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 Особенности правового регулирования информационной безопасности в условиях повышенной международной напряженности

Обучающийся В.В. Демихов _____
(Инициалы Фамилия) (личная подпись)

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

Тольятти 2022

Аннотация

Целью данной дипломной работы является изучение существующих механизмов правового регулирования информационной безопасности, выявление проблем и особенностей, возникающих в ходе практического применения как указанных механизмов в целом, так и отдельных правовых норм, в условиях международных санкций и новых угроз безопасности, разработка предложений по изменению существующих правовых механизмов. Было проведено исследование вопросов регулирования информационной безопасности в теоретическом и практическом аспекте, определены границы понятия информационной безопасности, а также состав общественных отношений, которые находятся во взаимном влиянии с состоянием информационной безопасности. На основании границ предмета регулирования был определен перечень основных нормативных правовых актов, проведен их анализ с точки зрения применения на практике. С учетом выявленных проблем и особенностей, были сформулированы предложения по внесению отдельных изменений в нормативные акты, а также намечены пути для возможной концептуальной перестройки системы нормативных правовых актов в сфере информационной безопасности.

Актуальность и оригинальность работы состоит в рассмотрении вопросов правового регулирования не только с сугубо правовой точки зрения, но и во взаимосвязи с техническими особенностями, влияющими на применимость и эффективность правовых механизмов. В рамках работы рассматривается ряд аспектов, существенно обострившихся в 2022 году, не затронутых ранее, либо представлявшихся менее приоритетными.

Областью применения данной работы является сфера разработки нормативных правовых актов по информационной безопасности.

Общие сведения о работе: 89 страниц, разделенных на вводную и заключительную часть, три главы и семь параграфов, общее количество используемой литературы и источников – шестьдесят четыре.

Оглавление

Введение

В рамках настоящего исследования будет рассмотрен вопрос правового регулирования информационной безопасности в Российской Федерации. Будет рассмотрено само понятие информационной безопасности в историческом и теоретическом ключе, рассмотрена многоаспектность данного понятия и сделан акцент на широкий круг общественных отношений, затрагиваемых при рассмотрении вопросов обеспечения информационной безопасности. В исследовании будут освещены вопросы, касающиеся технической стороны темы, правовой стороны, а также особенностей и проблем, возникающих на их стыке и при практическом применении существующих механизмов правового регулирования. Будет подробно рассмотрена существующая нормативная база и выявлены возможные пробелы правового регулирования с точки зрения соответствия современным и актуальным угрозам, возникающим в условиях повышенной международной напряженности.

Актуальность исследования обусловлена тем, что, в настоящее время роль информационных технологий в повседневной деятельности России, органов власти всех уровней, граждан и корпоративного сектора, является крайне высокой. Фактически, можно заметить критическую зависимость нормального функционирования нашего общества от использования информационных технологий. В то же время, нормальное и бесперебойное функционирование системы, широко использующей информационные технологии, представляется невозможным без обеспечения информационной безопасности. Особую важность данным вопросам придает складывающаяся международная обстановка. Некоторые иностранные государства предпринимают явно недружественные шаги в отношении Российской Федерации. К этим недружественным шагам присоединяются некоторые иностранные коммерческие компании, являющиеся разработчиками и поставщиками различного программного обеспечения и аппаратных средств.

Указанные обстоятельства приводят к возникновению новых угроз в области информационной безопасности, которые, в свою очередь, требуют новых оперативных мер реагирования, в том числе и на уровне правового регулирования. Одновременно с этим, некоторые отрасли права, смежные с информационным правом, начинают оказывать повышенное влияние на состояние информационной безопасности. Все это делает проблему комплексной и актуальной в сложившихся условиях.

Объектом исследования являются общественные отношения в области обеспечения информационной безопасности в Российской Федерации.

Предметом исследования являются механизмы правового регулирования информационной безопасности и нормы права, составляющие такие правовые механизмы, а также отдельные способы обеспечения информационной безопасности.

Целью настоящего исследования является изучение теоретической и практической разработанности темы, связанной с правовым регулированием информационной безопасности, выявление проблем и особенностей, возникающих в ходе практического применения существующих механизмов правового регулирования в условиях международных санкций, возникающих новых угроз безопасности, а также разработка отдельных решений по совершенствованию существующих механизмов правового регулирования.

В связи с поставленной целью, возникает потребность в решении ряда задач, а именно:

- рассмотреть сущность понятия «информационная безопасность», его роль и место в современной российской действительности;
- изучить научную литературу и современные исследования по теме;
- изучить основы правового регулирования информационной безопасности в России;
- изучить структуру нормативных правовых актов в сфере обеспечения информационной безопасности в Российской Федерации;

– выявить и проанализировать проблемы существующих правовых механизмов регулирования информационной безопасности;
– предложить способы и пути для решения выявленных проблем в существующих механизмах правового регулирования информационной безопасности.

Методологической базой исследования являются общенаучные методы познания (аналитический метод, включающий в себя принцип системности, объективности, дедукции и индукции), а также частноправовые методы познания (формально-юридический, сравнительно-правовой и другие).

Структура исследования обусловлена его целью и состоит из введения, трех глав основного текста, разделенных по тематическому принципу на семь параграфов, заключения, список используемой литературы и используемых источников

Глава 1 Теоретические основы регулирования информационной безопасности

1.1 Исторические аспекты зарождения и развития информационной безопасности

Начиная исследование любых вопросов, касающихся правового регулирования информационной безопасности, в первую очередь, необходимо определить содержание данного понятия. Информационная безопасность (далее – ИБ) представляет собой многоаспектную категорию, которая может рассматриваться с различных точек зрения. Связано это с широким наполнением составных частей данной категории. А именно: «информация» и «безопасность». В «Словаре русского языка» С.И. Ожегова дано следующее определение информации: «сведения об окружающем мире и протекающих в нем процессах, воспринимаемых человеком или специальным устройством» [30]. Необходимо упомянуть, что понятие «информация» неоднократно рассматривалось в трудах различных авторов и, в связи с этим, имеет большое количество различных определений и подходов. Среди основных подходов к определению информации выделяются: технический (научно-технический), философский, социально-политический (социально-гуманитарный). На основе различных трактовок понятия «информация», как правило, развиваются и строятся соответствующие трактовки понятия «информационная безопасность».

В рамках научно-технического подхода информационная безопасность чаще всего воспринимается как средства, методы и способы защиты информационных систем и данных, обрабатываемых в таких системах. При этом информационные системы рассматриваются в широком смысле, не обязательно как автоматизированные или автоматические. В рамках социально-политического подхода информационная безопасность рассматривается с точки зрения влияния информации на социально-

экономические и социально-политические процессы [1]. При таком подходе информация воспринимается как ресурс, от правильной обработки которого зависит направление развития общества. В этом смысле информационная безопасность выступает в роли совокупности механизмов, в широком смысле задающих правила обращения информации.

Исторически, информационная безопасность как отдельная научная или юридическая категория явно не выделялась до середины XX века. Вместе с тем, сами вопросы регулирования доступа к информации и необходимость контроля над оборотом информации начали возникать уже тогда, когда человеческое общество впервые осознало наличие негативного эффекта от возможного целенаправленного и деструктивного воздействия на потоки информации. Исходя из этого, можно выделить следующие основные этапы в развитии информационной безопасности:

- II век до н.э. – середина XIX века н.э. – использование естественных средств коммуникации (устное общение, письма на бумаге или иных физических носителях), защита указанных средств от несанкционированного получения или подделки (личные печати, подписи, ручные шифры), зарождение и развитие криптографии;
- вторая половина XIX века – начало XX века – начало использования технических средств связи (телеграф, телефон, радиосвязь), применение достижений криптографии на новом техническом уровне, возникновение технологий помехоустойчивого кодирования;
- 10-е – 40-е гг. XX века – развитие технических средств передачи и получения информации, появление и использование технических средств защиты информации, шифровальных машин, первая научная систематизация знаний об ИБ и информации как таковой;
- 40-е – 60-е гг. XX века – появление электронных вычислительных машин, использование первой компьютерной техники в обработке информации, преобладание организационно-административных

методов защиты информации путем ограничения физического доступа к электронным вычислительным машинам (далее – ЭВМ);

- 70-е – 80-е гг. XX века – появление вычислительных сетей и широкое распространение мобильных коммуникационных устройств, создание первых комплексных систем ИБ, объединяющих в себе технические и организационные подходы, создание первых документов стратегического планирования и единых концепций правового регулирования в сфере ИБ;
- конец XX века – наше время – появление и развитие глобальных вычислительных и информационно-коммуникационных сетей, вопросы ИБ регулируются на государственном уровне с использованием всего научно-технического и организационно-административного потенциала государства и различных транснациональных корпораций.

Легко заметить, что понимание и содержание понятия информационной безопасности исторически трансформировалось с учетом появления и внедрения достижений научно-технического прогресса. Одновременно с этим появлялись и механизмы правового регулирования, основанные на оценке возможных угроз и преимуществ, которые возникали при использовании технических средств. Так, на протяжении практически 2000 лет, от древнегреческой «скиталы» и шифра Цезаря, и до начала внедрения телеграфа, сущность обеспечения ИБ сводилась к недопущению прочтения злоумышленником информации, записанной на бумажном или ином физическом носителе. В это же время выделяется первая и основная угроза информационной безопасности, т.н. «человеческий фактор». Любой, даже самый совершенный, механизм ИБ не сможет качественно выполнять свою функцию в случае, если люди, которые посвящены в особенности его функционирования, начинают ему противодействовать. Из этого постепенно выделились два основных направления обеспечения информационной безопасности: применение технических средств и борьба с негативным влиянием человеческого фактора при передаче информации. Вместе с тем, на

данном этапе, как сами технологии, так и юридические механизмы, оставались практически неизменными. Так, для сокрытия или подтверждения подлинности информации использовались различные ручные или примитивные механические шифраторы, печати и подписи, а для уменьшения влияния человеческого фактора – угроза наказания за раскрытие информации, в качестве которого, как правило, выступала смертная казнь.

На втором этапе ключевым стало появление возможности мгновенной передачи информации на большие расстояния с использованием технических средств и, в первую очередь, телеграфа. К исторически возникавшим ранее проблемам защиты информации добавилась угроза физического несанкционированного подключения к линиям связи для перехвата информации, а также возможность искажения информации из-за помех или ошибок приема-передачи. В указанный период времени впервые происходит понимание роли и места технических средств передачи и защиты информации в структуре государства, впервые создаются нормативные правовые акты технического регулирования в области информационной безопасности, определяющие порядок применения технических средств передачи информации и защиты информации при такой передаче [53]. Начиная с этого момента и по сей день вопросы правового регулирования ИБ четко разделяются на регулирование и уменьшение влияния «человеческого фактора», а также на техническое регулирование в области использования технических средств передачи и защиты информации.

Третий временной этап отличался от предыдущего появлением и распространением технологий беспроводной передачи информации (радиотелеграф и радиотелефон). Данный этап характеризуется значительным усложнением уже существовавших механизмов криптографии и криптоанализа. Вместе с тем, также можно выделить и новый фактор обеспечения ИБ: физическую доступность оборудования, осуществляющего криптографические операции, а также передачу информации. В случае наличия физического доступа к такому оборудованию, возникают угрозы

получения несанкционированного доступа к информации за счет потери стойкости используемых алгоритмов. В этой связи начинает выделяться не только технический, но еще и технологический фактор обеспечения информационной безопасности, что также требует соответствующей корректировки нормативно-правовой базы в сфере защиты информации, обеспечения режима доступа к конфиденциальной информации.

Именно с четвертого этапа, характеризующегося появлением первых ЭВМ, можно начинать отсчет современных механизмов обеспечения ИБ как в правовом, так и в техническом и технологическом аспекте. Именно появление ЭВМ обусловило прорыв в скорости обработки информации, что привело к существенным изменениям в криптографической технике и методике. Одновременно с этим увеличилась степень зависимости безопасности в информационной сфере от технологического уровня государства и повысилась степень вовлеченности государства в вопросы обеспечения информационной безопасности.

Пятый этап, характеризующийся появлением вычислительных сетей локального и регионального уровня, приводит к появлению новых угроз, связанных с наличием самой возможности общего доступа к определенной информации. Именно в это время появляется понимание необходимости комплексного рассмотрения ИБ в том виде, в котором оно известно в настоящий момент. В это время возникает отдельное направление «компьютерная безопасность», которая является составной частью информационной безопасности и изучает способы и методы обеспечения безопасности информации, обрабатываемой с помощью ЭВМ и передаваемой с помощью вычислительных сетей. В это же время становится критически важным технологический уровень государства и используемой им компьютерной техники. Одновременно с этим возникает понимание угроз ИБ, возникающих при использовании иностранной элементной базы и комплектующих. Также в это время впервые обращают на себя уязвимости, связанные с ошибками в программном обеспечении (далее – ПО), которые

могут приводить к утечкам или потере информации. Из-за появления компьютерных сетей, становится возможной целенаправленная передача вредоносных данных, появляются первые компьютерные вирусы.

Последний из выделенных этапов характеризуется коренной перестройкой способов и методов обеспечения информационной безопасности. Главным фактором, обусловившим необходимость таких изменений, стало повсеместное распространение глобальной вычислительной сети «Интернет». На данном этапе информация, обрабатываемая с помощью различных средств вычислительной техники универсального назначения и пересылаемая с использованием глобальной вычислительной сети, приобрела крайне высокую ценность и стала важным ресурсом в государственном и международном масштабе. Информация затрагивает практически все сферы жизни общества, государства и даже человечества в целом. В этой связи возникает объективная необходимость построения единой системы обеспечения ИБ, которая будет включать в себя технические, технологические, социальные и юридические механизмы.

Анализируя весь путь исторического развития понятия информационной безопасности, можно утверждать, что данное понятие исторически находится на стыке двух основных направлений человеческой деятельности: технического и социально-гуманитарного. Информационная безопасность естественным образом включает в себя как развитие и применение технических средств, так и различные механизмы регулирования общественных отношений (в первую очередь – правовые и организационные). И именно в этом направлении, с учетом всех факторов, технических, технологических, образовательных, социальных, политических, юридических, должно строиться правовое регулирование в данной сфере на современном этапе развития Российской Федерации.

1.2 Современные исследования в области обеспечения информационной безопасности

Информационная безопасность представляет собой комплексное понятие, которое может рассматриваться с различных точек зрения. Во-первых, это одно из центральных понятий информационного права. С этой точки зрения информационная безопасность может рассматриваться как правовая категория. Во-вторых, информационная безопасность может рассматриваться как понятие, так или иначе используемое в различных технических науках и учебных дисциплинах. К числу таковых могут быть отнесены: криптография, компьютерная безопасность, проектирование информационных систем, управление IT-проектами, компьютерные сети, базы данных и экспертные системы, технологии и методы программирования, технологии сетей связи общего пользования, сети связи специального назначения и многие другие. В указанных науках и учебных дисциплинах информационная безопасность, в первую очередь, рассматривается с точки зрения способов, приемов, методов и технологий, позволяющих обеспечить конфиденциальность, целостность и доступность информации, методов и способов управления доступом к информации с технической точки зрения.

Явное нормативное определение понятия «информационная безопасность» не приводится на уровне федеральных законов. Подобное определение представлено в Доктрине информационной безопасности Российской Федерации (далее – Доктрина), то есть на уровне подзаконного акта – Указа Президента [49]. Согласно определению: «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».

