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.В. Хвалина
(Инициалы Фамилия) (личная подпись)

Руководитель доктор юрид. наук., профессор Д.А. Липинский
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Тема исследования: «Правовая политика в сфере информационной безопасности».

Актуальность исследования правовой политики в сфере информационной безопасности обусловлена возрастающей ролью информационных технологий в жизни общества. Современный мир не может обойтись без различных электронных сервисов и онлайн-платформ, которые являются хранилищем большого количества данных о людях и компаниях.

Объектом исследования являются общественные отношения, касающиеся организационно-правовых механизмов обеспечения информационной безопасности РФ.

Объект исследования – государственная политика в сфере обеспечения информационной безопасности.

Цель настоящего исследования заключается в анализе организационно-правовых механизмов обеспечения информационной безопасности РФ, а также в выявлении проблем и путей решения в сфере совершенствования системы информационной безопасности.

Для достижения указанной цели при написании данной выпускной работы были поставлены следующие задачи: изучить понятие информационной безопасности; рассмотреть принципы и основные составляющие национальной безопасности Российской Федерации в информационной сфере; отразить правовое регулирование обеспечения информационной безопасности в Российской Федерации; выявить проблемные аспекты обеспечения информационной безопасности; предложить пути совершенствования системы информационной безопасности на современном этапе.

Цель, задачи и логика научного исследования определили структуру ее исследования, которая состоит из введения, трех глав из шести параграфов, заключения и списка используемой литературы и используемых источников.

Оглавление

Введение 4
Глава 1 Общая характеристика информационной безопасности 7
1.1 Понятие информационной безопасности 7
1.2 Принципы и основные составляющие национальной безопасности Российской Федерации в информационной сфере 12
Глава 2 Правовые аспекты обеспечения информационной безопасности в Российской Федерации 20
2.1 Правовое регулирование обеспечения информационной безопасности в Российской Федерации 20
Глава 3 Проблемы обеспечения и совершенствования системы 38
информационной безопасности 38
3.1 Проблемные аспекты обеспечения информационной безопасности 38
3.2 Совершенствование системы информационной безопасности на современном этапе 48
Заключение 63
Список используемой литературы и используемых источников 67

Введение

Актуальность темы исследования. Современный мир стал очень зависим от информационных технологий, что приводит к увеличению рисков для безопасности личных данных, интеллектуальной собственности, национальной безопасности и т.д. Поэтому правовая политика в сфере информационной безопасности является крайне важной для защиты интересов государства и его граждан. Кроме того, быстрое развитие информационных технологий требует постоянного обновления законодательства и адаптации его к новым вызовам и угрозам. Поэтому исследование правовой политики в сфере информационной безопасности является актуальным и необходимым для обеспечения эффективной защиты информационных ресурсов и борьбы с киберпреступностью.

Актуальность исследования правовой политики в сфере информационной безопасности обусловлена возрастающей ролью информационных технологий в жизни общества. Современный мир не может обойтись без различных электронных сервисов и онлайн-платформ, которые являются хранилищем большого количества данных о людях и компаниях.

Однако в условиях развития информационных технологий, возникает угроза нарушения прав на личную жизнь, интеллектуальную собственность, что может привести к кражам персональных данных, кибератакам, распространению компьютерных вирусов и другим опасным последствиям.

Правовая политика в сфере информационной безопасности является одним из способов защиты национальных интересов и прав граждан. Этот вопрос становится особенно критически важным в условиях мировой пандемии, когда большинство людей работает удаленно и использует различные онлайн-сервисы для общения, работы и учебы.

Исследование правовой политики в сфере информационной безопасности поможет принимать правильные решения в области законодательства, сокращения угрозы киберпреступностей и усиления

защиты персональных данных, а также поможет прогнозировать будущие тенденции в этой сфере и эффективно реагировать на возникающие проблемы.

Все вышеуказанное обуславливает актуальность исследования.

Степень изученности темы. Проблемы обеспечения информационной безопасности рассматриваются исследователями с различных ракурсов. Так, отечественные ученые, такие как Шушков Г. М., Сергеев И. В. в основном акцентируют внимание на информационной безопасности как на залоге стабильности в обществе, гармоничного развития личности, суверенитета государства на международной арене и во внутренних делах. Иначе говоря, в расчет берется именно психологическая составляющая вопроса и механизмы противодействия попыткам влияния на общественное сознание извне через дозированную подачу информации, ограничение доступа к информации, блокирование возможностей публикации информации либо искажение информации в целом.

Объектом исследования являются общественные отношения, касающиеся организационно-правовых механизмов обеспечения информационной безопасности РФ.

Объект исследования – государственная политика в сфере обеспечения информационной безопасности.

Цель настоящего исследования заключается в анализе организационно-правовых механизмов обеспечения информационной безопасности РФ, а также в выявлении проблем и путей решения в сфере совершенствования системы информационной безопасности.

Для достижения указанной цели при написании данной выпускной работы были поставлены следующие задачи:

- изучить понятие информационной безопасности;
- рассмотреть принципы и основные составляющие национальной безопасности Российской Федерации в информационной сфере;
- отразить правовое регулирование обеспечения информационной безопасности в Российской Федерации;

- выявить проблемные аспекты обеспечения информационной безопасности;
- предложить пути совершенствования системы информационной безопасности на современном этапе.

Нормативно-правовая база исследования. В ходе работы были изучены как национальные стратегические документы Российской Федерации (Доктрина информационной безопасности Российской Федерации, Стратегия национальной безопасности Российской Федерации).

Методологическую основу работы составляют общенаучные и частнонаучные методы познания объективной действительности: аналитический, диалектико-логический, конкретно-исторический, системный, сравнительно-правовой, формально-юридический и функциональный методы.

Теоретическую основу исследования составляют работы правоведов и труды следующих отечественных исследователей, специалистов в области права: Мазитов Р.Р., А.И. Поздняков, Невзоров Р.Г., Аксенов С.Г., Гришина В.В., Волчинская Е.К., Прокофьев К.В. И.Л. Бачило, М.М. Китайчик, Ю.А. Нисневич, и др.

Структура и объем работы. Цель, задачи и логика научного исследования определили структуру ее исследования, которая состоит из введения, трех глав из шести параграфов, заключения и списка используемой литературы и используемых источников.

Глава 1 Общая характеристика информационной безопасности

1.1 Понятие информационной безопасности

Для полного и правильного понимания правовых основ обеспечения информационной безопасности в Российской Федерации необходимо в первую очередь разобраться в том, какова же сущность и содержание информационной безопасности современного российского общества.

Толковый Словарь Русского Языка С. И. Ожегова и Н. Ю. Шведовой определяет значение слова безопасность, как состояние, при котором не угрожает опасность, есть защита от опасности. В свою очередь традиция определять безопасность как защищенность интересов заложена официальными документами США.

Но национальные интересы как ключевое понятие безопасности используется в США с явно идеологической целью - «прикрыть» активную и агрессивную реализацию национальных интересов по всему миру весьма респектабельной риторикой обеспечения национальной безопасности. В тоже время в существующих официальных документах и теоретических работах по проблематике обеспечения национальной безопасности (в том числе и по видам безопасности, в частности, по информационной безопасности) понятие национальной безопасности является, несомненно, ключевым. Для работы, понятие «национальной безопасности» является родовым, так как информационная безопасность является неотъемлемой её частью. В связи с этим необходимо остановится, на более глубоком изучении понятия национальная безопасность [16, с.24].

На сегодняшний день, в современной науке существую три наиболее распространенных подхода к определению понятия «национальная безопасность» [27, с.4]:

- бывший официальный: национальная безопасность определяется как защищенность национальных интересов от внутренних и внешних угроз (наиболее распространен);

– системно-философский: национальная безопасность определяется как состояние социальной системы (общества, страны), при котором она сохраняет свою целостность, устойчивость (стабильность), способность к эффективному функционированию и устойчивому развитию, а на их основе – возможность надежной защиты всех реальных и потенциальных элементов (подсистем, сфер, объектов) от любых деструктивных внутренних и внешних воздействий. В рамках данного подхода смысловой акцент делается на внутренние и внешние условия достижения такого состояния, т.е. на профилактику;
– аксиологический: национальная безопасность есть защищенность национального достояния, материальных и духовных ценностей страны (народа, нации) от получения значимого ущерба.

Наиболее часто, национальную безопасность определяют, как защищенность интересов личности, общества, государства от внутренних и внешних угроз. В данной работе логично будет, придерживается определения данного понятия в соответствии со «Стратегией национальной безопасности Российской Федерации», по которой «национальная безопасность» - это состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации (далее - граждане), достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации [37, с.29].

На этом этапе и закладывается одно из важнейших, на наш взгляд, противоречий, так как под «информационной безопасностью» обычно понимается защищенность национальных интересов в информационной сфере.

Однако, с точки зрения более глубокого логического осмысления, можно подвергнуть критике данные понятия поскольку, во-первых, в них

скрыта тавтология (поскольку понятия «угроза» и «опасность» очень близки по смыслу и получается, что безопасность определяется как защищенность от опасностей).

Во-вторых, трудно понять смысл и содержание словосочетаний «угрожать интересам», «защищать интересы». Ведь интересы как осознанные потребности, устремления людей следует не столько защищать, т.е. сохранять, сколько удовлетворять, снимать, реализовывать.

По мнению доктора философских наук В.И. Попова, в формулировании основных понятий теории национальной и информационной безопасности более корректен и более обоснован научно аксиологический (ценностный) подход. Аксиология – философское учение о природе ценностей, их месте и роли в обществе, человеческой деятельности [19, с. 34].

В результате проведенных научных исследований в этой области удалось прийти к следующим выводам.

Под безопасностью логичнее понимать защищенность от получения значимого ущерба. Достигается она тогда, когда величина (с учетом вероятности) возможного ущерба, который может нанести любой из существующих источников опасности, меньше уровня, начиная с которого требуется принятие мер по предотвращению, снижению ущерба. Основной критерий эффективности деятельности по обеспечению безопасности - величина предотвращенного ущерба. Снижать ущерб можно посредством уменьшения, как его величины, так и вероятности (риска) получения. А национальная безопасность есть, таким образом, защищенность национального достояния (материальных и духовных национальных ценностей, ресурсов) от любых видов значимого для страны и ее народа ущерба. Отсюда информационная безопасность – защищенность информации и информационных ресурсов, и их носителей, от попыток нанесения ущерба или уничтожения.

