. Нинциева Т.М. Обеспечение информационной безопасности государства правовыми методами регулирования // В сборнике: Основные тенденции и принципы реализации положений Конституции Российской Федерации в различных отраслях правовой Российской Федерации Материалы 2 Международной научно-практической конференции, посвященной дню Конституции Российской Федерации. 2019. С. 129-134.

27. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 25-29.

28. О военном положении: Федеральный конституционный закон от 30 января 2002 г. № 1-ФКЗ (ред. от 01.07.2017) // Собрание законодательства Российской Федерации от 4 февраля 2002 г. N 5 ст. 375.

29. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ (ред. от 30.12.2021) // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448.

30. О безопасности: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ (ред. от 09.11.2020) // Собрание законодательства Российской Федерации от 3 января 2011 г. № 1, ст. 2

31. О парламентском контроле: Федеральный закон от 7 мая 2013 г. № 77-ФЗ (ред. от 14.03.2022) // Собрание законодательства Российской Федерации от 13 мая 2013 г. № 9, ст. 2304.

32. О внешней разведке: Федеральный закон от 10 января 1996 г. № 5-ФЗ (ред. от 09.11.2020) // Собрание законодательства Российской Федерации от 15 января 1996 г. № 3, ст. 143.

33. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3451.

34. О государственной гражданской службе Российской Федерации: Федеральный закон от 27 июля 2004 г. № 79-ФЗ (ред. от 30.12.2021) // Собрание законодательства Российской Федерации от 2 августа 2004 г. № 31, ст. 3215.

35. О полиции: Федеральный закон от 7 февраля 2011 г. № 3-ФЗ (ред. от 21.12.2021) // Собрание законодательства Российской Федерации от 14 февраля 2011 г. № 7, ст. 900

36. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ // Российская газета. 31 июля 2017. № 7333 (167).

37. О связи: Федеральный закон от 7 июля 2003 г. № 126-ФЗ (ред. от 14.07.2022) // Собрание законодательства Российской Федерации от 14 июля 2003 г. № 28, ст. 2895.

38. О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» и статьи 29 и 402 ГПК РФ: Федеральный закон от 13 июля 2015 г. № 264-ФЗ // Собрание законодательства Российской Федерации от 20 июля 2015 г. № 29 (часть 1), ст. 4390.

39. О внесении изменений в ст. 15.3 федерального закона «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 18 марта 2019 г. № 31-ФЗ // Собрание законодательства Российской Федерации от 25 марта 2019 г. № 12, ст. 1221

40. О защите детей от информации, причиняющей вред их здоровью и развитию: Федеральный закон от 29 декабря 2010 г. № 436-ФЗ (ред. от 01.07.2021) // Собрание законодательства Российской Федерации от 3 января 2011 г. № 1, ст. 48

41. О средствах массовой информации: Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 (ред. от 14.07.2022) // «Российская газета» от 8 февраля 1992 г. № 32.

42. О некоторых вопросах Совета Безопасности Российской Федерации: Указ Президента Российской Федерации от 7 марта 2020 г. № 175 // Собрание законодательства Российской Федерации от 9 марта 2020 г. № 10, ст. 1323.

43. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства Российской Федерации от 12 декабря 2016 г. № 50, ст. 7074.

44. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации от 5 июля 2021 г. N 27 (часть II) ст. 5351.

45. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: Указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации от 15 мая 2017 г. № 20, ст. 2901

46. Окинавская Хартия глобального информационного общества от 22 июня 2000 г. (Окинава) // «Дипломатический вестник» № 8, август 2000 г.

47. Определение Конституционного Суда Российской Федерации от 2 октября 2003 г. № 345-О «Об отказе в принятии к рассмотрению запроса Советского районного суда г. Липецка о проверке конституционности ч. 4 ст. 32 ФЗ «О связи» // Вестник Конституционного Суда Российской Федерации, 2004 г. № 1.

48. Остапенко Г.А., Плотников Д.Г., Рогозина А.С. Жизнестойкость элементов критической информационной инфраструктуры: аналитическая оценка с учетом возможных ущербов» // Информационная безопасность. Воронежский гос. техн. ун-т. 2013. № 3. С. 353-364.

49. Павлишин Б.И., Шевкуненко М.Ю., Инюкин А.Ф. Информационная безопасность как фактор обеспечения национальной безопасности России // В сборнике: Актуальные аспекты управления региональными экосистемами в условиях цифровизации экономики и общества: современные подходы и технологии. материалы международной научно-практической конференции. Кубанский государственный технологический университет. Краснодар, 2021. С. 288-292.

50. Паламарчук С.А. Цензура как один из методов обеспечения конституционной безопасности личности на примере «пакета Яровой» // Северо-Кавказский юридический вестник, 2017. № 4. С. 101-106.

51. Пашкин А.И. К вопросу о разграничении преступлений, предусмотренных ч. 1 ст. 205.1 и ст. 361 УК РФ // Альманах молодого исследователя. 2017. № 2. С. 97-100.

52. Погодин А.В., Путинцев А.В. Факторы-угрозы информационной безопасности в экстремальных трансформациях российской государственности в XX веке // Lex Russica. 2019. -№ 2. С. 163-175.

53. Полякова Т. А. Базовые принципы правового обеспечения инфор мационной безопасности // Труды института государства и права РАН. 2016. № 3 (55). С. 17-40.