Можно заметить, что уже на уровне данного определения, информационная безопасность рассматривается не обособленно, а в совокупности с такими понятиями, как права и свободы человека и гражданина, качество и уровень жизни граждан, территориальная целостность и социально-экономическое развитие государства, оборона и безопасность государства. Каждое из представленных понятий само по себе характеризуется большим количеством определяющих его факторов и широким спектром затрагиваемых общественных отношений. Можно отметить, что в самом определении констатируется связь информационной безопасности с различными сферами общественных отношений и безопасностью государства в целом.

В случае расширительной трактовки приведенного определения, можно заметить, что информационная безопасность затрагивает не только сферу регулирования информационного права, но и ряд других отраслей права, таких как: административное право, гражданское право, уголовное право, государственные и муниципальные закупки и другие. Таким образом, теоретические и практические работы и исследования в области ИБ должны иметь выраженный междисциплинарный характер. В случае, если работы выполнены с точки зрения правового регулирования, то они, как правило, затрагивают несколько отраслей права.

Выделяется несколько направлений исследований в сфере информационной безопасности. Среди них стоит упомянуть технические и технологические, экономические, правовые, организационные, гуманитарные и образовательные. Несколько отличаются от них концептуальные исследования, которые, как правило, объединяют в себе сразу несколько перечисленных аспектов.

Далее в тексте работы будет приведен ряд примеров современных исследований в области информационной безопасности. Рассмотрение

указанных исследований позволит точнее определить круг вопросов и сфер общественных отношений, на которые оказывает влияние информационная безопасность в рассмотренном ранее понимании. Одновременно с этим, каждый из поднятых вопросов поможет заложить основу для будущего анализа существующих механизмов правового регулирования с точки зрения их соответствия современным реалиям.

В области разработки и практического применения средств защиты различных категорий объектов информатизации, интересен подход А.А. Бурушкина, С.В. Соловьева и А.В. Ступникова. В своей статье «Об актуальности разработки методического обеспечения построения комплексных систем защиты информации в системах электронного документооборота при интеграции разноплатформенных программно-технических средств» [4] авторы раскрывают методические аспекты обеспечения информационной безопасности в системах электронного документооборота. Авторами отмечена высокая сложность разработки и создания эффективной защиты информации при интеграции систем электронного документооборота в работе органов государственной власти. Рассматриваются различные пути решения указанной проблематики.

В поддержку исследований в области электронного документооборота и внедрения электронной подписи, выступает также и И.Д. Королев, отмечающий юридическую значимость электронного документооборота, обусловленную прогрессирующим развитием технологий и повсеместным их распространением, в том числе и в архивной работе. В своей статье «Актуальные проблемы разработки, внедрения и применения систем электронного документооборота в действующих и перспективных автоматизированных системах, обрабатывающих конфиденциальную информацию» [23], автор затрагивает проблемы, возникающие в процессе внедрения электронной подписи в системы, обрабатывающие конфиденциальную информацию, относящуюся к государственной тайне. Среди актуальных проблем исследования, автором выделяется проблема

отсутствия системы электронного документооборота, удовлетворяющего всем требованиям федеральных органов исполнительной власти (далее – ФОИВ). Решение указанной проблемы автор видит в проведении опытно-конструкторских работ в части разработки систем электронного документооборота, позволяющих удовлетворить все требования органов исполнительной власти. Исходя из информации, имеющейся у автора настоящего исследования, можно заметить, что в настоящий момент подобные работы проводятся в части унификации программной платформы, на которой создаются и функционируют используемые ФОИВ информационные системы (с системами электронного документооборота (далее – СЭД), как составной частью информационных систем).

Второй проблемой в статье затронут вопрос массового применения в аппаратной части систем электронного документооборота иностранной элементной базы. Данный вопрос рассматривается в контексте реализации программ импортозамещения.

В части автоматизированной системы военного назначения (далее – АС ВН) И.Д. Королевым отмечена очевидная необходимость в улучшении коммуникации между предприятиями-разработчиками, специализированными организациями, проводящими тематические исследования и функциональными заказчиками, непосредственно эксплуатирующими систему электронного документооборота.

Основной же проблемой применения систем электронного документооборота в АС ВН, автор указывает недостаточную регламентацию применения указанной системы. В данном случае, возникает необходимость разработки концепции применения систем электронного документооборота, и составление на её базе руководящих документов, позволяющих регламентировать применение СЭД в АС ВН. Указанные принципы могут быть масштабированы в части применения в различных органах власти при работе со сведениями, составляющими государственную тайну, а также при работе с не засекреченной информацией.

В области правового регулирования защиты информации при реализации жизненного цикла государственных информационных систем можно отметить работу Н.Р. Гасановой и Д.И. Гусейновой «Системы защиты информации в ГИС» [5]. Авторы работы описывают и анализируют отдельные требования нормативных правовых актов в части организационных и технических мер защиты информации, используемых методов и средств обеспечения безопасности информации в государственных информационных системах (далее – ГИС). Анализируя приведенные в работе аспекты, автор настоящего исследования полагает необходимым отметить, что в существующих на данный момент условиях имеется необходимость в дополнении и уточнении классификационных признаков, на основании которых происходит определение масштаба систем. Кроме того, требуется расширение и уточнение описания на уровне нормативных правовых актов способов влияния технических средств обработки данных на функционирование ГИС, конкретизация мер по предотвращению подобного влияния. Указанные меры должны затрагивать не только нормативные правовые акты в области технического регулирования (как правило - подзаконные), но и нормативные акты, регламентирующие порядок разработки и технической поддержки ГИС. Особе внимание в данной сфере должно быть уделено законодательству в сфере государственных закупок.

В области защиты персональных данных, интересна работа Ю.А. Уваровой «Поддержка принятия решений в аудите информационной безопасности информационных систем персональных данных» [44]. Статья посвящена проблеме поддержки принятия решений при аудите ИБ автоматизированных систем, в которых осуществляется обработка персональных данных. Автор описывает одну из реализаций концепции автоматизированной проверки ИС на предмет наличия угроз безопасности при обработке персональных данных. В работе приводится пример автоматизированного программного средства, реализующего данную концепцию на основе вероятностных алгоритмов. Использование подобных

программных средств позволяет значительно повысить защищенность информационных систем за счет определения уязвимостей. Вместе с тем, в настоящий момент использование подобного программного обеспечения не является обязательным элементом процедуры классификации ГИС и аттестации информационной системы на предмет соответствия требованиям защиты информации. С учетом изложенного, автор исследования представляет целесообразным дополнить нормативные и методические документы, регламентирующие правила и порядок проведения процедуры аттестации и классификации ГИС. Данные вопросы регулируются приказами Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России).

Проблемам защиты персональных данных в медицинских учреждениях посвящен труд А.А. Захарова, Е.А. Оленникова, И.А. Куриленко и Д.В. Серикова «Модернизация информационных систем медицинских учреждений в соответствии с требованиями законодательства по защите врачебной тайны и персональных данных». В приведенной работе обозначены некоторые варианты, позволяющие осуществить переработку ИС медицинского назначения с целью соблюдения требований законодательства о защите персональных данных и иных видов информации ограниченного распространения (в частности – врачебной тайны). При этом сделан важный акцент на оптимизации затрат на подобные мероприятия. Для достижения цели авторами предлагается осуществить изменение логической компоновки ИС медицинского назначения путем разделения на несколько независимых подсистем. Это позволит явным образом выделить элементы, отвечающие за информационную безопасность, а также обеспечить обезличивание обрабатываемых персональных данных.

В продолжение обозначенной ранее проблематики следует обратить внимание на большое количество различных исследований, в которых тема информационной безопасности, так или иначе, затрагивается с технической точки зрения.

В указанной области интересен подход И.О Томилова и А.В. Трифанова, анализирующие применение технологии фаззинга для тестирования компьютерных программ на наличие уязвимости, в результате которой, вместо ожидаемых входных данных, в программу передаются случайные или специально сформированные данные. В качестве входных данных для тестирования, автором предлагается использовать обрабатываемые приложением файлы с целью выявления уязвимостей [43].

В статье А.В. Барабанова, А.С. Маркова и А.А. Фадин «Оценка возможности выявления уязвимостей программного кода при отсутствии исходных текстов программ» [2] также исследуются особенности проведения аудита безопасности, а также аттестационных и сертификационных испытаний программного обеспечения при условии отсутствия исходных кодов. Авторами показана возможность частично автоматического выявления уязвимостей, закладок и ошибок, а также подготовки отчетов сертификационных испытаний по заранее заданным шаблонам и наборам параметров проверок.

Проблема информационной безопасности в области компьютерных атак подробно описана в научном труде А.Ф. Белого и С.М. Климова «Алгоритм принятия решений по оценке функциональной устойчивости средств автоматизации в условиях компьютерных атак» [3]. В статье рассматриваются отдельные способы и методы оценки функциональной устойчивости программных продуктов в условиях интенсивных компьютерных атак. В основе лежит метод расчёта рисков обеспечения устойчивости по матрице рисков. Кроме того, предложен механизм принятия решений на основе данных оценки функциональной устойчивости.

В статье О.Н. Федорец «Комбинированная система защиты программного обеспечения от несанкционированного использования» [64] рассмотрена система, осуществляющая проверку подлинности и целостности программного обеспечения с целью перекрытия угроз информационной

безопасности через несанкционированное использование программного обеспечения.

В статье А.Н. Кулакова и Е.Б. Маховенко «Криптографические методы обеспечения информационной безопасности на основе идентификаторов в широковещательных системах» [25] предлагается идея аппаратной реализации прототипа системы, обеспечивающей широковещательную передачу данных в условиях незащищенного канала. С целью достижения высоких системных показателей эффективности, авторы исследования предлагают использование криптосистем с открытым ключом на базе идентификаторов. Эффект реализации таких криптосистем достигается путем оптимизации процедуры вычисления билинейного отображения.

Нельзя не заметить, что рассматриваемая тема во многом затронута не только с технической точки зрения, но и с точки зрения анализа механизмов правового регулирования. В диссертационном исследовании Г.О. Крылова «Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации» [24] автор фактически впервые проводит анализ зарубежных механизмов обеспечения информационной безопасности с точки зрения возможностей их реализации в рамках российской правовой системы. Некоторые вопросы, концептуально затронутые в рамках исследования, впоследствии были реализованы при подготовке Доктрины информационной безопасности России 2016 года.

В продолжение темы использования международного опыта и норм международного права в сфере информационной безопасности можно отметить диссертационное исследование Е. С. Зиновьевой «Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы» [15]. Автор рассматривает существующие и перспективные механизмы обеспечения информационной безопасности, основанные на нормах международного права, проблемы и развитие международного сотрудничества в данной сфере. Указанное исследование дает общее представление об используемых международно-правовых

механизмах обеспечения национальной безопасности, описывает реализованные и возможные пути имплементации норм международного права в российское законодательство об информационной безопасности. Однако, в то же время, изложенные там подходы, во многом, оказываются неработоспособны в современных условиях, когда ряд иностранных государств оказывает на Российскую Федерацию целенаправленное давление и ограничивает сотрудничество. Приведенные примеры исследований во многом показательны с той точки зрения, что использовавшиеся ранее подходы к правовому регулированию информационной безопасности в некоторой мере теряют актуальность в современных условиях из-за политически мотивированных ограничений в применении международных механизмов.

Рассматривая теоретическую разработанность темы правового регулирования информационной безопасности, нельзя не отметить ряд исследований, направленных на различные аспекты регулирования. В частности, некоторые исследования подтверждают ярко выраженный межотраслевой характер регулирования. В диссертационном исследовании А.С. Жарова «Конституционно-правовое регулирование информационной безопасности личности в Российской Федерации» [12] фактически впервые рассматриваются вопросы и проблемы обеспечения информационной безопасности личности именно в конституционно-правовом аспекте. Можно заметить, что указанное исследование затрагивает только одну сторону информационной безопасности – информационная безопасность личности. В то же время, как было показано ранее, понятие информационной безопасности намного шире. Следует констатировать ограниченность теоретической разработанности темы в отношении, например, конституционно-правового аспекта информационной безопасности государства в лице функционирования его органов. В качестве другого примера можно привести диссертационное исследование М. А. Ефремовой «Уголовно-правовая охрана информационной безопасности» [10]. В ходе

исследования, автором было дано детальное описание различных преступлений, посягающих на информационную безопасность личности и Российской Федерации, конкретизированы механизмы уголовно-правовой охраны права на информацию и защиты информации от неправомерного доступа, безопасности информационно-телекоммуникационных технологий.

Итак, в контексте темы данного исследования, можно заметить, что в России наблюдается устойчивый тренд на развитие научного и технического потенциала в области обеспечения информационной безопасности. Развитие научно-технической составляющей в целом подкрепляется существующей нормативно-правовой базой и правовыми механизмами, регулирующими использование технических средств в области обеспечения ИБ.

Можно выделить следующие основные технические направления, по которым ведутся исследования в области информационной безопасности:

- организационно-технические способы комплексной защиты объектов информатизации;
- продукция для проведения проверки программного обеспечения на предмет наличия потенциально опасных незадекларированных возможностей;
- исследования в области практической криптографии, криптоанализа и стеганографии;
- унификация программных платформ для разработки программного обеспечения для нужд государственных и муниципальных органов;
- методология обнаружения угроз информационной безопасности;
- технологии построения и эксплуатации защищенных виртуальных частных сетей;
- технологии защиты линий связи общего и специального назначения;
- методология обеспечения информационной и психологической безопасности личности;

– разработки в области создания отечественных электронных компонентов для использования в аппаратной части ГИС;
– методы и способы выявления незадекларированных возможностей и несанкционированных изменений в программном обеспечении;
– разработки и технологии защиты персональных данных при их автоматизированной и автоматической обработке.

Следует обратить внимание, что техническая составляющая исследований в области ИБ в целом динамично развивается и оперативно подстраивается под изменяющиеся условия действительности. Одновременно с этим стоит заметить, что ранее проведенные исследования в области правового регулирования информационной безопасности в некоторых аспектах теряют актуальность в современных условиях, поскольку они не в полной мере учитывают существующие в настоящее время угрозы для Российской Федерации. Для решения указанных вопросов в 2022 году активизируются новые исследовательские работы, которые призваны выработать механизмы, позволяющие нейтрализовать упомянутые новые угрозы.

1.3 Информационная безопасность в различных сферах общественных отношений

Ранее в ходе рассмотрения и анализа существующих работ по информационной безопасности было показано, что понятие информационной безопасности имеет ярко выраженный междисциплинарный характер, а само понятие находится на стыке различных технических и гуманитарных наук. Современные исследования содержат различную классификацию объектов, на которые направлена информационная безопасность. Одними из таких объектов могут выступать различные сферы общественных отношений. В данном контексте слово «направлена» следует понимать как с точки зрения того, что определенные сферы общественных отношений зависят от уровня

обеспеченности информационной безопасности, так и наоборот, с точки зрения того, что указанные сферы общественных отношений своими потребностями оказывают влияние на развитие механизмов информационной безопасности. В случае построения системы объектов информационной безопасности как различных сфер общественных отношений, появляется возможность явным образом установить структуру взаимосвязей отраслей права, задействованных в обеспечении механизмов информационной безопасности. На основании подобной структуры впоследствии можно будет выстроить общую систему нормативных правовых актов в сфере информационной безопасности и выделить систему государственных органов и наиболее важных частных предприятий, задействованных в обеспечении информационной безопасности.

В пп.1 п.5 Стратегии национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [51] (далее - Стратегия) раскрывается понятие национальной безопасности Российской Федерации. Согласно определению: «национальная безопасность Российской Федерации – это состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны».