Получается, что, безопасность – это скорее не отсутствие опасности, а защита от нее. Она составляет одно из условий самоопределения, саморазвития личности, различных общностей, людей, человечества в целом.

Составными частями системы информационной безопасности являются: законодательная, нормативно- правовая и научная база; политики информационной безопасности; инженерно-технические решения и инструменты обеспечения информационной безопасности; программно-технические комплексы и средства защиты информации.

Опасности и угрозы всегда указывают на взаимодействие двух сторон: субъекта, который выступает источником опасности, и объекта, на который направлена опасность или угроза.

В самом общем смысле под угрозой понимается потенциально возможное событие, наносящее ущерб чьим-либо интересам. Источники опасности – это условия и факторы, которые проявляют или обнаруживают враждебные намерения, вредоносные свойства, деструктивную природу и по своей сути имеют естественно-природное, техническое и социальное происхождение.

Объектом угроз и опасностей являются личность, общество, государство. Эта триада представляет собой целостную систему. Личность в системе является высшей целью общественно-политического и социально-экономического развития страны.

Однако современное законодательство Российской Федерации, в частности Доктрина информационной безопасности Российской Федерации, трактует информационную безопасность, именно как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

В свою очередь, понятие информационной сферы в вышеуказанном нормативно-правовом акте рассматривается как – совокупность информации, объектов информатизации, информационных систем, сайтов в

информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений. Так как исследование носит правовой характер, все же придется руководствоваться официальной трактовкой данного понятия [15, с. 32].

Вследствие вышеуказанного, необходим более детальный подход к теории информационной безопасности, т.к. появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость в том, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных.

Так постепенно защита экономической информации становится обязательной:

- разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации;
- принят федеральный закон "Об информации, информационных технологиях и о защите информации», который рассматривает проблемы обеспечения информационной безопасности и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Информационная безопасность для российской правовой системы является достаточно устоявшейся категорией, вместе с тем взгляды на ее сущность продолжают изменяться и сегодня. Безусловно, знаковым событием в данной сфере стало принятие Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646 [28].

В Доктрине приведено определение информационной безопасности Российской Федерации, под которой понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Под информационной безопасностью понимается защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.

1.2 Принципы и основные составляющие национальной безопасности Российской Федерации в информационной сфере

В сравнении с прошлым периодом становления российской внешнеполитической доктрины, сориентированной на информационный фактор, как инструмент глобализации, без которого невозможна нормальная интеграция в мировое сообщество, на текущем этапе развития России, безусловно ясно, что в условиях введения ограничительных мер в отношении нашего государства, необходимо выстраивать принципиально другое отношении к использованию информационных возможностей, как единственного инструмента способного противостоять внешним угрозам и рискам. При этом особое внимание, несомненно должно быть акцентировано на становлении такого важного направления, как информационная безопасность, в том числе развития соответствующей нормативно-правовой базы по данному вопросу.

Доктриной информационной безопасности закреплено, что информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Государственная политика РФ в сфере информационной безопасности осуществляется согласованными действиями всех участников системы обеспечения государственной безопасности, которую координирует Совет Безопасности Российской Федерации благодаря реализации организационных, нормативно-правовых и информационных мероприятий. При Совбезе создана межведомственная комиссия по информационной безопасности. В состав комиссии входят специалисты-представители из различных федеральных органов исполнительной и государственной власти, силовых структур.

Основная задача комиссии - анализ состояния информационной безопасности, прогнозирование и оценка угроз, далее - выработка предложений и рекомендаций Совету Безопасности по реализации государственной политики в данной области

Обеспечение безопасности в различных сферах, в том числе и информационной, является одной из значимых составляющих существования субъекта правовых отношений.

В Российской Федерации одним из первых был принят закон «О безопасности», которым определено понятие безопасность – состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз. Жизненно важными интересами являются потребности, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития как общества и государства, так и личности.

К основным объектам безопасности относятся:

- для личности – это ее права и свободы; для общества – его материальные и духовные ценности;
- для государства – его конституционный строй, суверенитет и территориальная целостность.

Именно государство является основным субъектом обеспечения безопасности, оно осуществляет функции в этой области через органы законодательной, исполнительной и судебной властей. Угроза представляет собой совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства.

Основными принципами обеспечения безопасности (в том числе информационной) являются:

- законность;
- соблюдение баланса жизненно важных интересов личности, общества и государства;
- взаимная ответственность личности, общества и государства по обеспечению безопасности;
- интеграция с международными системами безопасности.

Систему безопасности образуют органы законодательной, исполнительной и судебной властей, государственные, общественные и иные организации и объединения, граждане, принимающие участие в обеспечении безопасности в соответствии с законом, а также законодательство, регламентирующее отношения в сфере безопасности. Общее руководство государственными органами обеспечения безопасности осуществляет Президент Российской Федерации, который возглавляет специально организованный для этого орган – Совет безопасности Российской Федерации. Совет безопасности РФ рассматривает различные вопросы, в том числе и информационной безопасности.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность

информации, информационной инфраструктуры, субъектов, осуществляющих оборот информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной, социальной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет только возрастать.

Так как, в современной нормативной базе, под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства, необходимо определить само понятие «интересы».

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере заключаются в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении России.

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития российской информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и

правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере [36, с.11]:

- обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;
- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;
- развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;
- доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий

в целях обеспечения национальной безопасности Российской Федерации в области культуры;

- содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды [37, с.29]:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;
- угрозы информационному обеспечению государственной политики Российской Федерации;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Источники угроз информационной безопасности Российской Федерации подразделяются на внешние и внутренние. К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур;

- стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
- обострение международной конкуренции за обладание информационными технологиями и ресурсами;
- деятельность международных террористических организаций;
- увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
- деятельность космических, воздушных, морских и наземных технических и иных средств разведки иностранных государств;
- разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним.

К внутренним источникам относятся [1, с.28]:

- недостаточная экономическая мощь государства;
- неблагоприятная криминогенная обстановка;
- недостаточная координация деятельности федеральных органов государственной власти.

Общими методами обеспечения информационной безопасности страны являются – правовые, организационно-технические и экономические.

В каждой сфере жизнедеятельности общества и государства наряду с общими методами обеспечения информационной безопасности Российской Федерации могут использоваться частные методы и формы, обусловленные спецификой факторов, влияющих на состояние объектов.

Наиболее уязвимыми объектами обеспечения информационной безопасности являются система принятия решений по оперативным

действиям, связанным с развитием таких ситуаций и ходом ликвидации их последствий, а также система сбора и обработки информации о возможном возникновении чрезвычайных ситуаций.

Таким образом подвеем итоги первой главе исследования. Понятие информационной безопасности не заключается только лишь в обеспечении защиты самой информации.

Целью реализации обеспечения мероприятий информационной безопасности является построение комплексной системы информационной безопасности и её эффективная эксплуатация.

Анализ подходов различных авторов позволяет сформулировать определение информационной безопасности следующим образом: информационная безопасность — это защищенность информации, которая выражается в противостоянии случайным или намеренным влияниям внутренних и внешних опасностей, приводящих к причинению ущерба обладателям информационного ресурса, и обеспечивающего стабильное функционирование системы.

На сегодняшний день информационная безопасность, является необходимой составляющей безопасности национальной, и представляется собой, в объективном смысле – состояние, когда информационным ресурсам не угрожает никакая опасность. Но в официальной трактовке данного понятия заложено противоречие, так как в соответствии с ней информационная безопасность — это состояние защищенности жизненноважных интересов личности, общества и государства, что изначально закладывает в понятие ошибочный, на наш взгляд, смысл.

Глава 2 Правовые аспекты обеспечения информационной безопасности в Российской Федерации

2.1 Правовое регулирование обеспечения информационной безопасности в Российской Федерации

Созданием законодательной базы в области информационной безопасности государство стремится защитить свои информационные ресурсы.

В качестве нормативной правовой основы, непосредственно обеспечивающей информационную безопасность в указанной сфере, можно определить [3, с. 12]:

- Конституцию Российской Федерации;
- общепризнанные принципы и нормы международного права, а также международные правовые акты, ратифицированные Российской Федерацией в установленном порядке;
- федеральные законы и законы Российской Федерации: «О безопасности», «О государственной тайне», «О лицензировании отдельных видов деятельности», «О техническом регулировании», «О связи», «О коммерческой тайне», «Об электронной цифровой подписи», «О федеральной службе безопасности»;
- указы и распоряжения Президента Российской Федерации: «Доктрина информационной безопасности», «Об утверждении перечня сведений, отнесенных к государственной тайне», «О перечне должностных лиц органов государственной власти, наделяемых полномочиями по отнесению сведений к государственной тайне», «Вопросы Министерства обороны Российской Федерации»; « Об утверждении положения о Федеральной Службе Охраны Российской Федерации»;

- постановления Правительства Российской Федерации: «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»;
- нормативные правовые акты федеральных органов исполнительной власти ГОСТы, руководящие документы: Приказ ФСБ РФ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)», Приказ ФСО России от 12.09.2017 N 508 "Об утверждении Порядка организации работы по обеспечению доступа к информации о деятельности Федеральной службы охраны Российской Федерации" (Зарегистрировано в Минюсте России 06.10.2017 N 48450), Приказ ФСО России от 07.09.2016 N 443 "Об утверждении Положения о российском государственном сегменте информационно-телекоммуникационной сети "Интернет" (Зарегистрировано в Минюсте России 14.10.2016 N 44039).

Законодательство в этой сфере можно разделить на три группы в зависимости от их роли:

- нормативно-правовые акты, определяющие общие положения;
- нормативно-правовые акты, определяющие компетенцию уполномоченных органов;
- нормативно-правовые акты, определяющие механизм регулирования в данной сфере.

Рассмотрим более подробно данные группы [5, с. 2].

В целях охраны и защиты прав и свобод в информационной сфере Конституция Российской Федерации устанавливает гарантии, обязанности, механизмы защиты и ответственности. К основным конституционным положениям обеспечения информационной безопасности относятся. Гарантируя каждому право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, в то же время Конституция Российской Федерации предусматривает, что федеральным законом определяется перечень сведений, составляющих государственную тайну (ч. 4 ст. 29).