54. Полякова Т.А. Информационная безопасность через призму национального проекта «цифровая экономика»: правовые проблемы и векторы решений // Право и государство. 2019. № 2. С. 97-100.

55. Постановление Конституционного Суда Российской Федерации от 17 января 2019 г. № 4-П «По делу о проверке конституционности ст. 19.1 Закона РФ «О средствах массовой информации» в связи с жалобой гражданина Е.Г. Финкельштейна» // Вестник Конституционного Суда Российской Федерации, 2019, № 2.

56. Постановление Пленума Верховного Суда Российской Федерации от 15 июня 2010 г. № 16 «О практике применения судами Закона РФ «О средствах массовой информации» (в ред. от 2012 г.) // Бюллетень Верховного Суда Российской Федерации, август 2010 г. № 8.

57. Постановление Конституционного Суда Российской Федерации от 9 июля 2013 г. № 18-П «По делу о проверке конституционности п.п. 1, 5 и 6 ст. 152 ГК РФ в связи с жалобой гражданина Е.В. Крылова» // Вестник Конституционного Суда Российской Федерации, 2013 г. № 6.

58. Постановление Конституционного Суда Российской Федерации от 26 октября 2017 г. № 25-П «По делу о проверке конституционности п. 5 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» в связи с жалобой гражданина А.И. Сушкова» // Вестник Конституционного Суда Российской Федерации, 2017 г. № 6.

59. Расторгуев С.П. Философия информационной войны / С.П. Расторгуев. М., 2016. 495 с.

60. Сидорова Т.Ю. Преодоление цифрового разделения: международно-правовые аспекты // Сибирский юридический вестник. 2019. № 3 (86). С. 98-102.

61. Снытников А.А. Обеспечение и защита прав на информацию. М. 2001. 338 с.

62. Стрельцов А.А. Обеспечение информационной безопасности России: теоретические и методологические основы / А.А. Стрельцов; под ред. В.А. Садовничего и В.П. Шерстюка; Московский гос. ун-т им. М. В. Ломоносова, Каф. информ. безопасности. - Москва: МЦНМО, 2002. 289 с.

63. Табаков А.Р. Организация защиты персональных данных в информационных системах Российской Федерации // Евразийский юридический журнал. 2018. № 12. С. 399-400.

64. Талапина Э.В. Государственный суверенитет в глобальном информационном обществе // Динамика институтов информационной безопасности. Правовые проблемы: сборник научных трудов. - М.: Изд-во «Канон+» РООИ «Реабилитация», 2018. С. 52-60.

65. Травников Н.О. Проблемы закрепления института служебной тайны в российской правовой системе // Российский юридический журнал. 2019. № 1. С. 103-109.

66. Уголовный кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. № 63-ФЗ (ред. от 25.03.2022) // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954.

67. Улин В.М. Сравнительный анализ правового обеспечения информационной безопасности в России и за рубежом. Монография // М.: 2016. 182 с.

68. Улыбашев А.Х. Межотраслевой баланс как инструмент обеспечения национальной безопасности // Современные проблемы

безопасности и правопорядка в России: сборник статей. - М.: Русайнс, 2018. С. 172-175.

69. Фатьянов А.А. Правовые проблемы отнесения сведений к государственной тайне в условиях модернизации экономики // Административное право и процесс. 2012. № 7. С. 29-32.

70. Филатов В.В. Зарубежный опыт правового регулирования информационной безопасности // Wschodnioeuropejskie Czasopismo Naukowe (East European Scientific Journal). 2018. № 3(31). С. 69-72.

71. Филиппов В.М., Насонкин В.В., Папачараламбоус Ч. Права и интересы детей в информационной сфере: реформирование законодательства // Вестник Санкт-Петербургского университета. Право, Вып. 2., 2019. С. 362-372.

72. Шамсутдинов Р.Р. Анализ правовой защиты информации в США // Евразийский юридический журнал. 2018. № 1. С. 61-63.

73. Щедрин Д.Н. Некоторые аспекты правового регулирования кибербезопасности на территории Российской Федерации и зарубежных стран // Инновационные тенденции развития российской науки. Часть II: матлы XII междунар. науч.- практ. конф. молод. учен. (8-9апреля 2019 г.) / Краснояр. гос. аграр. ун-т. Красноярск, 2019. С. 132-135.

74. Cyber-Sicherheitsstategie fur Deutsthland 2016 URL: https://www.bmi.bund.de/cybersicherheitsstrategie-/BMI_CyberSicherheitsStrategie.pdf (дата обращения: 01.08.2022).

75. International Strategy for cyberspace (Prosperity, Security and Openness in a Networked World [Электронный ресурс] URL: https:whitehouse.gov/sites/default/rss_viewer/international_strategy_for_cyberspace.pdf. (Дата обращения: 04.08.2022).

76. Electronic Communications Privacy Act of 1986 [Электронный ресурс] URL: https:law.comell.edu/uscode/text/18/2510. (Дата обращения: 04.08.2022).

77. Microsoft Corp. против Соединенных Штатов. – Microsoft Corp. v. United States. [Электронный ресурс] URL: https://ru.qwe.wiki/wiki/Microsoft_Corp._v._United_States (Дата обращения: 04.08.2022).

78. Robbins v. Lower Merion School District. [Электронный ресурс] URL: https://en.wikipedia.org/wiki/Robbins_v._Lower_Merion_School_District (Дата обращения: 04.08.2022).