Из определения национальной безопасности РФ непосредственно можно выделить следующие основные направления обеспечения безопасности:

- безопасность личности (реализация прав и свобод граждан);
- безопасность общества (качество и уровень жизни, гражданский мир и согласие);

– безопасность государства (суверенитет, независимость, государственная целостность, социально-экономическое развитие).

Согласно п. 26 Стратегии, защита национальных интересов РФ обеспечивается за счет реализации следующих стратегических национальных приоритетов:

– сбережение народа России и развитие человеческого потенциала;
– оборона страны;
– государственная и общественная безопасность;
– информационная безопасность;
– экономическая безопасность;
– научно-технологическое развитие;
– экологическая безопасность и рациональное природопользование;
– защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти;
– стратегическая стабильность и взаимовыгодное международное сотрудничество.

Таким образом, Стратегия национальной безопасности определяет информационную безопасность в качестве одного из стратегических национальных приоритетов России.

Согласно п.56 Стратегии, целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве. Само понятие «информационное пространство» не имеет нормативного определения ни в тексте Стратегии, ни в других нормативных правовых актах. Вместе с тем, данное понятие достаточно полно раскрывается в различных научных трудах. Например, И.А. Добровольская выделяет два основных подхода к определению понятия «информационное пространство» - технический и гуманитарный. Согласно техническому подходу, информационное пространство – это совокупность систем, осуществляющих обработку, хранение и передачу информации с

применением различных технических средств и ресурсов. В то же время, гуманитарный подход определяет информационное пространство как совокупность знаний и информации, формирующейся и постоянно изменяющейся в процессе эволюции общества [9]. Объединяя указанные подходы, можно сделать вывод о том, что информационное пространство представляет собой интегрированную среду хранения, передачи и распространения информации обо всех сферах жизнедеятельности человеческого общества. Опираясь на такое определение, в контексте заявленных в Стратегии целей обеспечения информационной безопасности, можно констатировать, что степень обеспечения информационной безопасности может оказывать влияние на широкий спектр различных общественных отношений, так или иначе использующих в своей деятельности информационные технологии. Данное утверждение находит свое подтверждение при анализе п. 57 Стратегии, где заявлены задачи, решение которых должно позволить достигнуть целей обеспечения ИБ. Фактически, перечисленные в Стратегии задачи информационной безопасности, так или иначе, охватывают все основные направления обеспечения безопасности, перечисленные выше.

Некоторые исследования в области правового регулирования информационной безопасности посвящены анализу системы нормативных правовых актов информационного права, а также определения роли и места самого понятия информационной безопасности. В числе таковых можно упомянуть статьи Л.Г. Лименько «Отдельные аспекты правового регулирования информационной безопасности» [26] и А. И. Николаева «Правовое обеспечение информационной безопасности РФ»[29]. Авторами указанных статей приводится описание структуры правового регулирования в области информационной безопасности, анализ основных нормативных актов информационного права, описывается система государственных органов, ответственных за выработку и реализацию государственной политики в области информационной безопасности. Наиболее значимым

можно считать обоснование идеи кодификации законодательства в информационной сфере, которое должно привести к созданию Информационного кодекса. Вместе с тем, некоторые авторские тезисы являются, как минимум, спорными. Так, авторы статей рассматривают информационную безопасность в качестве института информационного права. С подобным подходом трудно согласиться, поскольку приведенный ранее анализ понятия «информационная безопасность», рассмотрение его многочисленных аспектов и проявлений, выделение факторов, влияющих на информационную безопасность, показывает, что нормы, регулирующие информационную безопасность, не обособлены в рамках отрасли информационного права. Кроме того, в отношении информационной безопасности нельзя сказать, что она представляет собой относительно небольшую и устойчивую группу правовых норм. Как было показано ранее и будет подтверждено далее в ходе настоящего исследования, информационная безопасность представляет собой междисциплинарное и межотраслевое понятие, не имеющее четких границ, а нормы, которые оказывают влияние на информационную безопасность, относятся к различным отраслям права и регулируют принципиально разные группы общественных отношений. Более того, система обеспечения информационной безопасности содержит в себе как регуляторные, как и охранительные нормы. С учетом изложенного, с определенной долей условности, информационную безопасность можно считать комплексным межотраслевым институтом права. Условность такого рассмотрения диктуется еще и тем, что информационная безопасность как правовая категория содержит в себе элементы, как частного, так и публичного права.

Анализ сфер общественных отношений, на которые оказывает непосредственное влияние информационная безопасность, можно начать с рассмотрения п. 48 – 57 Стратегии национальной безопасности РФ. Исходя из описанных задач государственной политики в сфере обеспечения ИБ, а также опираясь на их конкретизацию в тексте п. 10-29 Доктрины

информационной безопасности РФ, можно выделить следующие основные сферы общественных отношений, критически зависящие от состояния механизмов информационной безопасности:

- организация вооруженной защиты Российской Федерации;
- организация борьбы с проявлениями терроризма и экстремизма;
- организация контрразведывательной деятельности;
- организация работы со сведениями, составляющими государственную тайну;
- обеспечение неприкосновенности частной жизни;
- организация защиты персональных данных физических лиц;
- взаимодействие органов публичной власти с гражданами и организациями;
- организация культурной деятельности и развития культуры в РФ;
- организация работы сетей связи общего и специального назначения;
- организация деятельности средств массовой информации (далее – СМИ);
- организация работы отдельных отраслей промышленности в РФ;
- организация работы в сфере энергетики;
- организация функционирования судебной системы РФ;
- организация работы финансового и банковского сектора;
- организация работы системы образования в РФ;
- организация работы в сфере разработки программного обеспечения общего и специального назначения;
- организация международного взаимодействия с иностранными государствами;
- организация законотворческой деятельности;
- организация повседневной деятельности правоохранительных органов;
- государственные и муниципальные закупки.

Подчеркнем, что, так или иначе, информационная безопасность оказывает влияние на все без исключения сферы общественных отношений. Подобное влияние является неотъемлемой характеристикой современного цифрового общества. Вместе с тем, рассмотрение влияния на все сферы общественных отношений в РФ, а также на правовую систему РФ в целом выходит за пределы предмета данного исследования. По этой причине в представленный выше список вошли только те сферы, которые не просто сами зависят от состояния информационной безопасности, но и являются ее составной частью и в определенной мере задают направление развития технических и правовых механизмов информационной безопасности. То есть как раз те сферы, на которые направлена информационная безопасность в обозначенном ранее смысле.

Исходя из перечисленных основных сфер общественной жизни, а также учитывая положения п.33 Доктрины информационной безопасности, можно выделить перечень органов и организаций Российской Федерации, оказывающих преимущественное влияние на состояние информационной безопасности. Указанный перечень можно разделить на две основные группы: государственные органы (и государственные предприятия) и коммерческие организации.

Первая группа представлена следующим составом:

- Президент РФ
- органы исполнительной власти:
- органы законодательной власти (палаты Федерального Собрания)
- органы судебной власти (судебная система РФ)
- центральный Банк РФ
- органы власти субъектов Федерации и органы местного самоуправления.

В составе органов исполнительной власти можно выделить две основные подгруппы:

– органы власти, руководство деятельностью которых осуществляет Президент РФ;
– органы власти, руководство деятельностью которых осуществляет Правительство РФ.

К первой подгруппе можно отнести следующие органы:

– Министерство обороны РФ (ФСТЭК России):
– ФСБ России (НКЦКИ, ГосСОПКА):
– МВД России
– МИД России
– ФСО России
– Росгвардия

Вторая составляющая представлена следующими основными элементами:

– Минцифры России (Роскомнадзор, ФГУП ГРЧЦ);
– Минфин России;
– Минпромторг России;
– Минкультуры России;
– Минэкономразвития России (Роспатент);
– Минобрнауки России.

Группа коммерческих организаций состоит из различных предприятий и организаций всех организационно-правовых форм и форм собственности и включает в себя организации – разработчики программного обеспечения и организации – производители аппаратных компонентов.

Рассмотрим подробнее отдельные элементы структуры, оказывающие наиболее важное влияние на состояние информационной безопасности.

Ключевым элементом, оказывающим влияние на информационную безопасность, безусловно, является Президент РФ. В соответствии с п.32 Доктрины ИБ, он определяет состав системы обеспечения информационной безопасности. Одновременно с этим, в п.31 Доктрины ИБ подчеркнуто, что

система обеспечения ИБ строится на основе разграничения полномочий всех ее структурных элементов. Таким образом, именно Президенту принадлежит одна из ведущих ролей в определении объема полномочий каждого государственного органа в сфере обеспечения информационной безопасности.

Одним из важнейших элементов структуры является ФСБ России. Согласно ст. 11.2 Федерального закона от 03.04.1995 №40-ФЗ «О федеральной службе безопасности», на службу возложены полномочия по формированию и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств [54]. Помимо этого, согласно п.1 Указа Президента Российской Федерации от 22.12.2017 №60 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации», ФСБ России является федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации [50]. В этой же связи можно упомянуть НКЦКИ и центры Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак (далее – ГосСОПКА), которые осуществляют свою деятельность в соответствии с Положением о Национальном координационном центре по компьютерным инцидентам, утвержденным Приказом ФСБ России от 24.07.2018 №366 «О Национальном координационном центре по компьютерным инцидентам» [40].

Рассматривая ключевые элементы структуры, нельзя не упомянуть ФСТЭК России. Данная служба играет важную роль в осуществлении технического регулирования в области информационной безопасности. В частности, именно приказами ФСТЭК осуществляется определение

требований к информационным системам, применяющимся в государственных органах и подведомственных им государственных предприятиях, а также контроль над выполнением указанных требований в ходе различных аттестаций и сертификаций. Кроме того, служба осуществляет ряд полномочий, связанных с осуществлением экспортного контроля. В качестве примера осуществления экспортного контроля для целей обеспечения информационной безопасности можно привести зарубежное использование защищенных носителей для контейнеров электронной цифровой подписи с аппаратной реализацией или поддержкой алгоритмов ГОСТ Р 34.10-2012 и ГОСТ Р 34.11-2012.

Значительная роль МВД России в структуре органов, оказывающих влияние на информационную безопасность, заключается в том, что предварительное расследование (как в форме предварительного следствия, так и в форме дознания) по большой части преступлений, которые посягают на отношения в сфере информационной безопасности, осуществляется именно МВД. Так, М.А. Ефремова выделяет 3 группы преступлений, посягающих на отношения в сфере информационной безопасности (в скобках указан орган, осуществляющий предварительное расследование).

Первая группа включает в себя ст. 137 (СК РФ), 138 (СК РФ), 140 (СК РФ), 144 (СК РФ), 155 (МВД), 183 (МВД), 237 (СК РФ), 283 (ФСБ), 283.1 (ФСБ), 284 (ФСБ), 310 (все), 311 (ФССП РФ, иногда – остальные по ч.6 ст. 151 УПК РФ), 320 (СК РФ, иногда – остальные по ч.6 ст. 151 УПК РФ) УК РФ – преступления против права на информацию;

Вторая группа состоит из ст. 324 (МВД), 325 (МВД), 327 (МВД) УК РФ – преступления против безопасности информационных ресурсов;

Третья группа содержит ст. 272 (МВД), 273 (МВД) УК РФ – преступления против безопасности информационно-телекоммуникационных технологий [10].

С учетом положений ст. 150-151 УПК РФ, можно заметить, что в первой группе МВД может участвовать в производстве предварительного

расследования по 5 статьям УК из 13, во второй группе по 3 статьям УК из 3 и в третьей группе по 2 статьям УК из 2, а всего в 10 статьях УК из 18, то есть более половины.

ФСО России играет значительную роль в обеспечении информационной безопасности, поскольку является органом, обеспечивающим нормальное функционирование системы правительственной связи. Кроме того, ФСО является организатором системы межведомственного электронного документооборота, объединяющей между собой информационные системы различных органов власти всех уровней при обмене информацией, не содержащей сведений, составляющих государственную тайну.

Ключевую роль в обеспечении информационной безопасности в России играет Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минцифры России). Именно в ведении указанного министерства находится реализация большей части государственных программ, направленных на построение цифрового общества, внедрение информационных технологий в различные сферы жизни. Среди таковых можно отметить государственные программы «Информационное общество», «Цифровая экономика», «Электронное правительство» и другие. Также к полномочиям Минцифры отнесено ведение реестра отечественного ПО. Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) является органом, подведомственным Минцифры России. Его роль в обеспечении информационной безопасности заключается в том, что именно Роскомнадзор отвечает за выработку и практическое применение механизмов правового регулирования, направленных на обеспечение защиты персональных данных, контроля и надзора за деятельностью операторов связи, СМИ, а также в информационно-телекоммуникационной сети «Интернет». Роль Роскомнадзора в сфере обеспечения информационных аспектов

национальной безопасности, таким образом, в нашем государстве является исключительно важной.

Ранее при рассмотрении вопросов, касающихся современных исследований в области ИБ, была отмечена значительная роль некоторых коммерческих предприятий. К таковым можно отнести любые предприятия и организации любых форм собственности, осуществляющие разработку программного обеспечения, а также осуществляющих производство аппаратных компонентов для любых электронных вычислительных (компьютерных) систем.

Рассмотренная в рамках настоящего параграфа структура общественных отношений, имеющих взаимное влияние с состоянием информационной безопасности, а также выделенная система органов и организаций, может служить основой для построения структуры нормативных правовых актов в сфере информационной безопасности, что будет подробно рассмотрено далее. В данной связи можно подчеркнуть, что ярко выраженный межотраслевой характер самого понятия информационной безопасности будет иметь решающее значение в структуре механизмов правового регулирования.

Глава 2 Механизмы правового регулирования информационной безопасности в Российской Федерации

2.1 Законодательство в области информационной безопасности

В предыдущей главе данного исследования было показано, что понятие информационной безопасности является межотраслевым и междисциплинарным. Из этого следует, что правовое регулирование информационной безопасности не ограничивается какой-то одной отраслью права. Исходя из этого, при построении системы нормативных правовых актов в области информационной безопасности будут затронуты различные отрасли и подотрасли права.

Основным источником права в сфере информационной безопасности, вне всякого сомнения, является Конституция Российской Федерации [22]. Она закрепляет основные права и обязанности, которые далее реализуются и конкретизируется специальными правовыми механизмами информационной безопасности. К числу таковых относятся:

- право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений (ст. 23 Конституции);
- запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия (ст. 24 Конституции);
- право свободно искать, получать, передавать, производить и распространять информацию любым законным способом (ст. 29 Конституции);
- перечень сведений, составляющих государственную тайну, определяется федеральным законом (ст. 29 Конституции).

При рассмотрении правовых механизмов, регулирующих те или иные сферы общественных отношений, как правило, затрагиваются также и нормы

международного права. Согласно ч.4 ст. 15 Конституции Российской Федерации, общепризнанные принципы и нормы международного права и международные договоры Российской Федерации являются составной частью ее правовой системы и имеют приоритет над национальным законодательством. Вместе с тем, детальное рассмотрение различных международно-правовых механизмов в сфере информационной безопасности показывает, что на международном уровне не присутствует всеобъемлющих и детальных механизмов, которые могли бы в чистом виде эффективно применяться в реалиях российской правовой системы.