Такое законодательное решение вызвано необходимостью защиты суверенитета России, обеспечения ее обороны и безопасности и соотносится с предписаниями ч. 3 ст. 55 Конституции Российской Федерации, допускающей в указанных целях ограничение федеральным законом прав и свобод человека и гражданина, а, следовательно, и права на информацию. Исходя из этого, законодатель вправе устанавливать перечень сведений, которые могут быть отнесены к государственной тайне, регулировать отношения, связанные с их рассекречиванием и защитой, определять порядок допуска и доступа граждан к таким сведениям.

Наибольшую актуальность и значимость действенность нормативного обеспечения охраны национальных интересов приобретает в сфере международного (межгосударственного) военно-технического сотрудничества.

Также рассматриваемые вопросы отражены в Законе РФ «О безопасности», он закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности.

Для создания и поддержания необходимого уровня защищенности объектов безопасности в Российской Федерации разрабатывается система

правовых норм, регулирующих отношения в сфере безопасности, определяются основные направления деятельности органов государственной власти и управления в данной области, формируются или преобразуются органы обеспечения безопасности и механизм контроля и надзора за их деятельностью.

Для непосредственного выполнения функций по обеспечению безопасности личности, общества и государства в системе исполнительной власти в соответствии с законом образуются государственные органы обеспечения безопасности.

Основными принципами обеспечения безопасности являются [6, с. 30]:

- законность;
- соблюдение баланса жизненно важных интересов личности, общества и государства;
- взаимная ответственность личности, общества и государства по обеспечению безопасности;
- интеграция с международными системами безопасности.

При обеспечении безопасности не допускается ограничение прав и свобод граждан, за исключением случаев, прямо предусмотренных федеральным законодательством.

Граждане, общественные и иные организации и объединения имеют право получать разъяснения по поводу ограничения их прав и свобод от органов, обеспечивающих безопасность. По их требованию такие разъяснения даются в письменной форме в установленные законодательством сроки.

Положения Закона «О государственной тайне» обязательны для исполнения на территории Российской Федерации и за ее пределами всеми органами государственной власти, а также организациями, наделенными в соответствии с федеральным законом полномочиями осуществлять от имени Российской Федерации государственное управление в установленной сфере деятельности.

Федеральный закон «О связи» устанавливает правовые основы деятельности в области связи на территории Российской Федерации и на находящихся под юрисдикцией Российской Федерации территориях, определяет полномочия органов государственной власти в области связи, а также права и обязанности лиц, участвующих в указанной деятельности или пользующихся услугами связи определяет требования к функционированию единой сети связи России к продукции, связанной с обеспечением целостности, устойчивости функционирования указанной сети и ее безопасности, отношения, связанные с обеспечением целостности единой сети связи Российской Федерации и использованием радиочастотного спектра, соответственно устанавливаются и регулируются законодательством Российской Федерации в области связи [34].

Федеральный закон «О коммерческой тайне» регулирует отношения, связанные с установлением, изменением и прекращением режима коммерческой тайны в отношении информации, составляющей секрет производства (ноу-хау). Действие закона распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована и не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Целью Федерального закона «Об электронной цифровой подписи» является обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе.

Действие Федерального закона распространяется на отношения, возникающие при совершении гражданско-правовых сделок и в других предусмотренных законодательством Российской Федерации случаях, не

распространяется на отношения, возникающие при использовании иных аналогов собственноручной подписи.

Доктрина информационной безопасности, является логическим дополнением Стратегии национальной безопасности Российской Федерации. Ее основные требования детализируются в законодательных и иных нормативно–правовых актах, находят отражение в стратегии развития государства в виде целевых государственных программ и проектов.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Информационная сфера, являясь системообразующим фактором жизни общества, активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности, и в ходе технического прогресса эта зависимость будет возрастать [27, с. 5].

Интересы государства в информационной сфере заключаются в создании условий для гармоничного развития информационной инфраструктуры, для реализации конституционных прав и свобод человека и гражданина в области получения информации и пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности России, политической, экономической и социальной стабильности, в безусловном обеспечении законности и правопорядка, развитии равноправного и взаимовыгодного международного сотрудничества.

На основе национальных интересов Российской Федерации в информационной сфере формируются стратегические и текущие задачи

внутренней и внешней политики государства по обеспечению информационной безопасности.

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере [25, с. 15]:

- соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны;
- информационное обеспечение государственной политики Российской Федерации, связанное с доведением до российской и международной общественности достоверной информации о государственной политике, официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам;
- развитие современных информационных технологий, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники. Россия должна занять достойное место среди мировых лидеров микроэлектронной и компьютерной промышленности;
- защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и

телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.

Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» [30].

Перечень сведений, отнесенных к государственной тайне, содержит сведения в военной области, в области экономики, науки и техники, внешней политики и экономики, разведывательной, контрразведывательной и оперативно-разыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации, а также наименования государственных органов и организаций, наделенных полномочиями по распоряжению этими сведениями.

В военной области это сведения о:

- содержании или результатах выполнения целевых программ, научно-исследовательских, опытно-конструкторских работ по созданию или модернизации вооружения, военной техники;
- тактико-технических требованиях и характеристиках, возможностях боевого применения вооружения и военной техники;
- российском экспорте или импорте вооружения, военной техники, их ремонте или эксплуатации, об оказании технического содействия иностранным государствам в создании вооружения, военной техники, военных объектов или объектов оборонной промышленности, об оказании Российской Федерацией военно-технической помощи иностранным государствам, если разглашение этих сведений может нанести ущерб безопасности государства (ст. 72).

Государственные органы и организации, наделенные полномочиями по распоряжению сведениями, отнесенными к государственной тайне: МВД России, МЧС России, Министерство бороны Российской Федерации, Министерство здравоохранения Российской Федерации, Министерство науки и высшего образования Российской Федерации, Министерство

промышленности и торговли Российской Федерации, Министерство экономического развития Российской Федерации, ФСБ России, ФСО России, Российская государственная корпорация по атомной энергии «Росатом», Государственная корпорация по космической деятельности «Роскосмос», Главное управление специальных программ Президента Российской Федерации, ФСТЭК России и др. [19, с. 9].

Каждый государственный орган и каждая организация, указанные в перечне, наделены полномочиями по распоряжению сведениями отраслевой (ведомственной) принадлежности в пределах их компетенции, а также сведениями других собственников информации соответствующей тематической направленности по их представлению.

Компетенцию уполномоченных органов регулируют следующие нормативно-правовые акты.

Федеральный закон «О федеральной службе безопасности» определяет назначение, состав, правовые основы и принципы деятельности федеральной службы безопасности, направления деятельности, полномочия, силы и средства органов федеральной службы безопасности, а также порядок контроля и надзора за деятельностью органов федеральной службы безопасности.

Федеральная служба безопасности Российской Федерации является федеральным органом исполнительной власти, в пределах своих полномочий осуществляющим государственное управление в области обеспечения безопасности Российской Федерации, обеспечивающим информационную безопасность Российской Федерации и непосредственно реализующим основные направления деятельности органов федеральной службы безопасности, определенные законодательством Российской Федерации.

Руководство деятельностью ФСБ России осуществляется Президентом Российской Федерации.

К органам федеральной службы безопасности относятся:

– федеральный орган исполнительной власти в области обеспечения безопасности;
– управления (отделы) федерального органа исполнительной власти в области обеспечения безопасности по отдельным регионам и субъектам Российской Федерации (территориальные органы безопасности).

Деятельность органов федеральной службы безопасности осуществляется по следующим основным направлениям:

– контрразведывательная деятельность;
– борьба с терроризмом;
– борьба с преступностью;
– разведывательная деятельность;
– пограничная деятельность;
– обеспечение информационной безопасности.

Иные направления деятельности органов федеральной службы безопасности определяются федеральным законодательством. (Ст. 8)

Обеспечение информационной безопасности – деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочий:

– при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
– при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации.

Обязанностью органов федеральной службы безопасности является:

- организовывать и обеспечивать безопасность в сфере шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и в пределах своих полномочий в ее учреждениях, находящихся за пределами Российской Федерации;
- участвовать в разработке и реализации мер по защите сведений, составляющих государственную тайну; осуществлять контроль за обеспечением сохранности сведений, составляющих государственную тайну, в государственных органах, воинских формированиях, на предприятиях, в учреждениях и организациях независимо от форм собственности; в установленном порядке осуществлять меры, связанные с допуском граждан к сведениям, составляющим государственную тайну.

Права органов федеральной службы безопасности:

- оказывать содействие предприятиям, учреждениям и организациям независимо от форм собственности в разработке мер по защите коммерческой тайны;
- осуществлять на компенсационной или безвозмездной основе подготовку кадров для специальных служб иностранных государств, служб безопасности предприятий, учреждений и организаций независимо от форм собственности, если это не противоречит принципам деятельности органов Федеральной службы безопасности;
- осуществлять в соответствии со своей компетенцией регулирование в области разработки, производства, реализации, эксплуатации шифровальных (криптографических) средств и защищенных с использованием шифровальных средств систем и комплексов телекоммуникаций, расположенных на территории Российской Федерации, а также в области предоставления услуг по шифрованию информации в Российской Федерации, выявления электронных

устройств, предназначенных для негласного получения информации, в помещениях и технических средствах;

- осуществлять государственный контроль за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи, контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также в соответствии со своей компетенцией контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;
- участвовать в определении порядка разработки, производства, реализации, эксплуатации и обеспечения защиты технических средств обработки, хранения и передачи информации ограниченного доступа, предназначенных для использования в учреждениях Российской Федерации, находящихся за ее пределами.

Основными задачами ФСБ России в сфере защиты информации являются [16, с. 21]:

- обеспечение в пределах своих полномочий защиты сведений, составляющих государственную тайну, и противодействия иностранным организациям, осуществляющим техническую разведку;
- формирование и реализация в пределах своих полномочий государственной и научно-технической политики в области обеспечения информационной безопасности;
- организация в пределах своих полномочий обеспечения криптографической и инженерно-технической безопасности

информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом.