Действующее международное право определяет стандартные нормы защиты информации, однако они не в полной мере учитывают, что каждое государство имеет свои индивидуальные особенности в историческом, экономическом и политическом развитии. Так, в ст. 10 Европейской Конвенции о защите прав человека и основных свобод от 04.11.1950 установлено, что «каждый имеет право свободно выражать свое мнение [20]. Это право включает свободу придерживаться своего мнения и свободу получать и распространять информацию и идеи без какого-либо вмешательства со стороны публичных властей и независимо от государственных границ», однако, по мнению С.И. Гутника: «вполне очевидно, что это право не является абсолютным, поскольку существует множество обстоятельств, при которых свободное движение и обмен информацией могут наносить значительный ущерб государству и обществу в целом. Последствия от свободного движения негативной информации могут быть несоизмеримо велики в мировом информационном пространстве, что, в свою очередь, создаёт угрозу стабильности и безопасности мирового сообщества и всей человеческой цивилизации» [8].

Важным аспектом в сохранении национальной информационной безопасности является и тот факт, что Россия является многонациональной страной, что делает её уникальной, но в тоже время и более уязвимой по отношению к мононациональным странам. Как отметили З.А. Жаде и З.Ю.

Хуако, «важный аспект предупреждения межэтнической напряженности и обеспечения информационной безопасности- это национально ориентированная позиция всех структур политической системы: институтов гражданского общества, политических партий, средств массовой информации, общественных и религиозных объединений, экспертного сообщества, а также национальных культурных образований» [11]. Суть высказанных предложений заключается в том, что необходима разработка четкой информационной политики. Это позволит проводить профилактику проявления экстремизма, гармонизировать общественные отношения.

В целом, следует заметить, что в сфере обеспечения информационной безопасности несомненный приоритет по степени охвата регулируемых отношений имеет именно национальное законодательство, а не международно-правовые механизмы. Связано это с влиянием национальной специфики в данной сфере, с высокой степенью анонимности при реализации угроз информационной безопасности, а также со значительным влиянием политических и конъюнктурных факторов и что делает невозможным эффективное применение международно-правовых механизмов. Рассмотренная ситуация в определенной мере схожа с применением международно-правовых механизмов в сфере борьбы с терроризмом, где также велико отрицательное влияние политических факторов. Однако, следует заметить, что некоторые российские нормативные акты различных уровней содержат в себе отдельные положения и нормы из актов международного права, а отдельные акты технического регулирования опираются на международные стандарты. Таким образом, влияние международного права в сфере информационной безопасности РФ можно считать опосредованным.

Построение системы нормативных правовых актов, регулирующих отношения в сфере информационной безопасности, проведем, указывая перечень наиболее важных, на наш взгляд, источников в соответствии с их местом в иерархии и с разделением по органу, осуществившему принятие

соответствующего акта, опираясь на перечень ранее обозначенных ключевых органов и организаций. Иерархия будет построена по юридической силе соответствующего нормативного акта.

Отношения в сфере обеспечения ИБ регулируются нормативными правовыми актами следующих уровней, в порядке убывания юридической силы:

- конституция РФ;
- федеральные законы;
- указы президента;
- постановления правительства РФ;
- нормативные акты федеральных органов исполнительной власти;
- нормативные акты уровня субъектов РФ;
- нормативные акты муниципального уровня;
- локальные нормативные акты организаций и предприятий.

При рассмотрении приведенной иерархии следует отметить следующие отличительные черты:

- в системе отсутствуют нормативные правовые акты уровня федерального конституционного закона;
- любые нормативные акты федерального уровня имеют большую юридическую силу, чем акты регионального или муниципального уровня.

Действительно, в настоящий момент в РФ отсутствуют нормативные правовые акты в сфере информационной безопасности уровня федерального конституционного закона. Безусловно, некоторые из них, такие как, например, Федеральный конституционный закон от 06.11.2020 № 4-ФКЗ «О Правительстве Российской Федерации» или Федеральный конституционный закон от 31.12.1996 № 1-ФКЗ «О судебной системе Российской Федерации», содержат отдельные нормы, косвенно влияющие на состояние ИБ. Вместе с

тем, степень данного влияния не является определяющей. По этой причине изучение данных вопросов выходит за рамки настоящего исследования.

Вопрос о приоритете федерального законодательства в сфере информационной безопасности над региональным и муниципальным законодательством имеет как объективные предпосылки, так и явную правовую основу. Согласно п. «м» ст. 71 Конституции РФ, обеспечение безопасности личности, общества и государства при применении информационных технологий, обороте цифровых данных отнесено к ведению Российской Федерации. Согласно ч.1 ст. 76 Конституции РФ, по предметам ведения РФ принимаются федеральные законы, имеющие прямое действие на всей территории Российской Федерации. Согласно ч.5 той же статьи, законы и иные нормативные акты субъектов РФ не могут противоречить федеральным законам, принятым по вопросам, отнесенным к ведению РФ. В случае противоречия между федеральным законом и иным актов, изданным в Российской Федерации, действует федеральный закон. Указанное положение в полной мере относится к ситуации, когда в федеральных законах содержатся бланкетные нормы, отсылающие к различным подзаконным актам федерального уровня. Из этого следует, что любые подзаконные нормативные правовые акты федерального уровня в сфере ИБ, принятые в соответствии с федеральными законами и не противоречащие им, также имеют приоритет над нормативными актами субъектов РФ. Рассмотренная ситуация представляется автору исследования полностью обоснованной, поскольку позволяет осуществлять выработку единых подходов к осуществлению регулирования в сфере информационной безопасности. В данном случае указанная особенность представляется более приоритетной, чем учет региональной специфики, поскольку позволяет задействовать более развитый потенциал в научной и технической сфере, а также составить целостную картину состояния защищенности в сфере обеспечения информационной безопасности на всей территории Российской Федерации. Учитывая высокую связность компьютерных систем и высокую

скорость передачи информации, явная поддержка региональных различий в подходах представляется скорее вредной для целей обеспечения ИБ. Состояние любого локального узла информационной системы масштаба всей страны потенциально может оказывать свое негативное влияние на систему в целом.

В настоящее время, информационную безопасность принято отождествлять именно с угрозами в сфере компьютерных технологий в широком смысле (в программной и аппаратной части), и в данной области основополагающим правовым актом следует выделить Федеральный закон «Об информации, информатизации и защите информации», отражающий и конкретизирующий основные догмы Конституции РФ в сфере информационной безопасности. Так, в соответствии со ст. 1 указанного нормативного акта [58], «настоящий Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации;
- применении информационных технологий;
- обеспечении защиты информации».

Нельзя не заострить внимание на том, что до принятия актуального законодательства в сфере информационной безопасности, в России также действовали нормы, регулирующие отношения в исследуемой сфере. Федеральный закон РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» заменил действовавший до этого Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации». Целью разработки и последующего принятия Закона 2006 года явилась ратификация РФ в 2005 году Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года [21]. Как отмечают А.И Савченко и А.Н. Федоров [19], создание Закона «позволило:

- приблизить законодательство РФ к международной практике регулирования информационных отношений;
- устранить пробел в регулировании передачи информации как объекта гражданских прав;
- унифицировать, как с понятийной, так и с содержательной точки зрения, принципы и правила регулирования информационных отношений;
- заложить эффективную правовую основу создания и эксплуатации государственных и иных информационных систем;
- законодательно закрепить принципы использования информационно-телекоммуникационных сетей, в т.ч. при международном информационном обмене;
- установить основные правила и перечень способов защиты публичных и гражданских прав на информацию, защиты самой информации путем принятия основных правовых, организационных и технических (программно-технических) мер по ее защите».

Федеральный закон «Об информации, информационных технологиях и о защите информации» является центральным нормативным правовым актом информационного права, дает определение ряду категорий информационного права, а также задает базовые принципы механизмов правового регулирования данной отрасли права. На основе изложенных в законе принципов выстраивается, в числе прочего, и система нормативных правовых актов в области информационной безопасности.

Большое значение для построения правовых механизмов ИБ имеет Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности» [60]. В нем определяются основные принципы, содержание и направленность государственной политики по обеспечению безопасности государства во всех сферах, включая и сферу информационной безопасности. Данным нормативным актом осуществляется наиболее общее распределение

полномочий в сфере обеспечения безопасности между органами власти. В частности, именно на основании ст. 8 Федерального закона от 28.12.2010 №390-ФЗ «О безопасности» [60] Указы Президента Российской Федерации встраиваются в систему нормативных правовых актов в сфере безопасности (и информационной безопасности – как частный случай), а сам Президент наделяется широкими полномочиями и возглавляет систему органов, обеспечивающих безопасность во всех сферах.

Важным юридическим документом, позволяющим обеспечить баланс интересов государства, общества и личности, а также создать условия для гармоничного развития национальной информационной инфраструктуры, является Закон РФ от 27.12.1991 № 2124-1 «О средствах массовой информации», в котором отображаются основные понятия СМИ, организация их деятельности, а также порядок распространения информации и ответственность за нарушение законодательства о средствах массовой информации. Данным законом охраняется право на неприемлемость цензуры и четко прописаны моменты, когда не допускается массовое использование информации. К таким аспектам относятся недопустимость использования СМИ «в целях совершения уголовно наказуемых деяний, для разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань, а также запрещается использование в радио-, теле-, видео-, кинопрограммах, документальных и художественных фильмах, а также в информационных компьютерных файлах и программах обработки информационных текстов, относящихся к специальным средствам массовой информации, скрытых вставок и иных технических приемов и способов распространения информации, воздействующих на подсознание людей и (или) оказывающих

вредное влияние на их здоровье, а равно распространение информации об общественном объединении или иной организации, включенных в опубликованный перечень общественных и религиозных объединений, иных организаций, в отношении которых, судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным Федеральным законом от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» без указания на то, что соответствующее общественное объединение или иная организация ликвидированы или их деятельность запрещена» [13].

Безусловно, любая информация может иметь определенную ценность, однако, некоторая является настолько важной, что получение несанкционированного доступа к ней может привести к угрозам безопасности государства различной степени тяжести и в различных сферах. Из-за этого общество вынуждено создавать разнообразные системы и механизмы защиты информации, технические, организационные и правовые, регулирующие порядок оборота информации с ограниченным доступом (конфиденциальной информации) в Российской Федерации.

Проблема защиты конфиденциальной информации, как для организаций любой формы собственности, так и органов власти, в настоящее время стоит достаточно остро, поскольку, последняя является важнейшей составляющей любых информационных отношений. Вопросы правового регулирования использования и распространения информации в последнее время занимают одно из значительных мест в юридической литературе. Это обусловлено, прежде всего, тем, что содержание юридически значимой тайны заключается в том, что ее предмет образует информация, не предназначенная для широкого круга лиц, а ее разглашение может повлечь нежелательные последствия для владельцев и обладателей тайны.

Рассматривая организацию защиты отдельных видов конфиденциальной информации, можно констатировать, что для каждого вида конфиденциальной информации, государством разработан отдельный

правовой механизм ее защиты, например, персональные данные защищаются в соответствии с положениями Федерального Закона от 27.07.2006 № 152-ФЗ «О персональных данных», целью которого является «обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну» (ст. 6). К персональным данным, в соответствии со ст. 3 указанного нормативного акта, относится «любая информация, относящаяся к прямо или косвенно определённому или определяемому физическому лицу (субъекту персональных данных)» [59]. Тема организации защиты персональных данных и регулирования их обработки обладает высокой общественной значимостью и высоким уровнем потенциального вреда от неправомерной обработки персональных данных. В этой связи, можно заметить, что механизмы правового регулирования обработки персональных данных постоянно развиваются, а законодательными органами власти России предпринимаются оперативные меры по реагированию на вновь возникающие угрозы. Так, 06.04.2022 в Государственную Думу группой депутатов был внесен законопроект № 101234-8 «О внесении изменений в Федеральный закон «О персональных данных» и иные законодательные акты Российской Федерации по вопросам защиты прав субъектов персональных данных». В настоящий момент Федеральный закон принят под номером 266-ФЗ от 14.07.2022. Согласно тексту закона, вводятся дополнительные механизмы правового регулирования трансграничной передачи персональных данных, реагирования на инциденты, связанные с утечкой персональных данных, а также расширяется перечень полномочий Роскомнадзора в сфере контроля и надзора за обработкой персональных данных [63].

Помимо правового регулирования обработки персональных данных, к обеспечению информационной безопасности также имеют прямое отношение механизмы регулирования работы с иными видами конфиденциальной информации.

Что касается механизма осуществления защиты тайны следствия и судопроизводства, то сохранение в тайне указанной информации связано непосредственно с интересами производства предварительного расследования по уголовным делам. Связано данное положение с тем, что подобная информация касается не только производимых следственных действий, но и доказательной базы, хода расследования, круга подозреваемых лиц, свидетелей и иных лиц, участвующих в расследовании. На основании ст. 161 УПК РФ, «данные предварительного расследования могут быть преданы гласности лишь с разрешения следователя или дознавателя и только в том объеме, в каком ими будет признано это допустимым, если разглашение не противоречит интересам предварительного расследования и не связано с нарушением прав, свобод и законных интересов участников уголовного судопроизводства» [45]. Также недопустимо разглашение сведений о частной жизни участников судопроизводства, поскольку последние относятся к персональным данным. В этой связи, УПК РФ также можно считать нормативным правовым актом, содержащим нормы, регулирующие отношения в сфере информационной безопасности.

Что касается профессиональной тайны, то, как указывает С.В. Голубчиков, «предметом профессиональной тайны являются отношения, которые возникают между субъектами, участвующими в обработке и защите профессиональной тайны» [6]. К таким субъектам относятся владельцы (доверители) – физические лица, доверившие сведения другому лицу, держатели и пользователи – физические, юридические и иные лица, которым в силу их профессиональных обязанностей, были доверены в пользование сведения, составляющие профессиональную тайну. Что касается механизма защиты, он устанавливается согласно договору между доверителем и держателем. Помимо договора, защита профессиональной тайны установлена некоторыми Федеральными Законами, как, например, Федеральным законом от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в

Российской Федерации» [56], или «Основами законодательства Российской Федерации о нотариате» [31]. Врачебная тайна охраняется Федеральным Законом от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [61]. Федеральный Закон «О почтовой связи» от 17.07.1999 № 176-ФЗ ст. 15 охраняет тайну переписки» [55] и др. Сведения, являющиеся профессиональной тайной, охраняются положениями Гражданского и Уголовного Кодекса РФ.

Механизм защиты коммерческой тайны определен положениями Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [57]. Данный Закон устанавливает виды информации, которая является или не является коммерческой тайной. Так, «информация, составляющая коммерческую тайну, определяется как научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, в том числе ноу-хау, которая обладает действительной или потенциальной коммерческой ценностью в силу ее неизвестности третьи лицам, которые могли бы получить выгоду от ее разглашения или использования, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности правовые, организационные, технические и иные меры охраны» [16]. Законом определены права обладателя сведений, составляющих коммерческую тайну, которые возникают с момента установления им режима коммерческой тайны.

Охрана тайны интеллектуальной собственности происходит путем реализации норм ч.4 Гражданского кодекса Российской Федерации [7], направленных на защиту автора интеллектуальных произведений.

Федеральным Законом «Об информации, информационных технологиях и о защите информации» определено, что информация, составляющая государственную тайну, так же относится к конфиденциальной, однако, защита данного рода информации осуществляется в соответствии с Законом РФ от 21.07.1993 № 5485-1 «О

государственной тайне». Государственная тайна особо охраняется государством и представляет собой «защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации» [14].