Для решения основных задач в сфере защиты информации ФСБ России осуществляет следующие функции:

- в пределах своих полномочий разрабатывает меры по защите сведений, составляющих государственную тайну, осуществляет контроль за обеспечением сохранности сведений, составляющих государственную тайну, в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, воинских формированиях и организациях, осуществляет меры, связанные с допуском граждан к сведениям, составляющим государственную тайну, а также с допуском предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, с созданием средств защиты информации и с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны;
- координирует деятельность: федеральных органов исполнительной власти по осуществлению контрразведывательных мероприятий и мер по обеспечению собственной безопасности этих органов; федеральных органов исполнительной власти и организаций по обеспечению криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, а также систем шифрованной, засекреченной и иных видов специальной связи в Российской Федерации и ее учреждениях за рубежом; федеральных органов исполнительной власти в области разработки, производства, закупки, ввоза в Российскую Федерацию и вывоза из Российской Федерации специальных технических средств, предназначенных (разработанных, приспособленных,

запрограммированных) для негласного получения информации в процессе осуществления оперативно-разыскной деятельности, а также их оперативных подразделений по выявлению нарушений установленного порядка разработки, производства, реализации, приобретения в целях продажи, ввоза в Российскую Федерацию и вывоза из Российской Федерации специальных технических средств, предназначенных для негласного получения информации;

- определяет порядок осуществления контроля за обеспечением защиты сведений, составляющих государственную тайну, в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, воинских формированиях и организациях, а также порядок проведения мероприятий, связанных с допуском граждан к сведениям, составляющим государственную тайну, и с приемом на военную службу (работу) в органы безопасности;
- определяет порядок осуществления в пределах своих полномочий контроля за организацией и функционированием криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи, за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Российской Федерации и в ее учреждениях, находящихся за пределами Российской Федерации, а также за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;
- участвует в обеспечении закрытой телефонной, шифрованной и иных видов специальной связи с учреждениями Российской Федерации, находящимися за ее пределами (представительская связь), а также в

проведении работ по обеспечению ввода в эксплуатацию шифровальных комплексов (в том числе в учреждениях Российской Федерации, находящихся за ее пределами) и развитию системы представительской связи;

- участвует в разработке и реализации мер по обеспечению информационной безопасности страны и защите сведений, составляющих государственную тайну;
- в пределах своих полномочий разрабатывает и утверждает нормативные и методические документы по вопросам обеспечения информационной безопасности информационно-телекоммуникационных систем и сетей критически важных объектов, а также организует и осуществляет контроль за обеспечением информационной безопасности указанных систем и сетей;
- организует и проводит исследования в области защиты информации, экспертные криптографические, инженерно-криптографические и специальные исследования шифровальных средств, специальных и закрытых информационно-телекоммуникационных систем, а также информационно - телекоммуникационных систем и сетей критически важных объектов;
- осуществляет кадровое обеспечение органов безопасности, а также руководство деятельностью образовательных учреждений, входящих в систему органов безопасности;
- оказывает содействие организациям в разработке мер по защите коммерческой тайны;
- осуществляет иные функции.

Указ Президента РФ «Вопросы Министерства обороны Российской Федерации» устанавливает, что Министерство обороны России осуществляет межведомственный и ведомственный контроль за обеспечением защиты государственной тайны [31].

Механизм регулирования в данной сфере определяется Федеральным законом «О лицензировании отдельных видов деятельности» регулирует отношения, возникающие между федеральными органами исполнительной власти, органами исполнительной власти субъектов Российской Федерации, юридическими лицами и индивидуальными предпринимателями в связи с осуществлением лицензирования отдельных видов деятельности в соответствии с перечнем, предусмотренным п. 1 ст. 17 данного закона.

Федеральный закон «О техническом регулировании» регулирует отношения, возникающие при [33]:

- разработке, принятии, применении и исполнении обязательных требований к продукции или к связанным с ними процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации;
- разработке, принятии, применении и исполнении на добровольной основе требований к продукции, процессам проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнению работ или оказанию услуг;
- оценке соответствия;
- определяет права и обязанности участников регулируемых законом отношений.

Постановление Правительства РФ «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны». Постановление разработано в соответствии с Законом Российской Федерации «О государственной тайне» и в целях установления порядка допуска предприятий, учреждений и организаций к проведению работ, связанных с

использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны.

Постановление Правительства РФ «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности». Данное постановление утверждает правила разработаны в соответствии с Законом Российской Федерации «О государственной тайне» и являются обязательными для исполнения органами государственной власти, органами местного самоуправления, предприятиями, учреждениями и организациями, руководители которых наделены полномочиями по отнесению сведений к государственной тайне [21].

Приказ ФСБ РФ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)». Положение разработано во исполнение Федерального закона «О федеральной службе безопасности» с целью определения порядка разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну.

Национальный стандарт РФ ГОСТ Р ИСО/МЭК ТО 13335-4-2007 «Информационная технология. Методы и средства обеспечения безопасности». Данный стандарт является руководством по выбору защитных мер с учетом потребностей и проблем безопасности организации.

Таким образом, видно, что в Российской Федерации создана и постоянно совершенствуется нормативно-правовая база защиты информации составляющей государственную тайну во всех аспектах деятельности.

Развитие мира идет по пути глобализации всех сфер международной жизни, которая отличается высоким динамизмом и взаимозависимостью событий.

Реализуется государственная политика в области национальной обороны, государственной и общественной безопасности, устойчивого развития России, адекватная внутренним и внешним условиям. Созданы предпосылки для укрепления системы обеспечения национальной безопасности, консолидировано правовое пространство.

Основными направлениями обеспечения Российской Федерации являются стратегические национальные приоритеты, для создания безопасных условий реализации конституционных прав и свобод граждан Российской Федерации, осуществления устойчивого развития страны, сохранения территориальной целостности и суверенитета государства.

Таким образом, на сегодняшний день в Российской Федерации созрело много перспективных и имеющих существенную значимость вопросов, относящихся к защите информации не только личности и общества, но и возникающих при защите информации составляющей государственную тайну, которым необходима более детальная регламентация с правовой точки зрения.

Глава 3 Проблемы обеспечения и совершенствования системы информационной безопасности

3.1 Проблемные аспекты обеспечения информационной безопасности

Современная ситуация в Российской Федерации относительно уровня информационной безопасности в стране характеризуется высоким уровнем угрозы кибератак и киберпреступлений, а также возрастающей важностью информационных технологий в жизни общества и государства. В этой связи, правовая политика в сфере информационной безопасности становится все более актуальной.

Она направлена на обеспечение прав и свобод граждан в сфере информационных отношений, защиту национальной безопасности, интересов государства и бизнеса от киберугроз, противодействие киберпреступлениям и защиту персональных данных.

Правовая политика в этой сфере охватывает такие вопросы как установление стандартов безопасности информационных систем, нормирование деятельности провайдеров и операторов связи, регулирование сбора и использования информации о гражданах, меры по обнаружению и предотвращению кибератак, а также ответственность за нарушение правил и требований в сфере информационной безопасности.

Проблемные аспекты обеспечения информационной безопасности в стране следующие:

- Отсутствием единой международной системы норм и правил в области информационной безопасности.
- Нехватко й квалифицированных специалистов в области информационной безопасности.
- Недостаточной осведомленностью пользователей о возможных угрозах и способах защиты своих данных.

- Постоянным развитием технологий и появление новых угроз.
- Недостаточной координацией между различными организациями и ведомствами, ответственными за обеспечение информационной безопасности.
- Недостаточной финансовой поддержкой и инвестициями в сферу информационной безопасности.
- Низким уровнем осведомленности и готовности киберпреступников, что позволяет им успешно осуществлять атаки на объекты информационной инфраструктуры.
- Неэффективностью законодательства в области информационной безопасности и недостаточностью мер по пресечению киберпреступлений.
- Недостаточной защитой критически важных объектов информационной инфраструктуры, таких как энергетические системы, финансовые институты и государственные организации.

Охарактеризуем их более подробно.

Одним из основных проблемных аспектов обеспечения информационной безопасности является отсутствие единой международной системы норм и правил в этой области. Каждая страна имеет свои законы и правила, что может привести к различным подходам и противоречиям в решении вопросов информационной безопасности.

Еще одной проблемой является нехватка квалифицированных специалистов в области информационной безопасности. Большинство организаций не имеют достаточно квалифицированных сотрудников, что может привести к неправильному управлению информационными ресурсами и нарушению безопасности данных.

Также существует проблема недостаточной осведомленности пользователей о возможных угрозах и способах защиты своих данных. Многие пользователи не знают, как защитить свои личные данные и не следят за

безопасностью своих устройств, что может привести к утечке личной информации и краже денежных средств.

Одной из главных проблем также считается постоянное развитие технологий и появление новых угроз. Киберпреступники постоянно находят новые способы атак и взлома систем, что требует постоянного обновления и совершенствования мер безопасности.

Согласно вышеупомянутой доктрине информационной безопасности и анализу других законодательных и административных актов в области информационной безопасности в России, можно выделить следующие основные недостатки российской системы информационной безопасности

Существующие государственные ограничения, запрещающие использование и распространение определенных источников информации и данных, которые в большей степени применимы к информации из внешней среды России.

Еще одной проблемой обеспечения информационной безопасности в России является неполнота нормативно-правовой базы в этой области.

В результате в Российской Федерации не созданы институты информации, источников информации и СМИ на мировом уровне; некоторые нормативно-правовые акты трактуются неоднозначно или отклоняются от законов и стандартов, которые необходимо соблюдать в контексте защиты и распространения информации; нет четкого понимания прав и обязанностей лиц, участвующих в информационных отношениях, наказаний за предоставление ложной информации, либо они недостаточно строги для регулирования подобных случаев.

Эти аспекты доказывают отсутствие связи между государством, общественностью, СМИ и другими субъектами, когда речь идет о защите и использовании информации в России.

Во многих странах СМИ независимы и имеют право подавать информацию так, как они считают нужным. В России большинство СМИ ограничены в освещении событий федеральными, региональными и местными

властями. Это является формой искажения информации в пользу властей и нарушением прав граждан.

Помимо искажения информации СМИ, существует также проблема выражения людьми своего мнения и представления общественности той или иной информации.

Здесь следует отметить, что тенденция современного цифрового общества такова, что любой человек может выразить свое мнение через социальные сети, и его может увидеть большое количество людей. Те, кто публикует новости о важных событиях, таких как количество погибших в ДТП или решение суда, должны отвечать за свои слова. Во многих случаях дезинформация наказывается легким наказанием, что приводит к потере информации, поскольку она не основана на фактах и не является достоверной [16, с. 45].

Следующим проблемным аспектом является то, что частная жизнь всех граждан Российской Федерации не защищена. Российское законодательство, включая Конституцию, регулирует права и обязанности человека, что также означает, что такие аспекты, как семейная тайна, частная жизнь, переписка и другие, не соблюдаются в полной мере при отсутствии соответствующих правовых, организационных и технических положений.