Средствами защиты информации являются технические, криптографические, программные и другие средства, которые предназначены для защиты сведений, составляющих государственную тайну. Так, системой защиты государственной тайны является совокупность данных органов защиты, а также используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях. Л.Л. Попов отмечает, что «важнейшие полномочия в сфере защиты государственной тайны принадлежат Президенту РФ. Его полномочия в данной сфере определяются Конституцией РФ» [32], так же правовую основу охраны государственной тайны осуществляют: Палаты Федерального Собрания, Правительство РФ, органы государственной власти Российской Федерации, органы государственной власти субъектов РФ и органы местного самоуправления. Непосредственно защитой государственной тайны занимаются органы ФСБ России, Федеральная служба по техническому и экспортному контролю, Министерство обороны РФ, Служба внешней разведки РФ. Различные органы государственной власти, учреждения и организации обеспечивают защиту сведений, составляющих государственную тайну, в соответствии с возложенными на них задачами и в пределах своей компетенции.

Рассматривая вопросы правового регулирования информационной безопасности нельзя не отметить, что вся система обеспечения информационной безопасности не в состоянии эффективно работать в ситуации, когда отсутствуют механизмы привлечения к ответственности за нарушение установленных норм и правил, либо за различные деструктивные

воздействия на механизмы системы. Ответственность за нарушения в сфере обеспечения информационной безопасности определяются положениями Гражданского (в части возмещения вреда) и Уголовного Кодексов, а также Кодекса РФ об Административных Правонарушениях. В частности, ст.ст. 137, 138, 140, 144, 155 , 183, 237, 283, 283.1, 284, 310, 311, 320, 324, 325, 327, 272, 273, 274, 274.1, 274.2 УК РФ определяют уголовную ответственность за преступления в сфере информационной безопасности [46]; ст.ст. 5.1, 5.3, 5.4, 5.5, 5.8, 5.25, 5.39, 5.53, 5.54, 5.55, 6.13, 6.13.1, 6.21, 6.26, 6.27, 7.12, 7.29, 7.29.2, 7.29.3, 7.30, 7.32.6, 8.5, 8.5.2, 10.7, 13.2-13.47, 14.20, 14.29, 15.12-15.13, 15.48, 16.3, 17.13, 19.7, 19.7.1, 19.7.2, 19.7.2-1, 19.7.3, 19.7.5, 19.7.5-2, 19.7.7, 19.7.8, 19.7.9, 19.7.10, 19.7.10-1, 19.7.10-2, 19.7.10-3, 20.3-20.3.4, 20.23, 20.24 КоАП РФ определяют административную ответственность за правонарушения, посягающие на отношения в сфере информационной безопасности (в широком смысле) [18]. Таким образом, и УК РФ, и КоАП РФ являются нормативными актами, содержащими нормы в сфере ИБ.

Полноценное обеспечение информационной безопасности в части нормального функционирования государственных и муниципальных органов невозможно себе представить без устойчивой и бесперебойной работы используемых в этих органах средств автоматизации. Речь идет о государственных информационных системах, с использованием которых автоматизируется выполнение одной или нескольких функций государственного или муниципального органа. Согласно ч.2 ст. 14 Федерального закона № 149-ФЗ, государственные информационные системы создаются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. В первую очередь, речь идет о Федеральном законе № 44-ФЗ от 05.04.2013 «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [62]. Рассмотренный закон входит в систему нормативных актов в сфере информационной безопасности с той

точки зрения, что его положения определяют принципиальные вопросы по созданию и эксплуатации ГИС.

Завершая рассмотрение нормативных правовых актов уровня федерального закона и выше, регулирующих отношения в сфере информационной безопасности, можно отметить, что прослеживается явная тенденция к разделению отдельных регулирующих функций между различными нормативными актами. Вместе с тем, можно заметить наличие центрального нормативного правового акта в этой сфере, определяющего ключевые понятия в данной сфере регулирования. Это обстоятельство может служить основой для возможной будущей кодификации законодательства в сфере информации и, в частности, информационной безопасности. С другой стороны, нельзя не отметить присутствие большого количества бланкетных норм, требующих конкретизации на уровне подзаконных нормативных актов. Далее будут рассмотрены наиболее важные из них.

2.2 Основные подзаконные нормативные правовые акты в области информационной безопасности

Большое количество правовых механизмов в сфере информационной безопасности содержат положения, требующие конкретизации на уровне различных подзаконных актов. Рассмотрим основные подзаконные нормативные акты, являющиеся частью обозначенных механизмов. Следует заметить, что количество подобных нормативных актов различных уровней, имеющих отношение к информационной безопасности, составляет несколько сотен, и детальное рассмотрение каждого из них выходит за рамки предмета настоящего исследования. По этой причине подробно будут рассмотрены только некоторые наиболее важные подзаконные нормативные акты.

Из подзаконных актов ключевое значение для информационной безопасности, безусловно, играет ряд Указов Президента, представляющих собой документы стратегического планирования. К таковым можно отнести

уже ранее упомянутые: Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [51] и Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [49].

Первая версия Доктрины информационной безопасности была разработана и утверждена Президентом в 2000 году. По своей сути, она являлась развитием Концепции национальной безопасности РФ в информационной сфере и должна была задать единое направление развития механизмов правового регулирования информационной безопасности. Вместе с тем, принимаемые государством меры по обеспечению информационной безопасности с течением времени требуют корректировки, поскольку угрозы в информационной сфере постоянно меняются с учетом последних технических достижений, а также в контексте изменения общественно-политической обстановки. В связи с этим, были предприняты адекватные меры по усовершенствованию отечественного законодательства.

Действующая Доктрина информационной безопасности Российской Федерации, принятая и подписанная Президентом РФ 5 декабря 2016 г., «является документом стратегического планирования в сфере обеспечения национальной безопасности РФ, в котором развиваются положения Стратегии национальной безопасности РФ, утвержденной Указом Президента РФ от 31.12.2015 № 683, а также других документов стратегического планирования в указанной сфере». Существенным отличием новой Доктрины является то, что в ней закрепляются и значительно расширяются основные понятия и термины, недостаточно интерпретируемые в предыдущем документе, а выделение терминологии в отдельный раздел Доктрины, осуществляет постановку более четких границ правового регулирования документа [28].

Сравнивая предыдущую и действующую Доктрину, стоит отметить, что Первая приоритетом устанавливала вопрос возрастания влияния

информационных технологий на национальные интересы государства, а также делала определенный акцент на информационной безопасности личности, в то время как документ 2016 года уделяет преимущественное внимание информационным технологиям в разрезе развития общественных отношений [27].

Стоит подчеркнуть также, что действующая доктрина формирует основные положения Стратегии национальной безопасности, касающиеся:

- тенденций усиления конфронтации среди мировых лидеров в области глобального информационного пространства;
- возможных угроз безопасности и устойчивости функционирования российской критической информационной инфраструктуры;
- вопросов деятельности, связанной с использованием информационных и коммуникационных технологий в сфере преступлений террористической и экстремистской направленности;
- возможности импортозамещения с целью уменьшения критической зависимости от иностранных технологий и промышленной продукции.

Можно отметить тот факт, что курс на импортозамещение прослеживается в обоих документах. Данная задача выделяется как основная для нашей страны. Меж тем, в новой Доктрине экономическая сфера обеспечения информационной безопасности сосредоточена именно на необходимости формирования национальной отрасли информационных технологий и информационной безопасности, следствием которого должна послужить ликвидация какой-либо зависимости от зарубежных информационных технологий.

Помимо документов стратегического планирования, можно также выделить Указы Президента, отражающие оперативную реакцию государства на вновь возникающие угрозы в сфере ИБ. Так, например, к таковым можно отнести Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [52]. Указанный нормативный акт стал шагом к перераспределению

полномочий государственных органов в сторону создания единой системы органов, ответственных за выработку и реализацию мер по обеспечению информационной безопасности. Согласно данному нормативному акту, ФСБ России получила полномочия по изданию обязательных для исполнения указаний в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Также в документе формулируются положения по созданию и государственной аккредитации центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, к которым перейдут аналогичные полномочия в будущем. Отдельное внимание в документе уделяется также необходимости качественного локального регулирования вопросов, касающихся информационной безопасности на объектах критической информационной инфраструктуры (далее – КИИ) и иных стратегически важных объектах.

Помимо общих вопросов, затрагивающих систему информационной безопасности в целом, Указами Президента также регулируются отдельные направления, связанные с защитой отдельных видов информации. Так, например, в соответствии с Указом Президента РФ 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» определяются сведения о сущности изобретения, полезной модели или промышленного образца, подлежащие защите в соответствии с нормами ГК РФ [47].

В соответствии с Указом Президента РФ от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны» [48] реализуются полномочия Межведомственной комиссии, контролирующей и координирующей деятельность различных государственных органов по защите государственной тайны.

Рассматривая подзаконные нормативные акты по информационной безопасности нельзя не упомянуть деятельность Правительства в данной

сфере. Нормативными актами Правительства, как правило, осуществляется регулирование конкретных направлений информационной безопасности. Так, например, Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» играет важную роль в цифровизации деятельности государственных органов [35]. Названное постановление определяет наиболее общие и важные положения, касающиеся разработки программного обеспечения для автоматизации деятельности государственных органов и подведомственных им предприятий.

Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливаются специальные требования к уровню защищенности персональных данных при их обработке в информационных системах, требования к защите персональных данных при их обработке в информационных системах, и требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных. Также проводится типизация актуальных угроз для информационных систем, и устанавливаются критерии для определения 4 уровней защищенности информационных систем [34].

Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» определяет порядок отнесения несекретной информации к категории информации ограниченного распространения, порядок обращения с такой информацией

во избежание её разглашения [33]. В данном случае речь идет об информации, составляющей служебную тайну.

Следует подчеркнуть, что Правительство РФ осуществляет оперативное реагирование на вновь возникающие угрозы в сфере информационной безопасности. Это выражается, в числе прочего, в выработке конкретных мер, направленных на преодоление угроз. Так, Постановлением Правительства РФ от 15 июля 2022 г. №1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» исполняются требования ранее упомянутого Указа Президента РФ от 01.05.2022 № 250 [52]. В частности, конкретизируются требования к организациям, имеющим стратегическое значение или обслуживающим объекты КИИ РФ, в части обязанности создания и функционирования специализированных подразделений по ИБ и правового статуса заместителей руководителя по ИБ [38]. В этой же связи можно отметить Постановление Правительства РФ от 22.08.2022 № 1478, которым были введены новые правила использования различного ПО на объектах КИИ РФ [39].

Еще одним примером деятельности Правительства РФ, направленной на регулирование в сфере ИБ, можно считать работу по унификации технологий, используемых для создания и эксплуатации ГИС. Согласно Постановлению Правительства РФ от 12.10.2020 № 1674 «О проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех» [37], в настоящий момент в ряде органов реализуется пилотный проект по использованию единой цифровой платформы Российской Федерации «ГосТех», разработанной при участии ПАО «Сбербанк». Указанное обстоятельство можно считать шагом к

обеспечению единого подхода к обеспечению информационной безопасности во всех государственных органах. Вместе с тем, выбранный инструмент имеет неоднозначные оценки с точки зрения эффективности, что будет показано далее в ходе исследования.

Рассмотренные выше подзаконные нормативные акты уровня Указа Президента или Постановления Правительства своими положениями развивают и конкретизируют отдельные направления регулирования. Вместе с тем, данные документы носят достаточно общий характер. Дальнейшая конкретизация отдельных правовых механизмов, регулирующих отношения в сфере информационной безопасности, осуществляется на уровне приказов отдельных федеральных органов исполнительной власти. Документы такого уровня определяют явные технические детали отдельных правовых механизмов, устанавливают четкий порядок осуществления прав и обязанностей участников отношений в сфере обеспечения ИБ. Среди них можно выделить различные административные регламенты и перечни технических требований, обязательных для соблюдения.

Так, например, ФСБ России осуществляет регулирование в части координации деятельности ГосСОПКА, а также в части лицензирования деятельности, связанной с разработкой и использованием шифровальных (криптографических) средств, иных средств защиты конфиденциальной информации, а также проведения работ, связанных с использованием сведений, составляющих государственную тайну, допуска организации к таким работам. Указанные направления регулируются следующими нормативными актами:

- приказ ФСБ России от 24.07.2018 №366;
- приказ ФСБ России от 29.12.2020 № 641;
- приказ ФСБ России от 29.12.2020 № 639;
- приказ ФСБ России от 11.04.2014 № 202.

В деятельности ФСТЭК России в качестве наиболее важных нормативных актов можно выделить нормативные акты, которые определяют

технические требования к ГИС и системам защиты информации в объектах КИИ. К таковым можно отнести:

- приказ ФСТЭК России от 29 апреля 2021 г. № 77 «Об утверждении Порядка организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну»;
- приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»;
- приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;
- приказ ФСТЭК России от 21 сентября 2016 г. № 131 «Об организации работы по разработке перечней правовых актов и их отдельных частей (положений), содержащих обязательные требования, соблюдение которых оценивается при проведении мероприятий по контролю в рамках видов федерального государственного контроля в сфере компетенции ФСТЭК России»
- приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

  и другие.

Рассматривая роль отдельных ФОИВ в построении правовых механизмов обеспечения ИБ, нельзя не отметить Минцифры России. Помимо координации деятельности по реализации различных государственных программ, направленных на построение цифрового общества и цифровой экономики, данное министерство также оказывает влияние на выработку государственной политики в сфере информационных технологий и, в

частности, информационной безопасности. Одним из важных направлений деятельности Минцифры России, оказывающим прямое влияние на информационную безопасность, является ведение реестра отечественного ПО. Сведения из указанного реестра используются при в ходе аттестации ГИС на предмет соблюдения требований об использовании отечественного ПО и соблюдения запрета использования иностранного ПО при наличии отечественных аналогов. Таким образом, вопросы ведения реестра отечественного ПО имеют непосредственное отношение к информационной безопасности, а положения, определяющие условия допуска и исключения программных продуктов из реестра оказывают значительное влияние на общее состояние защищенности в рассматриваемой сфере. Данные вопросы регулируются Приказом Министерства цифрового развития, связи и массовых коммуникаций РФ от 21 февраля 2019 г. № 62.

Следующими в иерархии должны быть рассмотрены нормативные акты в сфере ИБ субъектов РФ и муниципальных образований. При их рассмотрении следует еще раз подчеркнуть, что они могут иметь решающего значения в построении системы механизмов обеспечения ИБ. Исходя из ранее озвученных тезисов, можно отметить, что местное регулирование в данной сфере должно в полной мере подчиняться общероссийским принципам и реализовывать механизмы, выработанные на федеральном уровне, возможно, с учетом некоторой местной специфики там, где таковая присутствует. Данный вопрос является принципиальным, поскольку позволяет использовать более значительный научный и технический потенциал федерального уровня, а также снижает вероятность использования злоумышленниками местных особенностей и отношения к информационной безопасности для нанесения ущерба системам и информационным ресурсам федерального уровня. По этой причине в рамках данного исследования не уделяется значительного внимания нормативных правовым актам уровня субъектов РФ и муниципальных образований.

Завершая рассмотрение подзаконных нормативных актов в сфере ИБ можно еще раз отметить их значительное количество, а также относительно большое количество различных государственных органов, осуществляющих регулирование. Подзаконные нормативные акты федерального уровня играют важную роль в системе нормативных правовых актов в области информационной безопасности, поскольку определяют конкретные способы и пути реализации положений законодательства, а также конкретизируют технические детали, которые могут иметь решающее значение для эффективной работы механизмов обеспечения ИБ. На данном уровне возможно наиболее оперативное реагирование на вновь возникающие угрозы в данной сфере за счет более простой процедуры внесения изменений в текст нормативных правовых актов.

Можно отметить, что полученные данные по особенностям построения структуры нормативных правовых актов в сфере информационной безопасности позволяют в дальнейшем провести исследование существующих правовых механизмов на предмет применимости содержащихся в них норм современным угрозам в данной сфере.

Глава 3 Предложения по совершенствованию механизмов правового регулирования информационной безопасности

3.1 Анализ и оценка факторов, оказывающих негативное влияние на состояние информационной безопасности

Ранее в ходе исследования было показано, что информационная безопасность затрагивает весьма широкий перечень различных общественных отношений. Это обусловлено, во многом, значительным проникновением информационных технологий в различные сферы жизни. Вместе с тем, можно заметить, что ряд информационных технологий, широко применяющихся в России, имеет значительную степень зависимости от различных факторов, на которые оказывают прямое или косвенное влияние иностранные государства и транснациональные корпорации. Учитывая текущее направление развития международной обстановки, можно констатировать, что подобное влияние приобрело сугубо негативную и деструктивную форму. В подобных условиях становится критически необходимым актуализировать основные направления подобного деструктивного влияния и определить наиболее эффективные меры противодействия.

Оценку факторов, оказывающих преимущественно негативное влияние на состояние ИБ, проведем на основе рассмотрения некоторых направлений ИБ, изложенных в действующей Доктрине информационной безопасности 2016 года [49], ранее рассмотренных исследований в области информационной безопасности, а также собранного автором исследования фактического материала об особенностях функционирования отрасли разработки и внедрения программно-аппаратных комплексов. В этом ключе можно выделить следующие основные, взаимно пересекающиеся, группы факторов:

– технические (факторы, определяемые уровнем развития науки и техники в области ИБ);
– организационно-технические (факторы, определяемые особенностями практического использования достижений науки и техники в деятельности государственных органов и коммерческих предприятий);
– правовые (факторы, определяемые содержанием правовых норм, регулирующих отношения в области ИБ);
– экономические (факторы, определяемые текущим уровнем развития экономики РФ, ее зависимости от международной кооперации);
– смешанные (факторы, находящиеся на стыке различных групп, из числа перечисленных выше).

В формате настоящего исследования не представляется возможным привести полный анализ всех факторов, оказывающих влияние на состояние ИБ по каждой группе. По этой причине будут упомянуты лишь наиболее важные и существенные факторы.

Для группы технических факторов можно выделить следующие основные составляющие:

– существенная доля элементной базы иностранного производства в аппаратной части применяющихся программно-аппаратных комплексов;
– широкое распространение иностранного программного обеспечения общего и специального назначения для разработки, сборки и эксплуатации применяющихся программно-аппаратных комплексов;
– отсутствие пригодных универсальных программных решений для автоматизации деятельности государственных органов;
– наличие широкого спектра недокументированных возможностей программного обеспечения в составе ГИС;
– низкая надежность механизмов интеграции технических решений, используемых в различных ФОИВ.

Рассматривая вопросы использования иностранной элементной базы в программно-аппаратных комплексах, эксплуатируемых в РФ, необходимо подчеркнуть, что этот вопрос является составной частью более широкой проблемы импортозамещения в сфере разработки и производства микроэлектроники. Действительно, в РФ проблема импортозамещения стоит крайне остро, в том числе, и с точки зрения обеспечения информационной безопасности. Следует заметить, что значительная часть работ по импортозамещению в сфере информационных технологий, проводившихся с 2014 года, выполнялась таким образом, что цели работ достигались лишь формально. Некоторые применяемые решения удовлетворяли критериям импортозамещения, однако, ликвидируя одни угрозы и уязвимости, одновременно оставляли другие. Ярким примером подобного решения в области микроэлектроники и создания собственной элементной базы и электронных компонентов для серверного оборудования является разработка и производство процессоров семейства «Байкал» и «Эльбрус». Указанные процессоры создаются на базе отечественной архитектуры. Однако компании-разработчики не имеют значительных собственных производственных мощностей на территории Российской Федерации. В результате, основная часть производственного процесса не имеет локализации в России и осуществлялась на территории иностранных государств (например, на территории частично признанной Китайской Республики, остров Тайвань, компания TSMC). В современных условиях, при наличии явных недружественных действий отдельных иностранных государств, указанное обстоятельство равноценно фактическому отсутствию указанных процессоров. Отсюда, актуальным является проведение аналитических и опытно-конструкторских работ в части организации собственных технологических процессов по производству электронных компонентов на территории Российской Федерации, а также расширения номенклатуры отечественных компонентов, используемых в серверном оборудовании. Это позволит заместить импортные составляющие и в

дальнейшем обеспечивать функционирование информационных систем на отечественной элементной базе.

Одновременно с проблемами импортозамещения в части аппаратного обеспечения, следует рассматривать сходные проблемы с использованием иностранного программного обеспечения. Так, большая часть используемых в настоящий момент операционных систем для серверов и рабочих станций представляет собой иностранные разработки, допускающие внедрение незадекларированных возможностей. Подобная ситуация складывается также в используемых инструментах для разработки, сборки и эксплуатации программного обеспечения. Наиболее удобные инструменты разработки ПО (например, Jet Brains Intellij IDEA, Microsoft Visual Studio), средства сборки (Apache Maven и т.д.), сервера приложений (Apache Tomcat, Glassfish), связующее ПО (Apache ActiveMQ), промышленные поисковые системы (ElasticSearch), офисные пакеты (Microsoft Office) представляют собой иностранное программное обеспечение. Отсутствие или низкое качество отечественных аналогов связано, по мнению автора исследования, с господствующей в индустрии разработки программного обеспечения идеологией отказа от разработки новых программных продуктов при наличии существующих аналогов, удовлетворяющих требуемым характеристикам. При этом не имеет значения происхождение программного продукта. Так, при разработке программного обеспечения для государственных нужд зачастую используется иностранное программное обеспечение или отдельные компоненты, инструменты для разработки и развертывания программного обеспечения. Аналоги многих из них отсутствуют в реестре отечественного ПО. В то же время, отечественные разработчики не видят смысла в создании программных продуктов, для которых есть зарубежные аналоги. В результате имеет место замкнутый круг причины и следствия. Решение этой проблемы выходит за рамки темы исследования, однако в целом необходимо принятие мер, которые позволят побудить отечественных разработчиков создавать свои аналоги программных

продуктов, пусть даже и уже представленных зарубежными образцами. Понимание сути проблемы во многом становится повсеместным в результате введения против Российской Федерации масштабных международных санкций, ограничивающих возможность обновления иностранного ПО или же существенно повышающих степень риска внедрения и использования незадекларированных возможностей.

В рамках группы организационно-технических факторов следует выделить следующие элементы:

- наличие приоритета частных интересов отдельных разработчиков программного обеспечения, подкрепленного их лоббистскими возможностями, над технической эффективностью предлагаемых ими решений;
- высокая степень формализма при принятии управленческих решений в части коммуникации между разработчиками и эксплуатантами программно-аппаратных комплексов;
- недостаточная степень технической грамотности пользователей ГИС;
- недостаточная степень материально-технического оснащения территориальных органов ФОИВ для эффективного применения современных достижений науки и техники;
- недостаточный уровень технической компетенции отдельных исполнителей государственных и муниципальных контрактов.

Для данной группы основной акцент можно сделать на существующем явлении, когда лоббистские возможности отдельных разработчиков программного обеспечения позволяют им занимать лидирующие позиции в области автоматизации деятельности государственного сектора. Это приводит к тому, что наличие «бренда» превалирует над технической эффективностью предлагаемых ими решений. В качестве примера можно привести ситуацию, складывающуюся вокруг единой цифровой платформы РФ «ГосТех». Указанная платформа, по замыслу разработчиков, должна стать универсальным программным средством для разработки специального

программного обеспечения для нужд всех государственных органов РФ. До 31 декабря 2022 года реализуется эксперимент (пилотный проект) по переводу отдельных ГИС некоторых ФОИВ на использование указанной платформы [37]. По состоянию на октябрь 2022 года автор настоящего исследования имеет крайне противоречивые данные о технической эффективности и степени пригодности единой цифровой платформы «ГосТех» для решения поставленных перед ней задач. Однако, не смотря на то, что эксперимент еще не завершен, а объективные данные об эффективности применявшихся технических средств не доведены до сведения лиц, принимающих решения, в настоящий момент уже вынесен на общественное обсуждение проект Постановления Правительства РФ [41], которым будет регулироваться применение платформы «ГосТех» для создания и эксплуатации ГИС. Вместе с тем, некоторые из заявленных целей и потенциальных способов применения возможностей платформы, могут оказаться недостижимы с технической точки зрения, что позволяет усомниться в правильности выбранного инструмента для достижения целей автоматизации деятельности государственного сектора. Однако, сама концепция, направленная на унификацию программных средств, используемых при построении ГИС, представляется правильной. С учетом изложенного, представляется целесообразным проведение научно-исследовательских и опытно конструкторских работ по разработке, созданию и внедрению другой универсальной цифровой платформы, на базе которой будут строиться все информационные системы любого назначения для нужд органов власти. В дальнейшем представляется целесообразным принятие мер регулирования, направленных на продвижение и использование подобной платформы в деятельности и коммерческих организаций. Курс на реализацию описанной концепции может быть закреплен на уровне нормативных правовых актов уровня федерального закона.

Наиболее важной для целей настоящего исследования представляется группа правовых факторов. В рамках нее можно выделить следующие ключевые факторы:

- принципиальная неработоспособность некоторых международно-правовых механизмов обеспечения информационной безопасности;
- наличие пробелов в механизмах ответственности за создание угроз информационной безопасности РФ;
- значительное количество нормативных правовых актов в области ИБ, наличие конкурирующих норм в источниках одинаковой юридической силы в отсутствие явно заданного приоритета;
- отставание документов стратегического планирования от текущей обстановки;
- несовершенство правовых механизмов защиты отдельных видов конфиденциальной информации;
- противоречие интересов государства и существующих правовых механизмов защиты авторских и смежных прав;
- несовершенство законодательства в области государственных закупок в части применимости к разработке программного обеспечения;
- взаимные пересечения полномочий различных государственных органов в сфере обеспечения ИБ.

Следует заметить, что в условиях введения политически мотивированных ограничений международного сотрудничества в различных сферах, включая и сферу обеспечения ИБ, представляется необходимым проработка новых международно-правовых механизмов, альтернативных существующим (в первую очередь по составу участников) [17].

Одной из проблем стоит упомянуть отсутствие согласованной структуры нормативных правовых актов в сфере информационной безопасности. Как было неоднократно отмечено, различные аспекты информационной безопасности регулируются не связанными друг с другом

нормативными правовыми актами различного уровня, а согласованные изменения в них требуют большой работы по выявлению всех взаимосвязей и взаимозависимостей. Указанная проблема может быть решена путем кодификации законодательства в этой сфере. И, хотя данный вопрос неоднократно поднимался в трудах различных авторов, в настоящий момент работы по кодификации ведутся профильными государственными органами недостаточно интенсивно.

В качестве другой проблемы можно отметить отсутствие единого органа, отвечающего за реализацию мер по обеспечению информационной безопасности. В настоящий момент полномочия в данной сфере разделены между Президентом РФ, Правительством РФ, ФСБ России, ФСТЭК России, Роскомнадзором, МВД России и центрами ГосСОПКА. С марта текущего года была активизирована работа, направленная на централизацию полномочий в указанной сфере. Однако данная работа еще далека от завершения.

Также можно выделить проблему соответствия действующей доктрины информационной безопасности существующим реалиям. Если рассматривать положения Доктрины информационной безопасности, то следует отметить, что в п.5 прямо говорится о том, что Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации и развивает положения Стратегии национальной безопасности Российской Федерации и других документов стратегического планирования в указанной сфере. Можно обратить внимание на тот факт, что действующая в настоящий момент Доктрина информационной безопасности опирается на не действующую, устаревшую Стратегию национальной безопасности Российской Федерации, утвержденную Указом Президента Российской Федерации от 31 декабря 2015 г. № 683. Следует подчеркнуть, что вопросы обеспечения информационной безопасности оказывают влияние на все основные направления национальной безопасности. В этой связи представляется

очевидным актуальность и важность изучения вопросов, касающихся средств, способов и методов, а также факторов, оказывающих влияние на обеспечение информационной безопасности. Упущения и недостатки в данной сфере могут оказывать значительное деструктивное влияние на общество и государство в целом.

Рассматривая правовые факторы нельзя не упомянуть о несоответствии текущей обстановке некоторых конкретных правовых механизмов. Наиболее подробно выделенные факторы будут рассмотрены далее в ходе разработки и формулирования предложений по совершенствованию правовых механизмов регулирования ИБ.

Подробное рассмотрение экономических факторов не является целью настоящего исследования. Вместе с тем, можно констатировать значительную степень влияния данных факторов на упомянутые ранее технические и организационно-технические. Среди наиболее значительных экономических факторов можно выделить следующие:

- слабая экономическая база отраслей промышленности, задействованных в производственном цикле микроэлектроники;
- наличие критической зависимости от импорта технологий, участвующих в производственных цепочках аппаратной части ГИС.

В используемой в рамках исследования классификации, смешанные факторы затрагивают сразу несколько направлений обеспечения ИБ. Разумеется, многие из перечисленных ранее факторов, отнесенных к отдельным группам, имеют внешние зависимости, пересекающиеся с другими группами. Вместе с тем, существует фактор, оказывающий, по мнению автора исследования, ключевое влияние на все остальные, перечисленные ранее, факторы. Речь идет о существующей системе образования по специальностям, представители которых задействованы в реализации перечисленных ранее направлений деятельности. Данный фактор в полной мере можно отнести в группу смешанных, поскольку он затрагивает элементы и технической составляющей, и правовой, и экономической.

Необходимо подчеркнуть, что, поскольку обеспечение информационной безопасности лежит на стыке технической и правовой сферы деятельности, важным представляется организация подготовки специалистов, обладающих одновременно компетенциями, как в сфере информационных технологий, так и в юриспруденции. В частности, в настоящий момент уже реализуется ряд программ подготовки специалистов такого профиля в отдельных государственных образовательных учреждениях высшего образования по специальностям: «Информационно-аналитические системы безопасности» (отдельные специализации) и «Правовое обеспечение национальной безопасности» (отдельные специализации). Также подготовка соответствующих кадров реализуется путем освоения последовательно двух программ высшего образования или же осуществления профессиональной переподготовки после освоения одной из программ высшего образования.

Завершая рассмотрение различных групп факторов, оказывающих влияние на состояние информационной безопасности, следует подчеркнуть, что качественное и полноценное обеспечение безопасности в данной сфере может быть реализовано только при условии системной проработки и реализации мер, направленных на устранение недостатков по каждому из выделенных факторов.

3.2 Предложения по изменению нормативных правовых актов в области обеспечения информационной безопасности

Ранее в ходе анализа правовых факторов, оказывающих наиболее важное влияние на состояние информационной безопасности в РФ, было установлено, что отдельные правовые механизмы не в полной мере соответствуют актуальным вызовам в данной сфере. Дальнейшее применение существующих правовых механизмов может увеличить степень риска и поставить под угрозу устойчивость государства и нормальное функционирование общества в данной сфере. На основании информации,

полученной в ходе данного исследования, могут быть сформулированы отдельные предложения по внесению изменений в существующие правовые механизмы, регулирующие отношения в сфере информационной безопасности.