В результате возникает проблема, что правоохранительные органы не защищают частную жизнь и персональные данные российских граждан, которые иногда даже используются в собственных целях. Отсутствует адекватный уровень защиты данных. В России один из самых высоких уровней киберпреступности в мире. Кроме того, часто происходят взломы аккаунтов в социальных сетях и несанкционированное вторжение в частную жизнь людей сверх предоставленных им прав для раскрытия преступлений или вычисления определенных фактов о лицах.

Существуют проблемы с государственным управлением информационным пространством в Российской Федерации. Существуют также негативные аспекты участия России в глобальном информационном

пространстве и мировой цифровой экономике. В силу технологической отсталости России и уровня развития информационного пространства возникают сбои в международной поставке информации в этой сфере на территорию России и в эффективности работы СМИ, телекоммуникационных компаний и других субъектов.

Следующие проблемы связаны с незначительной поддержкой органами государственной власти развития данной сферы в России и устранения угроз информационной безопасности. К ним относятся неэффективность контроля федеральных органов власти над региональными в этой сфере, а также общая низкая информированность государственных органов, как региональных, так и национальных, об уровне информационной безопасности даже в стратегически важных коммерческих организациях.

Низкая эффективность работы правоохранительных органов и других государственных органов по обеспечению сохранности государственной тайны. В последние годы особенно остро встала проблема нарушения права на защиту информации и ее конфиденциальности со стороны общественных деятелей, должностных лиц и представителей СМИ, предоставляющих ложную информацию по тем или иным вопросам, не подлежащую разглашению.

Как и во многих других сферах деятельности, в области информационной безопасности наблюдается утечка высококвалифицированных кадров из-за низкого уровня заработной платы по сравнению с зарубежными странами. Это снижает компетентность и эффективность команд, организующих защиту, использование и доступность информации.

Проблема усугубляется санкциями, введенными в результате последних событий в экономической и политической ситуации в России, низкой эффективностью импортозамещения, кризисом, падением курса рубля и т.д. Таким образом, иностранные партнеры получат доступ к информации о

российских компаниях, государственных органах и политических решениях, и при необходимости смогут использовать полученные данные о России.

Информационные технологии и цифровая экономика являются тенденциями современного мира, но именно информационной безопасности в России не уделяется достаточного внимания. Большое внимание уделяется развитию цифровой экономики, совершенствованию методов оборудования, использованию новых технологий, компьютеризации всех слоев населения, развитию деловой активности в Интернете и другим аспектам.

Однако недостаточное законодательное и судебное обеспечение регулирования информационной безопасности, недостаточное финансирование противодействия угрозам в этой сфере приводят к ухудшению информационной безопасности и использованию информационного оружия против политических и экономических интересов России.

Таким образом, проблемы информационной безопасности России заключаются в следующем Ограниченность органов государственной власти, несовершенство правовой структуры, зависимость СМИ от органов государственной власти и подчинение им, низкая ответственность за предоставление ложной информации, незащищенность персональных данных, высокий уровень киберпреступности, неэффективная политика защиты информации, низкий уровень защиты государственной тайны, отток квалифицированных кадров, отток иностранных технологий.

Процесс регулирования информационного обеспечения всех видов социальной деятельности и их структур в мировом и российском информационном пространстве является важной составляющей информационной безопасности. Как гарант сохранения информации, государство должно четко определить политику правового развития в этой области.

Важным вопросом является регулирование обмена информацией в сети Интернет. По аналогии с теорией права можно выделить два подхода к

вопросу правового регулирования Интернета. Первый - в пользу абсолютной свободы, второй - в пользу верховенства закона в Интернете.

Первый подход основан на веб-традиции и имеет много сторонников в интернет-сообществе. Второй подход менее распространен, против него решительно выступает часть интернет-пользователей, а сторонники "интернет-анархистов" и "интернет-фундаменталистов" борются с ним организованными акциями протеста. Другая тенденция заключается в том, что большинство пользователей Интернета негативно относятся к государственному контролю за содержанием распространяемых материалов.

И это несмотря на то, что Россия является одной из ведущих стран в области информационного законодательства. Помимо положений Конституции РФ и норм международного характера, инкорпорированных в национальное законодательство, одной из особенностей российской правовой системы является наличие законов, содержащих информационное законодательство в чистом виде (Федеральный закон "Об информации, информатизации и защите информации" от 25.01.95 № 24-ФЗ, Федеральный закон "Об участии в международном информационном обмене" от 04.07.96 № 85-ФЗ).

В существующих официальных документах и теоретических работах по проблематике обеспечения национальной безопасности (в том числе и по видам безопасности, в частности, по информационной безопасности) понятие национальной безопасности является, несомненно, ключевым. Для работы понятие «национальной безопасности» является родовым, так как информационная безопасность является неотъемлемой её частью. В связи с этим необходимо остановится, на более глубоком изучении понятия национальная безопасность [6, с.30].

На сегодняшний день, в современной науке существую три наиболее распространенных подхода к определению понятия «национальная безопасность».

Существует также большое количество законов, регулирующих разные стороны информационной деятельности применительно к конкретным явлениям: Закон РФ «О средствах массовой информации», Федеральные законы «О государственной поддержке средств массовой информации и книгоиздания Российской Федерации», «О рекламе», Законы РФ «Об авторском праве и смежных правах», «О правовой охране программ для электронных вычислительных машин и баз данных».

Имеется огромное количество Указов Президента РФ и Постановлений Правительства РФ, принято также значительное количество документов по вопросам телевидения и радиовещания, отдельным средствам массовой информации.

За последние годы в этой области можно наблюдать значительные сдвиги под влиянием реальных процессов информатизации. Правовой основой здесь является Федеральный закон «Об информации, информатизации и защите информации», которым наиболее детально урегулированы вопросы правового режима информационных ресурсов.

За последние несколько лет в отношении Российской Федерации последовательно были введены более 56 пакетов санкционных нормативно-правовых актов. Наиболее расширенный список у Соединенных Штатов Америки. В него вошли около трёхсот сорока пяти юридических лиц, из которых на двести тридцать две компании распространены только направленные ограничения (в отношении руководства и сотрудников), а на одиннадцать ограничения по экспорту (комплексные ограничения в деятельности).

В общей сложности под запреты попали сто двадцать две банковские (инвестиционные) организации, восемьдесят узкотехнологичных организаций и предприятий военного назначения, восемьдесят компаний нефтяной и газодобывающей промышленности, двадцать одна транспортная и логистическая компания, шестнадцать строительных организаций.

Пятьдесят восемь юридических лиц из более чем трехсот организаций, попавших под санкции Америки и её союзников, зарегистрированы за пределами России. Большую часть указанного списка США составляют дочерние компании ПАО «Газпром», ПАО «НК «Роснефть», Государственная корпорация развития «ВЭБ.РФ», ПАО «Сбербанк», ПАО «Банк ВТБ» а также государственная корпорация «Ростех» и «Роскосмос».

Основным направлением оказания санкционного давления помимо экономического сектора стало информационное пространство. Крупные западные медиа холдинги и ведущие СМИ, в части касающейся создания негативных информационных поводов в отношении российских компаний и высшего политического руководства Российской Федерации. На сегодняшний день под ограничения на въезд в США и страны Евросоюза попали 210 видных российских политиков и бизнесменов.

При этом органами, отвечающими за внешнюю политику, в частности Госдепартаментом США, на постоянной основе проводятся информационные акции, направленные на дискредитацию лиц и компаний, попавших в санкционные списки.

Важную роль в становлении современной информационной безопасности Российской Федерации, сыграл переход от тоталитарного государства к демократическому, который послужил толчком к развитию законодательства в информационной сфере вследствие того, что на первый план вышли права человека и общества, чего, де-факто, не существовало в Союзе советских социалистических республик. Чтобы ликвидировать данный разрыв в информационной сфере, законодателю пришлось принимать профильные нормативные акты в максимально сжатые сроки, что, в определенной степени отразилось на их качественном содержании.

В наибольшей степени недостатки и отрицательные характеристики действующего нормативного закрепления понятия «информационной безопасности» и в целом всей информационной сферы проявились именно в условиях санкционной политики Соединенных Штатов Америки и её

международных партнеров, в результате чего российская правовая система остро нуждается в немедленном совершенствовании действующих нормативно-правовых актов по указанной проблематике;

На сегодняшний день информационная безопасность, является необходимой составляющей безопасности национальной (государственной), и представляет собой, в объективном смысле – состояние, когда информационным ресурсам (главным образом общественному сознанию российского общества) не угрожает никакая опасность.

При этом в официальной трактовке данного понятия заложено противоречие, так как в соответствии с ней информационная безопасность – это состояние защищенности жизненноважных интересов личности, общества и государства, что изначально закладывает в понятие ошибочный смысл, в связи с тем, что понятие «жизненно важные интересы» это классический подход западной науки, перенятый российской правовой системой на заре 21 века. По мнению автора, интересы не могут нуждаться в защите как в таковой. Интересы можно продвигать и реализовывать. С точки зрения российского права, конкретным объектом защиты должны выступать реальные данные и информационное сознание граждан Российской Федерации, подвергающиеся беспрерывным атакам из вне.

Таким образом, исследование правовой политики в сфере информационной безопасности является актуальным в свете необходимости обеспечивать безопасность национальной информационной инфраструктуры, защиту прав и интересов граждан и государства, а также предупреждение возможных киберугроз.

3.2 Совершенствование системы информационной безопасности на современном этапе

Для решения отмеченных ранее проблем в обеспечении информационной безопасности и угроз, влияющих на защиту информации в России, требуется комплекс мер направленных на устранение негативных аспектов российского информационного пространства.

Первым направлением, которое призвано совершенствовать обеспечение информационной безопасности России, является минимизация нарушений прав и свобод граждан на получение, предоставление, использование информации в соответствии с нормативно-правовыми актами в сфере информационного пространства России.

С целью осуществления данной цели, необходимо решение следующих задач:

- совершенствование инструментов нормативно-правового регулирования информационной безопасности в сфере конфиденциальной информации, в том числе защите интеллектуальной собственности;
- обеспечение полной независимости СМИ;
- недопущение распространения информации, которая ведет к конфликтам на основе национальной, религиозной и других признаков вражды.

Для повышения эффективности борьбы с распространением подобной ифнормации необходимо законодательно закрепить повышение сумм штрафов за подобные действия со стороны правонарушителей.