Как было ранее показано, одним из ключевых нормативных правовых актов в сфере ИБ является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [58]. Анализируя положения указанного закона, можно заметить, что некоторые его положения не полностью соответствуют новым угрозам в сфере информационной безопасности и создают некоторые препятствия для эффективного противодействия подобным угрозам. К таковым можно отнести состав основных принципов правового регулирования. Так, в п.8 ст. 3 Федерального закона № 149-ФЗ [58] закреплен принцип, согласно которому не допускается установление нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, за исключением случаев, установленных федеральными законами в отношении государственных информационных систем. Одновременно с этим, согласно ч.6 ст. 14 того же Федерального закона [58], требования к порядку создания государственных информационных систем утверждаются Правительством Российской Федерации. Также, согласно ч.2 ст. 14 Федерального закона № 149-ФЗ, государственные информационные системы создаются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. В итоге возникает ситуация, когда для информационных систем, не являющихся государственными, принципиально не допускается ситуация установления преимуществ в использовании определенных информационных технологий. Для ГИС возможность установления преимуществ рассматриваются как исключительная ситуация и вынесена в другой федеральный закон, а также на уровень подзаконных актов. Указанные

обстоятельства не соответствуют декларируемому курсу на преимущественное использование отечественных технических средств при создании и эксплуатации информационных систем любого уровня. В этой связи, представляется целесообразным внести изменения в Федеральный закон [58], исключив из числа основополагающих принципов правового регулирования п.8 ст. 3.

Как было замечено ранее, определение самого понятия «информационная безопасность» приводится на уровне подзаконного акта – Указа Президента РФ [49]. Одновременно с этим, понятие «информационная безопасность» не расшифровывается в нормативных правовых актах уровня федерального закона. С одной стороны, подобная ситуация позволяет оперативно уточнять указанное понятие за счет более простой процедуры внесения изменений и принятия Указов Президента. С другой стороны, это демонстрирует неполную ясность в определении границ одной из центральных категорий информационного права. В этой связи, представляется целесообразным дополнить ст. 2 Федерального закона №149-ФЗ [58] новым пунктом, закрепив в нем понятие «информационная безопасность», четко разделив его с существующим понятием «защита информации».

В настоящий момент в различных отраслях права имеет место практика по выделению «центрального» нормативного правового акта уровня федерального закона в данной отрасли права. Остальные федеральные законы, имеющие пересечения и дополнения в предмете регулирования, не должны противоречить «центральному» или же их нормы должны включаться в текст «центрального» закона. Представляется целесообразным распространить подобную практику на отрасль информационного права. В рассматриваемом случае таковым может стать именно Федеральный закон №149-ФЗ. В этой связи автор исследования считает необходимым внести изменения в ч.1 ст. 4 Федерального закона [58] и изложить ее в следующей редакции: «Законодательство Российской Федерации об информации,

информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других Федеральных законов, регулирующих отношения по использованию информации и принятых в соответствии с настоящим Федеральным законом», - а также дополнить ст. 4 Федерального закона №149-ФЗ частью 1.1 следующего содержания: «Нормы законодательства в области информации и информационной безопасности, содержащиеся в других законах, должны соответствовать настоящему Федеральному закону».

Рассматривая Федеральный закон №149-ФЗ, можно заметить, что ст. 12.1 Федерального закона устанавливает базовые принципы ведения Реестра отечественного ПО (далее – Реестр), а также основные требования к программному обеспечению, которое может быть включено в Реестр. Согласно ч.6 ст. 12.1 Федерального закона, Правительству РФ предоставлено право установления дополнительных требований к ПО, а также определение порядка ведения Реестра. В настоящий момент существует запрет на использование иностранного программного обеспечения для нужд государственных и муниципальных органов при наличии аналога в Реестре. Таким образом, факт наличия/включения конкретного ПО в Реестр влечет за собой значительные правовые и организационные последствия для государственных и муниципальных органов, использующих иностранные аналоги данного ПО. Вместе с тем, на практике возникают ситуации, когда правообладатель российского ПО, включенного в Реестр до момента ухудшения международной обстановки, впоследствии кардинальным образом меняет условия предоставления и распространения (использования) данного ПО. Например, это может проявляться таким образом, что первоначально некоторое ПО предоставляется на основе бесплатной лицензии и в таком качестве включается в реестр отечественного ПО, а затем это же ПО через процедуру внесения изменений в реестровую запись, предоставляется на возмездной основе без изменения функциональных

возможностей. По факту в реестровой записи может быть изменено название программного обеспечения (используемый бренд) на новое, предполагающее исключительно использование на основе платной лицензии. Таким образом, возникают предпосылки для необоснованного увеличения расходов федерального бюджета в связи с реализацией плановых программ цифровой трансформации. Также из-за этого могут быть существенно сорваны сроки перевода отдельных ГИС на отечественное ПО. В этой связи, представляется целесообразным закрытие подобной возможности путем введения нового основания для исключения ПО из Реестра. Так, предлагается дополнить п.33 Правил ведения Реестра, утвержденных Постановлением Правительства РФ № 1236 от 16 ноября 2015 года [36] пунктом «е» следующего содержания: «изменение условий лицензионного договора или правил предоставления доступа к программному обеспечению, влекущее увеличение стоимости приобретения экземпляра программного обеспечения или стоимости единицы времени использования (предоставления доступа) программного обеспечения без изменения функциональных возможностей или характеристик самого программного обеспечения».

При рассмотрении системы нормативных правовых актов в сфере ИБ было показано, что в качестве меры реагирования на резкое усиление угроз информационной безопасности, в мае 2022 года был принят Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [52]. Данный нормативный акт имеет во многом оперативный характер, однако он содержит ряд важных норм, регулирующих отношения в сфере ИБ. Уровень мер, изложенных в нем, требует дальнейшей проработки и, отчасти, отражения на уровне федеральных законов. Это связано, в числе прочего, с необходимостью решения вопроса об установлении ответственности за нарушение обязательных персонализированных требований ФСБ России или центра ГосСОПКА (пп «д» и «е » п. 1 Указа Президента). Можно отметить наличие явной общественной опасности в ситуации, когда ответственное

лицо организации, получившее персонализированное требование об осуществлении конкретных мер в области обеспечения ИБ, проигнорировало его или саботировало его исполнение, что привело к возникновению тяжких последствий или причинению ущерба. Представляется, что на основе конструкции основного состава преступления, предусмотренного ч.1 ст. 274 УК РФ [46], может быть сконструирован особо квалифицированный состав, предусматривающий ответственность за нарушение или неисполнение обязательных персонализированных требований уполномоченных органов по защите информации. Особо квалифицированный состав может быть выделен на основе признака субъекта преступления (должностное лицо структурного подразделения, осуществляющего функции по обеспечению информационной безопасности органа или организации) и специфической формы поведения субъекта при наличии дополнительного условия (неисполнение персонализированного требования уполномоченного органа по защите информации). Таким образом, ст. 274 УК РФ может быть дополнена частью третьей, диспозиция которой может быть изложена следующим образом: «Деяния, предусмотренные частью первой и второй настоящей статьи, совершенные должностным лицом структурного подразделения, осуществляющего функции по обеспечению информационной безопасности в органе или организации, в нарушение ранее вынесенного решения уполномоченного органа по защите информации о применении неотложных организационных и технических мер в области информационной безопасности». Вопрос об определении объемов и содержания санкции за совершение подобного преступления может являться предметом отдельного исследования. Однако, уже на данный момент выглядит необходимым предусмотреть использование (в качестве дополнительного) наказания, предусмотренного п. «б» ст. 44 УК РФ, то есть лишения права занимать должности, связанные с обеспечением информационной безопасности или заниматься деятельностью, связанной с обеспечением информационной безопасности [46].

Поскольку из всех правоохранительных органов, осуществляющих функции предварительного расследования по уголовным делам, наиболее высокий уровень технических компетенций присутствует в системе органов безопасности, представляется целесообразным определить, что предварительное следствие должно производиться следователями органов ФСБ России. Соответственно, предлагается внесение соответствующих изменений в п.2 ч.2 ст. 151 УПК РФ (добавление ст. 274 части третьей) и п.3 ч.2 ст. 151 УПК РФ (по ст. 274 должны быть указаны только часть первая и вторая) [45].

Рассматривая недостатки механизмов защиты отдельных разновидностей конфиденциальной информации и их влияние на состояние ИБ, нельзя обойти вниманием вопросы защиты персональных данных. Как было показано ранее, в 2022 году в Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» уже были внесены изменения, затрагивающие, в числе прочего, вопросы контроля и надзора за осуществлением трансграничной передачи персональных данных [63]. Однако, анализируя новые правовые механизмы, можно заметить определенные уязвимости. Так, например, представляется, что предложенный разрешительный порядок осуществления деятельности по трансграничной передаче персональных данных содержит некоторые потенциально угрожаемые моменты. Согласно новой редакции ч.2 ст. 12 Федерального закона «О персональных данных»: «Уполномоченный орган по защите прав субъектов персональных данных утверждает перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных. В перечень иностранных государств, обеспечивающих адекватную защиту прав субъектов персональных данных, включаются государства, являющиеся сторонами Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных, а также иные иностранные государства, не являющиеся стороной Конвенции Совета Европы о защите физических лиц при автоматизированной обработке

персональных данных, при условии соответствия положениям указанной Конвенции действующих в соответствующем государстве норм права и применяемых мер по обеспечению конфиденциальности и безопасности персональных данных при их обработке» [59]. Одновременно с этим, согласно ч.10-11 ст. 12, в период рассмотрения уведомления оператора о намерении осуществлять трансграничную передачу персональных данных на территорию государств, обеспечивающих адекватную защиту прав субъектов персональных данных, возможность трансграничной передачи не ограничивается. Таким образом, законом будет допускаться ситуация, когда на протяжении 10 дней (и более, при некоторых обстоятельствах) может осуществляться трансграничная передача персональных данных граждан России в иностранные государства, включая, в числе прочих, недружественные. И даже в случае, если по истечении 10 дней будет принято решение о запрещении или ограничении передачи, обеспечение удаления уже переданных данных может оказаться невозможным по обстоятельствам, не зависящим от оператора, а определяемым политической волей иностранного государства. Таким образом, представляется целесообразным дополнить текст ч.2 ст. 12 Федерального закона «О персональных данных» [59] положением, предусматривающим, что иностранное государство ни при каких обстоятельствах не может быть включено в перечень государств, обеспечивающих адекватную защиту прав субъектов персональных данных, в случае, если оно включено в перечень иностранных государств и территорий, совершающих в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия. Для этих целей могут быть использованы как уже существующие перечни иностранных государств, например предусмотренные Распоряжением Правительства Российской Федерации от 05.03.2022 №430-р [42], так и разработаны новые.

При рассмотрении вопросов информационной безопасности нельзя не подчеркнуть высокую важность обеспечения бесперебойной работы средств

автоматизации, используемых в государственных и муниципальных органах. В последнее десятилетие развитие средств автоматизации для нужд государственных органов шло по пути укрупнения используемых информационных систем, создания «единых» систем, в рамках которых автоматизируется сразу значительное количество различных функций государственного органа. В случае если возникнет ситуация, в которой, независимо от причины, подобная система перестанет функционировать, деятельность органа власти может оказаться парализованной на неопределенный срок. Как показывает практика, подобная угроза может быть существенной даже в отношении ГИС, не являющихся частью КИИ РФ.

Согласно ч.2 ст. 14 Федерального закона № 149-ФЗ, государственные информационные системы создаются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд. В первую очередь, речь идет о Федеральном законе №44-ФЗ от 05.04.2013 «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [62]. Одним из основных принципов осуществления закупок для государственных и муниципальных нужд является принцип обеспечения конкуренции. Согласно ему, преимущественно должны использоваться конкурентные способы определения поставщика. Использование неконкурентных способов является исключением. Более того, в результате крупной реформы законодательства о государственных закупках, проведенной в 2021 году, было сокращено количество различных способов определения поставщика и сделан абсолютный приоритет на использовании конкурентных способов. Вместе с тем, может сложиться ситуация, когда при проведении конкурса на оказание услуг по технической поддержке некоторой государственной информационной системы, конкурс (не имеет значения, открытый или закрытый) будет выигран организацией, которая не обладает необходимыми знаниями конкретно об этой системе и о специфике автоматизируемых

процессов государственного органа, хотя при этом формально соответствует критериям, установленным в закупочной документации. В этом случае может сложиться ситуация, когда услуги по технической поддержке государственной информационной системы будут оказываться на кардинально более низком уровне в течение адаптационного периода, пока новый поставщик будет изучать устройство и особенности функционирования системы. Для информационных систем промышленного уровня, находящихся в эксплуатации уже длительное время, подобный период может составлять до нескольких месяцев за счет накопленных недокументированных особенностей программной реализации. В случае возникновения критических сбоев в указанный период, поставщик может оказаться не в состоянии оперативно их устранить. Таким образом, государственный орган будет не в состоянии осуществлять одну или несколько своих функций. В условиях повышенной международной напряженности, подобная ситуация может создавать значительные риски для безопасности Российской Федерации в целом.

Описанная выше ситуация может быть предотвращена в случае дополнения существующего механизма правового регулирования процедуры осуществления закупок для государственных нужд. Представляется, что необходимо предоставить государственным органам право использования неконкурентного способа определения поставщика. А именно: закупки у единственного поставщика. Согласно ч.1 ст. 93 Федерального закона №44-ФЗ [62], установлен обширный перечень ситуаций, в которых заказчиком может осуществляться закупка у единственного поставщика. Предлагается дополнить ч.1 ст. 93 пунктом 62 следующего содержания: «осуществление закупок услуг по технической поддержке в ходе эксплуатации государственных информационных систем, используемых для реализации и автоматизации одновременно нескольких полномочий государственного органа». Действие подобной меры во времени представляется целесообразным сохранить, как минимум, в течение периода повышенной

международной напряженности, присутствующей на данный момент. Достаточно очевидно, что предлагаемая норма является потенциальным коррупциогенным фактором. Вместе с тем, анализ ч.1 ст. 93 Федерального закона №44-ФЗ показывает, что подобные исключения уже неоднократно делались законодателем в отношении закупок отдельных видов товаров, работ и услуг, как правило, осуществляемых в целях обеспечения национальной безопасности. В складывающихся условиях представляется, что обеспечение информационной безопасности путем создания правового инструмента для организации бесперебойной деятельности государственных органов, должно являться одним из главных приоритетов для федерального законодателя.

Завершая рассмотрение обозначенных вопросов, можно прийти к выводу, что состояние защищенности в сфере ИБ обеспечивается не только правовыми, но и техническими, организационными, экономическими и другими методами. Степень защищенности в информационной сфере однозначно зависит от общего состояния экономики государства, его правовой системы и правовой культуры, технической грамотности населения, качества образования. Предложенные точечные изменения в некоторые действующие нормативные акты различных уровней потенциально могут позволить парировать отдельные угрозы ИБ, возникающие в настоящий момент. Вместе с тем, остается открытым вопрос о создании единой системы правовых механизмов в области ИБ, которые действовали бы во взаимосвязи и наиболее подходящим образом регулировали бы всю отрасль информационного права и информационную безопасность в частности. В настоящее же время все правовые механизмы в данной сфере являются разобщенными, а изменения в них носят во многом оперативный и несистемный характер.

Заключение

Целью настоящей выпускной квалификационной работы являлось рассмотрение вопросов правового регулирования в сфере информационной безопасности в современных условиях повышенной международной напряженности.

В ходе проведенного исследования было установлено, что информационная безопасность представляет собой многоаспектное понятие, механизмы правового регулирования которого распределены по различным отраслям права. Сама по себе тема регулирования информационной безопасности является достаточно разработанной как с правовой, так и с технической точки зрения. Существует большое количество публикаций и научных работ, затрагивающих отдельные аспекты данного явления с различных точек зрения.