Так, в статье 8 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» необходимо добавить пункты 10,11, в которых будет отражаться информация об ответственности за нарушение Конституционных прав и свобод граждан, а также пунктов 1-8 Федерального закона. Кроме того, следует указать

конкретные проявления наказания и их причины в КоАП РФ и УК РФ в зависимости от серьезности правонарушения и ответственности.

В настоящее время в информационном пространстве РФ нет неограниченного права граждан на тайну переписки, звонков, конфиденциальных данных, поскольку правоохранительные органы могут использовать и получать эти данные в случаях, разрешенных законодательством РФ. Под запретом цензуры не подразумевается распространение любой информации, а лишь снижение контроля над средствами СМИ, предоставление им большей степени свободы. Недопущение конфликтов на расовой, национальной, религиозной основе особенно актуально учитывая сложность и насыщенность структуры населения РФ [5, с.5].

Следующим направлением совершенствования обеспечения информационной безопасности России является эффективное функционирование политики в области доведения до граждан достоверной, полной информации о политических решениях, государственной политики, органах власти, их деятельности при помощи общедоступных источников информации как в Интернете, так и в газетах, журналах, на радио, по телевизору, в объявлениях и других.

Для того чтобы данное направление было реализовано на практике необходимо следующее:

- всеми возможными способами развивать и поддерживать субъекты информационного пространства РФ, обеспечивать своевременность, доступность, полноту, достоверность информации;
- повысить эффективность государственных информационных ресурсов, их наполняемость и обновляемость.

Для реализации описанных выше задач необходимо в Федеральном законе от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» установить максимальные сроки на обновление информации и закрепить размеры сумм материальной поддрежки

регионам для обеспечения информационной безопасности субъектов РФ. На данный момент уже существуют некоторые программы и инструменты реализации данных задач.

Так, в государственном управлении информационной безопасностью выделена программа под названием Электронная Россия, которая содержит основы по цифровизации российской экономики. Данная программа, несмотря на свою сложность, помогает многим государственным органам создавать сайты и страницы в социальных сетях для информирования граждан и максимальной активизации защиты от недостоверной информации, опровергая их фактами государственной статистики и аналитики. Данная программа повышает прозрачность государственных органов.

В законодательстве для реализации данного направления необходимо принять следующие изменения: в Доктрине Информационной безопасности в главе 5 статье 34 добавить принципы своевременности и обновляемости поступающей от органов государственной власти информации, в статье 35 добавить к задачам государственных органов в рамках деятельности по обеспечению информационной безопасности помощь субъектам информационной среды и развитие данной сферы в РФ.

Кроме того, в статье 14 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации информационных технологиях и о защите информации» необходимо добавить пункты содержащие информацию о необходимости развития государственных информационных систем, особенно в части обновляемости и оперативности информации.

Следующим направлением совершенствования обеспечения информационной безопасности России является улучшение системы защиты информации, развитии технологий в данной сфере, повышение эффективности средств цифровизации, телекоммуникации. А также обеспечение необходимым оборудованием, программами всех субъектов информационной индустрии в целях обеспечения максимально энергоемкого и эффективного использования информационных ресурсов.

С целью осуществления данной цели, необходимо решение следующих задач:

- повышение эффективности инфраструктуры российской информационной среды;
- совершенствование использования информационных услуг и государственных информационных ресурсов;
- совершенствование взаимодействия российских наукоемких предприятия по производству и реализации информационных технологий и продуктов с зарубежными партнерами, а также улучшение производства российских технологий и программ на основе полученного опыта из других стран;
- увеличение материальной и инфраструктурной поддержки организаций, занимающихся вопросами информационной безопасности, производства и реализации информационных услуг и продуктов, а также реализующих и использующих информационные технологии на внутреннем и внешнем рынках.

Для реализации указанных выше мер в Доктрине информационной безопасности в статье 27 необходимо добавить пункты е, ж, з, в которых будут нормативно закреплены аспекты совершенствования совместной работы российских и зарубежных предприятий в сфере информационных технологий и защиты информации, повышения уровня финансирования данной сферы, развития инфраструктуры информационной среды в России.

Цифровая экономика в России является перспективным и развивающимся элементом, поэтому многие зарубежные инвесторы и компании в данной сфере хотят наладить сотрудничество с российскими. Для еще больших темпов роста рынка и развития информационных технологий, даже в период санкций и кризиса, необходимо предоставлять таким предприятиям и инвесторам особые выгодные условия и всячески поддерживать разработку информационных ресурсов отечественными предприятиями.

Следующим направлением совершенствования обеспечения информационной безопасности России является повышение эффективности защиты информационных ресурсов, продуктов и услуг от проникновений и взломов, связанных с дальнейшей утечкой, хищением, искажением, уничтожением, повреждением, неправильной обработкой и другими процессами нарушающими целостность, достоверность, конфиденциальность информации и систем ее защиты.

Для того чтобы данное направление было реализовано на практике необходимо следующее:

- повысить качество и количество производства программ и оборудования по защите данных на наукоемких и стратегически важных предприятиях России;
- с помощью существующего и вновь разработанного инструментария обеспечения информационной безопасности, реализовать процессы, которые приведут к повышению защищенности информации, представляющей собой государственную тайну;
- повысить эффективность и вовлеченность отечественных предприятий и их разработок в мировую цифровую экономику.

В целях реализации данного направления и поставленных для его реализации задач, необходимо в статье 16 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации информационных технологиях и о защите информации» добавить пункты 7 и 8, в которых будет отражена информация о совершенствовании программ и оборудования в сфере информационной безопасности, развитии защиты информации, представляющей собой государственную тайну.

На сегодняшний день уже проработано и использовано достаточно направлений, которые способствовали совершенствованию обеспечения информационной безопасности России и которые необходимо дальше развивать [35, с. 5].

Формирование и дальнейшее совершенствование нормативно-правового обеспечения сферы информационной безопасности в России. К нынешнему времени уже принят ряд законов, указов, постановлений и других нормативно-правовых актов, регулирующих защиту информации в России, в том числе описанные в работе законы, Доктрина информационной безопасности и международные соглашения России со странами-партнерами в интеграционных группировках, например, со странами ЕАЭС.

Уже большинство государственных органов, предприятий, организаций различных видов деятельности, размеров, направлений перешли к обеспечению информационной безопасности самыми современными и эффективными средствами защиты, существующими на данный момент. С каждым днем число таких предприятий и средств защиты увеличивается.

Необходимо продолжение работы в этом направлении, чтобы эти средства становились более эффективными, доступными и были реализованы, в том числе для обеспечения информационной безопасности отдельной личности, а не только на микро-, макроуровнях.

Ведется также работа по совершенствованию государственной системы защиты информации, процессу сертифицирования, лицензирования информационных ресурсов, продуктов, услуг. Необходимо дальнейшее повышение требований к качеству реализуемых информационных средств на территории страны.

Для реализации описанных выше мер и решения отмеченных проблем, необходимо решить следующие задачи совершенствования обеспечения информационной безопасности России:

– сплоченная работа федеральных, региональных и местных государственных органов по созданию программ, которые будут способствовать повышению уровня информационной безопасности страны и информированности населения о решениях, плановых показателях и тенденциях в данной сфере;

- повышение эффективности подготовки и обора кадров для осуществления деятельности в информационной среде;
- совершенствование информационной инфраструктуры посредством международного сотрудничества и использования глобальных технологий, ресурсов, сети;
- детальная проработка мер, инструментов деятельности государственных органов по обеспечению информационной безопасности России и ее регионов;
- повышение эффективности системы прогнозирования, выявления и методов борьбы с угрозами информационной безопасности, а также выработка единой политики для федерального уровня, субъектов РФ и местных властей;
- создание новых и совершенствование действующих нормативно-правовых актов в сфере защиты информации;
- улучшение качества взаимодействия с зарубежными партнерами в сфере информационных технологий, наукоемких производств;
- создание технологической базы для защиты России в разные периоды ее развития, на современном этапе кризиса, санкций и пандемии;
- совершенствование и обновление оборудования, программ и технологий защиты информации, содержащей государственную тайну
- формирование системы показателей, по которым количественно будет выражаться оценка уровня информационной безопасности страны в целом, ее субъектов, органов власти, СМИ и наиболее важных производств;
- повышение наказания и законодательное установление мер за нарушение мер по защите информации в органах власти, правоохранительных структурах, субъектах цифровой экономики России;

- повышение осознанности в необходимости обеспечения информационной безопасности и совместная с гражданами помощь в реализации данной цели;
- развитие инновационных, научных аспектов функционирования системы защиты информации;
- совершенствование реализации государственной информационной политики.

Для осуществления реализации на практике данных задач совершенствования информационной безопасности России необходимо в Доктрине информационной безопасности в статьях 35, 36 расширить полномочия государственных органов в сферах деятельности по обеспечению информационной безопасности и развитию системы защиты информации в стране.

Так, к полномочиям следует отнести в том числе развитие инфраструктуры в области информационной безопасности, совершенствование взаимодействия с зарубежными партнерами в области защиты информации, формирование количественной оценки системы информационной безопасности на уровне хозяйствующих субъектов, регионов и всей страны в целом.

Кроме того, поскольку обеспечение информационной безопасности является составным элементом национальной безопасности во всех сферах, то в статьях 23, 25 необходимо добавить направления в соответствии с предложенными выше задачами. В статье 12 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 03.04.2020) «Об информации информационных технологиях и о защите информации» в пункте 1 расширить аспекты государственного регулирования в сфере применения информационных технологий, а в пункте 2 полномочия государственных органов, органов местного самоуправления в данной сфере.

Таким образом, для совершенствования обеспечения информационной безопасности России были предложены следующие направления и меры:

минимизация нарушений прав и свобод граждан в данной сфере, совершенствование государственной политики защиты информации, совершенствование нормативно-правового обеспечения, создание новых средств защиты для граждан, предприятий и органов власти, повышение требований к качеству информационных ресурсов, повышение эффективности защиты информационных ресурсов, продуктов и услуг от проникновений и взломов. В работе были предложены следующие меры по внесению изменений в действующие нормативно-правовые акты: в статье 12 Федерального закона от 27.07.2006 N 149-ФЗ «Об информации информационных технологиях и о защите информации» в пункте 1 расширить аспекты государственного регулирования в сфере применения информационных технологий, а в пункте 2 полномочия государственных органов, органов местного самоуправления в данной сфере, в статьях 25, 26 необходимо добавить направления в соответствии с предложенными выше задачами, в статьях 35, 36 расширить полномочия государственных органов в сферах деятельности по обеспечению информационной безопасности и развитию системы защиты информации в стране.