Было показано, что информационная безопасность является неотъемлемой частью безопасности государства в целом, национальной безопасности. Наличие широкого спектра угроз в указанной сфере создает предпосылки к нарушению нормального функционирования государственного аппарата и, как следствие, к перспективе утраты политической, экономической и социальной стабильности и, возможно, даже суверенитета.

В условиях обострения международной обстановки вокруг Российской Федерации, нормативно-правовое регулирование информационной безопасности, приобретает важное значение для обеспечения безопасности государства. Многие из существовавших ранее проблем обострились, некоторые аспекты, казавшиеся ранее не столь важными, обрели, внезапно, высокую значимость. Требуется не только разработка и внесение дополнений в существующие нормативные правовые акты различных уровней, но и детальный комплексный научный анализ данной сферы.

Подводя итоги рассмотрения существующих механизмов правового регулирования информационной безопасности, можно заметить, что, несмотря на вполне сформировавшуюся правовую базу в области информационной безопасности, остаётся ряд проблем, требующих решения.

Так, первой проблемой стоит выделить отсутствие согласованной структуры нормативных правовых актов в сфере информационной безопасности. Как было отмечено, различные аспекты информационной безопасности регулируются не связанными друг с другом нормативными правовыми актами различного уровня, а согласованные изменения в них требуют большой работы по выявлению всех взаимозависимостей. Указанная проблема может быть решена путем кодификации законодательства в этой сфере. И, хотя данный вопрос неоднократно поднимался в трудах различных авторов, в настоящий момент работы по кодификации практически не ведутся.

Второй проблемой, напрямую вытекающей из первой, можно выделить наличие отдельных недостатков и уязвимостей в существующих механизмах правового регулирования. Часть из них была затронута в рамках настоящего исследования. В качестве оперативного пути решения проблемы было предложено внесение точечных изменений в отдельные нормативные правовые акты. Комплексное же решение состоит в построении и анализе карты взаимосвязей всей системы нормативных правовых актов в сфере ИБ с последующей кодификацией и оптимизацией законодательства в данной сфере.

В качестве третьей проблемы можно отметить отсутствие единого органа, отвечающего за реализацию мер по обеспечению информационной безопасности. В настоящий момент полномочия в данной сфере разделены между ФСБ России, ФСТЭК России, Роскомнадзором, МВД России и центрами ГосСОПКА РФ. В текущем году была активизирована работа, направленная на централизацию полномочий в указанной сфере. Однако данная работа еще далека от завершения.

Четвертая проблема заключается в фактически частичном срыве реализации процессов импортозамещения в сфере информационных технологий в целом и информационной безопасности в частности. Решение данной проблемы выходит за рамки рассмотрения исключительно правовых механизмов и должно предполагать комплексное и стратегическое решение на федеральном уровне.

Наконец, последней, пятой, можно выделить проблему не полной актуальности действующих документов стратегического планирования и, в частности, доктрины информационной безопасности. Представляется необходимым установление одним из основных приоритетов государственной политики возможности автономного функционирования всей информационной сферы Российской Федерации, без использования иностранного программного и аппаратного обеспечения, а также без потери качества функционирования. Россия должна быть готова сохранить для граждан, организаций и государственных органов возможность использовать все преимущества цифрового общества даже в условиях, когда использование иностранной элементной базы и программного обеспечения будет в значительной степени прекращено.

Не смотря на то, что вопрос наличия проблем в существующих механизмах обеспечения информационной безопасности неоднократно являлся предметом исследования различных авторов, современные условия выводят на первый план некоторые проблемы, которые ранее обходились стороной. Для их решения было обозначено два основных подхода: первый – оперативный, заключающийся во внесении точечных изменений в ряд нормативных правовых актов; второй – концептуальный и стратегический, заключающийся в перестройке системы нормативных правовых актов в указанной сфере. Автором работы были предложены отдельные конкретные шаги для реализации оперативного подхода, а также намечены возможные направления дальнейших исследований для реализации концептуального подхода.

Список используемой литературы и используемых источников

1. Атаманов Г. А. Информационная безопасность в современном российском обществе (социально-философский аспект): дис. канд. филос. наук: 09.00.11 / Геннадий Альбертович Атаманов; [Волгогр. гос. ун-т]. – Волгоград, 2006. – 168 с.
2. Барабанов А.В., Марков А.С., Фадин А.А. Оценка возможности выявления уязвимостей программного кода при отсутствии исходных текстов программ // Информационное противодействие угрозам терроризма. 2011. № 16. С. 86-89.
3. Белый А.Ф., Климов С.М. Алгоритм принятия решений по оценке функциональной устойчивости средств автоматизации в условиях компьютерных атак// Известия ЮФУ. Технические науки, 2010 № 11 (112). С 6-22
4. Бурушкин А.А., Соловьев С.В., Ступников А.В. Об актуальности разработки методического обеспечения построения комплексных систем защиты информации в системах электронного документооборота при интеграции разноплатформенных программно-технических средств// Информационное противодействие угрозам терроризма, 2009, №13 С. 4-9
5. Гасанова Н.Р., Гусейнова Д.И. «Системы защиты информации в ГИС» [Электронный ресурс] // Материалы VIII Международной студенческой научной конференции «Студенческий научный форум» Режим доступа: https://scienceforum.ru/2016/article/2016029527 (дата обращения: 01.05.2022)
6. Голубчиков С. В., Новиков В. К., Баранова А. В Виды профессиональной тайны и её защита // Гуманитарные, социально-экономические и общественные науки. 2018. №1. С. 1-7
7. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ // Собрание законодательства Российской Федерации, N 52 (ч.I), 25.12.2006, ст.5496

8. Гутник С. И. Уголовно-правовая характеристика преступных посягательств в отношении персональных данных// Дисс…канд. юрид. наук. – Красноярск: 2017 241 с.

9. Добровольская И.А. Понятие «Информационное пространство»: различные подходы к его изучению и особенности // Вестник РУДН. 2014. №4. URL: https://cyberleninka.ru/article/n/ponyatie-informatsionnoe-prostranstvo-razlichnye-podhody-k-ego-izucheniyu-i-osobennosti (дата обращения: 25.05.2022)

10. Ефремова М. А. Уголовно-правовая охрана информационной безопасности // Дисс…докт. юрид. наук – М.: 2017 - 427 с.

11. Жаде З.А. Хуако З.Ю. Информационная безопасность в контексте межэтнической напряженности // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2016. №1 (174). С.87-94

12. Жаров А.С. Конституционно-правовое регулирование информационной безопасности личности в Российской Федерации // Дисс…канд. юрид. наук. - М.: 2006 - 215 с.

13. Закон РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» // Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448

14. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» // «Российская газета» от 21 сентября 1993 г. № 182

15. Зиновьева Е. С. Международное сотрудничество по обеспечению информационной безопасности: проблемы, субъекты, перспективы // Дисс. на соискание уч. степени доктора наук./ Москва, 2017 - 332 с.

16. Информационное право : учебник для вузов / М. А. Федотов [и др.] ; под редакцией М. А. Федотова. М.: Издательство Юрайт, 2020. 497 с.

17. Коблова Ю.А. Совершенствование институционального механизма обеспечения информационной безопасности РФ // Информационная безопасность регионов. 2014. №3 (16). С. 66-70

18. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ // Собрание законодательства Российской Федерации от 7 января 2002 г. № 1 (часть I) ст. 1

19. Комментарий к Федеральному закону от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (Савченко А.И., Федоров А.Н.). - (постатейный, издание второе, перераб. и доп.). – «Деловой двор», 2021.

20. «Конвенция о защите прав человека и основных свобод» (Заключена в г. Риме 04.11.1950) (вместе с «Протоколом [N 1]» (Подписан в г. Париже 20.03.1952), «Протоколом N 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом N 7» (Подписан в г. Страсбурге 22.11.1984)) [Электронный ресурс] // КонсультантПлюс: справочно-правовая система / Режим доступа: URL: http://base.www.consultant.ru/ (дата обращения 01.02.2022 г.)

21. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28 января 1981 г.) //Собрание законодательства РФ от 03.02.2014 № 5 ст. 419

22. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // Собрание законодательства РФ 2014. №15. ст.1691

23. Королев И.Д. Актуальные проблемы разработки, внедрения и применения систем электронного документооборота в действующих и перспективных автоматизированных системах, обрабатывающих конфиденциальную информацию // Молодой ученый, 2018, № 13 (199). С. 45-50

24. Крылов Г. О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации // Дисс. … канд. юрид .наук – М.: 2007. 327 с.

25. Кулаков А.Н., Маховенко Е.Б. Криптографические методы обеспечения информационной безопасности на основе идентификаторов в широковещательных системах// Информационное противодействие угрозам терроризма. 2009. № 13 С. 58-60

26. Лименько, Л. Г. Отдельные аспекты правового регулирования информационной безопасности // Молодой ученый. 2017. № 45 (179). С. 118-121.

27. Мещерякова А. «Сравнение Доктрин ИБ РФ 2000 года и 2016 года» [Электронный ресурс] // НвсФ ФГУП «НТЦ «Атлас»/ Режим доступа: https://www.atlas (дата обращения: 20.02.2022)

28. Мысев А.Э., Морозов Н.В. Правовое регулирование информационной безопасности в Российской Федерации // Отечественная юриспруденция. 2019. №3 (35). С. 51-55

29. Николаев, И. А. Правовое обеспечение информационной безопасности РФ // Молодой ученый. 2019. № 47 (285). С. 344-346.

30. Ожегов С.И. Словарь русского языка. – М, 1989. 953 с.

31. Основы законодательства Российской Федерации о нотариате (утв. ВС РФ 11.02.1993 N 4462-1) // «Российская газета» от 13 марта 1993 г.

32. Попов Л. Л. Информационное право: учебник / Л. Л. Попов, Ю. И. Мигачев, С. В. Тихомиров. М. : Норма : Инфра-М, 2019. 496 с.

33. Постановление Правительства РФ от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» // Собрание законодательства Российской Федерации от 25 июля 2005 г. № 30 ст. 3165

34. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в

информационных системах персональных данных» // Собрание законодательства Российской Федерации от 5 ноября 2012 г. № 45 ст. 6257

35. Постановление Правительства РФ от 06.07.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации» [электронный ресурс] // Режим доступа: http://static.government.ru/media/acts/files/0001201507080013.pdf дата обращения: 15.07.2022)

36. Постановление Правительства Российской Федерации от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [электронный ресурс] // Режим доступа: http://publication.pravo.gov.ru/Document/View/0001201511200006 дата обращения: 18.08.2022)

37. Постановление Правительства РФ от 12.10.2020 № 1674 «О проведении эксперимента по созданию, переводу и развитию государственных информационных систем и их компонентов на единой цифровой платформе Российской Федерации «ГосТех» // Собрание законодательства Российской Федерации 2020г. № 42 ст. 6637

38. Постановление Правительства РФ от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» [электронный ресурс] /Право/ Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202207190035 дата обращения: 27.08.2022)

39. Постановление Правительства РФ от 22.08.2022 № 1478 «Об утверждении требований к программному обеспечению, в том числе в составе программно-аппаратных комплексов, используемому органами государственной власти, заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, Правил согласования закупок иностранного программного обеспечения, в том числе в составе программно-аппаратных комплексов, в целях его использования заказчиками, осуществляющими закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации, а также закупок услуг, необходимых для использования этого программного обеспечения на таких объектах, и Правил перехода на преимущественное использование российского программного обеспечения, в том числе в составе программно-аппаратных комплексов, органов государственной власти, заказчиков, осуществляющих закупки в соответствии с Федеральным законом «О закупках товаров, работ, услуг отдельными видами юридических лиц» (за исключением организаций с муниципальным участием), на принадлежащих им значимых объектах критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202208260051 дата обращения: 05.09.2022)

40. Приказ ФСБ России от 24.07.2018 № 366 «О Национальном координационном центре по компьютерным инцидентам» (вместе с «Положением о Национальном координационном центре по компьютерным инцидентам»)

41. Проект Постановления Правительства РФ «Об утверждении Положения о единой цифровой платформе Российской Федерации «ГосТех» и внесении изменений в постановление Правительства Российской Федерации от 6 июля 2015 г. № 676» [электронный ресурс] / Режим доступа: https://regulation.gov.ru/projects#npa=132245 дата обращения: 24.10.2022)

42. Распоряжение Правительства Российской Федерации от 05.03.2022 №430-р // Собрание законодательства Российской Федерации 2022 №11 ст. 1748

43. Томилов И.О. Трифанов А.В. Поиск уязвимостей в программном обеспечении без наличия исходного кода// Интерэкспо Гео-Сибирь.2017. №2 С. 75-80

44. Уварова Ю.А. Поддержка принятия решений в аудите информационной безопасности информационных систем персональных данных// Информационное противодействие угрозам терроризма, 2010 № 14 С. 15-17

45. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ // Собрание законодательства Российской Федерации от 24 декабря 2001 г. № 52 (часть I) ст. 4921

46. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. N 25 ст. 2954

47. Указ Президента РФ от 06.03.1997 № 188 «Об утверждении Перечня сведений конфиденциального характера»// Собрание законодательства Российской Федерации, 2015, N 29, ст. 4473

48. Указ Президента РФ от 6 октября 2004 г. № 1286 «Вопросы Межведомственной комиссии по защите государственной тайны» // Собрании законодательства Российской Федерации от 11 октября 2004 г. № 41 ст. 4024

49. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»

[электронный ресурс] /Право/ Режим доступа: http://publication.pravo.gov.ru/ (дата обращения: 20.05.2022)

50. Указ Президента РФ от 22.12.2017 №60 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»

51. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] Режим доступа: http://publication.pravo.gov.ru/ (дата обращения: 02.06.2022)

52. Указ Президента РФ от 01.05.2022 №250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // Российская газета - Федеральный выпуск № 95(8743)

53. «Устав телеграфический» / Свод законов Российской империи. Том двенадцатый. 1857 г. – 65 с.

54. Федеральный закон от 03.04.1995 №40-ФЗ «О федеральной службе безопасности» // Собрание законодательства Российской Федерации от 10 апреля 1995 г. № 15 ст. 1269

55. Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» // Собрание законодательства Российской Федерации от 19 июля 1999 г. № 29 ст. 3697

56. Федеральный закон от 31.05.2002 № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации» (с изм. и доп., вступ. в силу с 01.03.2022) // Собрание законодательства Российской Федерации от 10 июня 2002 г. № 23 ст. 2102

57. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне»// Собрание законодательства Российской Федерации от 9 августа 2004 г. № 32 ст. 3283

58. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание

законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3448

59. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»// Собрание законодательства Российской Федерации от 31 июля 2006 г. № 31 (часть I) ст. 3451

60. Федеральный закон от 28.12.2010 №390-ФЗ «О безопасности» // Собрание законодательства Российской Федерации от 3 января 2011 г. № 1 ст. 2

61. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» // Собрание законодательства Российской Федерации от 28 ноября 2011 г. № 48 ст. 6724

62. Федеральный закон от 05.04.2013 №44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» // Собрание законодательства Российской Федерации, 2013 № 14 ст. 1652

63. Федеральный закон от 14.07.2022 № 266-ФЗ «О внесении изменений в Федеральный закон «О персональных данных», отдельные законодательные акты Российской Федерации и признании утратившей силу части четырнадцатой статьи 30 Федерального закона «О банках и банковской деятельности» [Электронный ресурс] Режим доступа: http://publication.pravo.gov.ru/Document/View/0001202207140080 (дата обращения: 02.08.2022)

64. Федорец О.Н. «Комбинированная система защиты программного обеспечения от несанкционированного использования» // ФГУ «3 ЦНИИ Минобороны России», г. Москва, 2016 С.111-118