В Доктрине информационной безопасности в статье 27 необходимо добавить пункты е, ж, з, в которых будут нормативно закреплены аспекты совершенствования совместной работы российских и зарубежных предприятий в сфере информационных технологий и защиты информации, повышения уровня финансирования данной сферы, развития инфраструктуры информационной среды в России.

В Российской Федерации созрело много перспективных и имеющих существенную значимость вопросов, относящихся к информационной безопасности не только личности и общества, но и возникающих при защите информации составляющей государственную тайну (и другие виды тайн, напр.: коммерческую, врачебную, банковскую и т.д.) которым необходима более детальная регламентация с правовой точки зрения. В частности, темпы принятия законодательных актов регламентирующих, например, борьбу с

киберпреступностью, защиту сознания граждан в сети Интернет, значительно уступают темпам появления новых форм и методов незаконного получения (или уничтожения) информационных ресурсов. При этом, наибольшую опасность в наше время представляет то, что иностранными государствами задействован ряд специальных служб и организаций, направленных на подрыв информационной безопасности российского государства;

Также хотелось бы отметить законы, принятые в 2019 г. Новый закон о неуважении власти вносит поправки в статью 20.1 КоАП РФ («Мелкое хулиганство») и в закон «Об информации, информационных технологиях и защите информации»). Согласно этим изменениям, если на информационном ресурсе будут обнаружены материалы, «предназначенные для неограниченного круга лиц, выражающие в неприличной форме явное неуважение к обществу, государству, официальным государственным символам РФ, Конституции РФ и органам, осуществляющим государственную власть в РФ», то доступ к такому ресурсу будет блокироваться Роскомнадзором.

Для граждан, которые распространяют такие материалы, предусмотрена административная ответственность: штраф от 30 до 100 тыс. руб. за первое нарушение, штраф от 100 до 200 тыс. руб. или административный арест до 15 суток — за повторное нарушение. А при дальнейших нарушениях штраф увеличится ещё больше: от 200 до 300 тыс. руб. или арест до 15 суток.

Полномочиями по выявлению сайтов в сети "Интернет", на которых содержится информация, выражающая в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам РФ, Конституции РФ или органам, осуществляющим государственную власть в РФ, наделяется Генеральный прокурор РФ и его заместитель.

Обнаружив указанную информацию, Генеральный прокурор РФ или его заместитель должны направить в Роскомнадзор требование о принятии мер по

удалению указанной информации и по ограничению доступа к информационным ресурсам, распространяющим указанную информацию.

Роскомнадзор определяет провайдера хостинга или иное лицо, обеспечивающее размещение информационного ресурса, на котором содержится обнаруженная информация, и направляет ему информацию о выявлении запрещенной информации с требованием удалить ее.

Незамедлительно с момента получения требования Роскомнадзора провайдер хостинга информирует о поступившем требовании владельца информационного ресурса, на котором размещена информация, и указывает на необходимость ее удаления.

Владелец информационного ресурса должен удалить противоправную информацию в течение суток с момента получения уведомления от провайдера хостинга.

В случае непринятия провайдером хостинга и (или) владельцем информационного ресурса мер по удалению информации, сайт, на котором размещена информация, подлежит блокировке.

В случае удаления противоправной информации, владелец информационного ресурса уведомляет об этом Роскомнадзор, который, после проверки удаления информации, направляет оператору связи уведомление о прекращении блокировки сайта.

В мае 2019 года принят Федеральный закон о «Суверенном интернете». В соответствии с законом будет создана национальная система маршрутизации интернет-трафика, главная задача которой обеспечение надежной работы российского сегмента интернета в случаях сбоев или целенаправленного масштабного внешнего воздействия. Закон был «подготовлен с учетом агрессивного характера принятой в сентябре 2018 года Стратегии национальной кибербезопасности США». Так, в подписанном Президентом США документе декларируется принцип «сохранения мира силой», Россия же впрямую и бездоказательно обвиняется в совершении хакерских атак, откровенно говорится о наказании», указывают авторы

Законопроекта. «В этих условиях необходимы защитные меры для обеспечения долгосрочной и устойчивой работы сети Интернет в России, повышения надежности работы российских интернет-ресурсов», — говорится в пояснительной записке.

При этом в документе определяются необходимые правила маршрутизации трафика, организуется контроль их соблюдения, создается возможность для минимизации передачи за рубеж данных, которыми обмениваются между собой российские пользователи. Законом вводятся новые понятия: «точка обмена трафиком», «номер автономной системы».

В соответствии с поправками, на госорганы, органы местного самоуправления, ГУПы и МУПы, государственные и муниципальные учреждения при осуществлении взаимодействия в электронной форме, в том числе с гражданами и организациями, возлагается обязанность обеспечивать возможность осуществления такого взаимодействия в соответствии с правилами и принципами, установленными нацстандартами РФ в области криптографической защиты информации, утвержденными в соответствии с ФЗ «О стандартизации в Российской Федерации».

Функции по координации обеспечения устойчивого, безопасного и целостного функционирования интернета на территории России возлагаются на Роскомнадзор.

Также определяются трансграничные линии связи и точки обмена трафиком. Их владельцы, операторы связи, обязываются при возникновении угрозы обеспечить возможность централизованного управления трафиком.

Кроме того, предусматривается возможность установки на сетях связи техсредств, определяющих источник передаваемого трафика.

Техсредства должны будут обладать возможностью ограничить доступ к ресурсам с запрещенной информацией не только по сетевым адресам, но и путем запрета пропуска проходящего трафика. Создается инфраструктура, позволяющая обеспечить работоспособность российских интернет-ресурсов в

случае невозможности подключения российских операторов связи к зарубежным корневым серверам.

При этом вводится необходимость проведения регулярных учений органов власти, операторов связи и владельцев технологических сетей по выявлению угроз и отработке мер по восстановлению работоспособности Рунета.

Защитная реакция и превентивные меры свойственны и органам надзора в области информатизации.

Специфика сферы правового регулирования и обеспечения информационной безопасности заключается в том, что здесь необходима уравновешенность между профилактической и непосредственной работой по обеспечению безопасных условий развития сферы информатизации и информатики в целом. Все те недоработки в области правового регулирования и неупорядоченности организации сфер и производства информации, сфер социальной жизни обслуживания информационно-коммуникативным ресурсом, о которых уже сказано, являются источником угроз в области информационной безопасности.

Важно отметить, что социально-политическая обстановка, сложившаяся в мире в результате окончания так называемой «холодной войны» между Западом и Востоком, по существу, так и не коснулась такого ее важного элемента, как ведение разведки. Большинство западных стран по сей день продолжают модернизировать и развивать свои специальные службы и организации, совершенствовать средства технической разведки, наращивать других возможностей.

Наряду с важными и наиболее существенными приоритетами иностранных спецслужб в сферу их интереса все чаще входят вопросы технологий, промышленности, торговли, развития компьютерных технологий, доступ к которым открывается в связи с процессом глобализации, развитием иных региональных интеграционных процессов, широким внедрением систем искусственного интеллекта.

В этих условиях реализация устаревшей модели ориентации на практику предыдущих лет, несет в себе скрытую угрозу основным государственным интересам России в военной, политической, экономической и других сферах. На текущем этапе Российская Федерации находится в положении необходимости совершенствования сложившейся системы информационной безопасности как в административном плане, так и в развитии основных концептуальных, методологических и юридических подходов к информационной безопасности.

Вопросы, связанные с информационным правом, требуют от правительства рассмотрения различных направлений деятельности в информационном секторе. Все эти направления можно объединить в единый блок, сформировав специализированный информационный сектор, объединяющий проблемы создания, производства и использования информационных носителей и информационных технологий в широком смысле.

Вторым крупным блоком системы государственного управления является деятельность по организации использования носителей информации и информационных ресурсов в различных сферах общественного развития.

Пока федеральным органом, непосредственно выполняющим государственные задачи на уровне системы федеральных органов исполнительной власти, является Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Существуют также специализированные государственные органы, которые занимаются организацией и использованием отдельных информационных ресурсов.

Это Федеральная архивная служба и Федеральная служба статистики. Государственный технический комитет. Совет Безопасности Российской Федерации уделяет большое внимание вопросам информации. Он охватывает информационные процедуры государственных и местных органов власти и их взаимодействие. Деятельность органов государственной власти - законодательной, исполнительной и полицейской - может быть продуктивной

и эффективной только при использовании информационных технологий в работе механизмов каждого института и в системе взаимодействия органов власти.

Другим блоком государственного управления в области информационных технологий является деятельность каждого отдельного учреждения и государственного органа, которые самостоятельно обеспечивают процедуры информационной поддержки своей деятельности по мере необходимости.

С началом двадцать первого века с появление передовых информационных технологий и развитие систем искусственного интеллекта, объем хранения и скорость обработки информации несмотря на незначительное повышение уровня защиты информации, в большей степени вызвали появление новых угроз, чтобы делает эффективность обеспечения информационной безопасности намного ниже. Учитывая интенсивность появления сверхновых угроз в информационной сфере, таких как появления криптовалют, развитие хакерских групп, сбор мегаданных в отношении пользователей ведущими IT-корпорациями, не приходится говорить о том, что законодательство большинства стран мира успевает вводить новые НПА, которые позволили бы повысить уровень защиты сознания людей от существующих рисков.

Таким образом, для нашей страны сегодня является важным сознание российским политическим руководством насущной необходимости совершенствования нормативно-правового регулирования информационной сферы, и информационной безопасности как ее составляющей.

Заключение

Подводя итоги выпускной квалификационной работы по теме правового обеспечения информационной безопасности российского государства на современном этапе, хочется сделать вывод, что действующая правовая система нашего общества сталкивается с многообразием постоянно возникающих рисков и угроз, влияющих на целостность критической информационной инфраструктуры Российской Федерации, и в конечном итоге на сознание российских граждан.

Законодательная власть в лице Федерального Собрания Российской Федерации пытается достаточно гибко реагировать на вызовы современности, то есть успевать за нормативным сопровождением технического прогресса, темпы которого постоянно увеличиваются, а бюрократические механизмы не дают полноценно осуществлять своевременное правовое сопровождение.

Только за последний период наше государство столкнулось с появлением сверхновых информационных угроз, таких как: распространение криптовалют, стремление хакерских группировок нанести информационный и политический ущерб, постоянный сбор и накопление мегаданных о гражданах международными IT-корпорациями, развитие систем искусственного интеллекта и другие.

Ситуация осложняется тем, что все вышеперечисленные угрозы возникают в условиях развития антироссийской санкционной политики, направленной на дискредитацию высшего политического руководства государства и влияние на информационное сознание граждан Российской Федерации. В этой связи с 2014 года Соединенными Штатами Америки и их союзниками принято более двухсот нормативных правовых актов различной ведомственной принадлежности и уровней. Новые пакеты санкций продолжают приниматься и на сегодняшний день. Что неминуемо сказывается на подрыве основ информационной безопасности России.

Президентом Российской Федерации Владимиром Владимировичем Путиным неоднократно подчеркивалась важность указанной тематики, так в своем выступлении на заседании Совета Безопасности от 23.10.2017 г. он особо подчеркнул необходимость повышения защищенности информационных систем и сетей связи государственных органов, а также обязательность усиления персональной ответственности руководителей за обеспечение информационной безопасности.

Необходимо отметить, что российский законодатель постоянно предпринимает попытки своевременно реагировать на поступающие угрозы. Так, на протяжении последнего периода времени произошли два фундаментальных события в указанной области. Это принятие новой редакции Доктрины информационной безопасности в 2016 году и принятие в 2017 году Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры». Особенно важно обратить внимание, что принятие этих нормативных актов создало условие для внесения в УК России статьи 274.1 «Неправомерное воздействие на критическую информационную систему», что может стать хорошим инструментом пресечения преступлений в сфере информационной безопасности, к сожалению, несмотря на то, что с момента вступления указанной статьи в силу с 1 января 2018 года, правоприменительной и судебной практики на сегодняшний день автору найти не удалось, и юридической науке еще только предстоит выяснить её эффективность в дальнейшем.

Подводя итоги квалификационной работы, хотелось бы отметить, что высказанные положения, выносимые на защиту в значительной мере подтвердились. В частности, были выявлены некоторые отрицательные черты формирования нормативной базы на новом для нашей страны этапе. Переход от тоталитарного строя к демократическому в полной степени не завершено до сих пор. Часть нормативных актов в сфере информационной безопасности были «приняты на скорую руку» и по своей сути скопировали западные стандарты, что не могло не отразиться на их качестве.

Рассмотрения полномочий органов и ведомств, задействованных в обеспечении информационной безопасности, указывают на то, что на сегодняшний день информационная безопасность, является необходимой составляющей безопасности национальной (государственной).

В дипломной работе рассмотрено один из главных спорных вопросов по указанной тематики, касающийся использования термина «информационная безопасность» и его содержания. В большинстве нормативных актов информационная безопасность представляет собой, в объективном смысле – состояние, когда информационным ресурсам (главным образом общественному сознанию российского общества) не угрожает никакая опасность. При этом в официальной трактовке данного понятия заложено скрытое логическое противоречие, так как в соответствии с ней информационная безопасность – это состояние защищенности жизненноважных интересов личности, общества и государства, что изначально закладывает в понятие ошибочный, на наш взгляд, смысл. При этом остается не понятным, как можно защищать интересы, скорее они нуждаются в реализации, возможно в продвижении, но не в защите. Возможным выходом из данной ситуации автор видит использование результатов аксиологического подхода, то есть раскрытие понятия через систему ценностей.

В этом аспекте необходимо особенно подчеркнуть что, для нашей страны сегодня является важным сознание российским политическим руководством насущной необходимости выработки единого подхода к понятию информационной безопасности, в связи с чем, авторам представляется верным, рассмотреть возможность внесения изменений в часть первую Доктрины информационной безопасности Российской Федерации, предложив вместо существующей формулировки «Под информационной безопасностью Российской Федерации понимается состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и

свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» следующую «Под информационной безопасностью Российской Федерации защищенность информации, информационных ресурсов, и их носителей, от попыток уничтожения, внесения изменений или нанесения любого другого значимого ущерба».

Таким образом, в условиях непрерывного информационного давления стран Запада во главе с США, очевиден факт того, что информационная сфера стала не только важнейшей сферой международного сотрудничества, а в первую очередь объектом соперничества. Проблемы в сфере информационных отношений, формирования информационных ресурсов и пользования ими обостряются вследствие политического и экономического противоборства западной коалиции стран против Российской Федерации, которая, к сожалению, ещё во многом уступает в информационном и технических аспектах, в связи с чем перед российским законодателем стоит еще множество сложных и важных вопросов.

Список используемой литературы и используемых источников

1. Антипов, А. Информационная безопасность как объект правового регулирования // Первая миля. – 2016. – № 3 (56). – С. 28-29.
2. Вербицкая, Т. Суды о национальной безопасности // ЭЖ-Юрист. – 2016. – № 13. – 94 с.
3. Емелькина, И. В. Основные характеристики российского менталитета в условиях информационного общества // Информационное право. – 2017. – № 1. – 30 с.
4. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» // СЗ РФ.1997. № 41. Ст. 8220-8235.
5. Калинин, А.Ю. Информационная безопасность и информационное право России // Представительная власть - XXI век: законодательство, комментарии, проблемы. – 2017. – № 1 (152). – 11 с.
6. Кардашова, И. Б. О проблемах исследования обеспечения национальной безопасности // Административное право и процесс. – 2019. – № 5. – С. 30-31.
7. Карягина, А. В. История информационной правовой политики и безопасности в Российской Федерации: доктринальный и стратегический подходы // История государства и права. – 2012. – № 8. – 41 с.
8. Козлов С.С., Тимошенко В.А. Комментарий к Федеральному закону от 21 июля 1993 г. № 5485-1 «О государственной тайне» // ООО «Новая правовая культура». 2006. С. 125 – 170.
9. Козориз, Н. Л. Информационная безопасность в системе противодействия опасности // Информационное право. – 2016. – № 1. – 31 с.
10. Козориз, Н.Л. Информационная безопасность в глобальном информационном пространстве // Право и государство: теория и практика. – 2018. – № 7 (103). – 150 с.
11. Комментарий к Конституции Российской Федерации (под ред. В.Д. Зорькина, Л.В. Лазарева) // « Эксмо» . 2010. С. 12-13

12. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учётом поправок, внесённых Законами Российской Федерации о поправках к Конституции Российской Федерации от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // СЗ РФ. 2014. N 31. ст. 4398.

13. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере. – М.: Логос. – 2018. – С. 48-

14. Куракин, А. В. Информационная безопасность в системе государственной службы / А. В. Куракин, Г. Н. Кулешов, П. В. Несмелов // Административное и муниципальное право. – 2017. – № 2. – 203 с.

15. Мигачев, Ю. И. Правовые основы национальной безопасности (административные и информационные аспекты) / Ю. И. Мигачев, Н. А. Молчанов // Административное право и процесс. – 2018. – № 1. – 49 с.

16. Михайлёнок, О. М. Политические аспекты информационной безопасности личности // Власть. – 2015. – № 12. – 70 с.

17. Нестеров А.В. Философия защиты информации // Научно-техническая информация. Серия 1. Организация и методика информационной работы. 2004. № 3, С. 28

18. Номоконов, В. А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. – 2018. – № 24. – 55 с.

19. Попов, В. В. Информация как фактор воздействия на политическую жизнь общества (социокультурный аспект) // Вопросы безопасности. – 2015. – № 6. – 98 с.

20. Постановление Правительства РФ от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» // Российская газета.1995. № 17.

21. Постановление Правительства РФ от 15 апреля 1995 г. № 333 «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны» // Российская газета.1995. № 17.

22. Постановление Правительства РФ от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности // Российская газета. 1994.

23. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ–2005)» // Зарегистрировано в Минюсте РФ. 2005. № 6382.

24. Распоряжение Президента РФ от 16 апреля 2005 г. № 151–рп «О перечне должностных лиц органов государственной власти и организаций, наделяемых полномочиями по отнесению сведений к государственной тайне» //СЗРФ. 2005. №17.

25. Смирнов, А. А. К вопросу о понятии, объекте и содержании информационно-психологической безопасности // Административное право и процесс. – 2016. – № 1. – 39 с.

26. Снетков, В. Н. Обеспечение информационной безопасности в условиях гражданского общества // Проблемы права в современной России: сборник статей международной межвузовской научно-практической конференции. – СПб.: Изд-во Политехн. ун-та. – 2018. – 426 с.

27. Соколова, С. Н. Информационное право и государственное регулирование информационной безопасности / С. Н. Соколова, Ю. М. Сенив // Информационное право. – 2016. – № 2. – 7 с.

28. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации"// "Собрание законодательства РФ", 12.12.2016, N 50, Ст. 7074.

29. Указ Президента РФ от 16 августа 2004 г. № 1082 «Вопросы Министерства обороны Российской Федерации» // СЗ РФ.2004.№ 34.

30. Указ Президента РФ от 30 ноября 1995 г. № 1203 «Об утверждении перечня сведений, отнесенных к государственной тайне» // Российская газета.1995. № 246.

31. Федеральный закон от 04.05.2011 N 99-ФЗ «О лицензировании отдельных видов деятельности» (с изм. и доп., вступ. в силу с 1.03.2019) // СЗ РФ. 09.05.2011. № 19. Ст. 2716.

32. Федеральный закон от 05.03.1992 N 2446-1-ФЗ «О безопасности» // Российская газета № 103. 06.05.1992 .

33. Федеральный Закон от 27 декабря 2002 г. № 184–ФЗ «О техническом регулировании» // Российская газета. 2002. № 245.

34. Федеральный Закон от 7 июля 2003 г. № 126–ФЗ «О связи» // Российская газета. 2003. № 135.

35. Холопова, Е. Н. Информационная безопасность пограничных органов на современном этапе: понятие, структура / Е. Н. Холопова, А. С. Бойцов // Информационное право. – 2019. – № 5. – 9 с.

36. Цибуля, А. Н. К вопросу о состоянии информационной безопасности государства в условиях современных вызовов и угроз / А. Н. Цибуля, В. А. Гордин // Военно-юридический журнал. – 2017. – № 3. – 24 с.

37. Ческидов, М. А. Влияние развития информационной экономики на экономическую безопасность государства // Вестник СГСЭУ. – 2019. – № 3 (47). – С. 28-30.