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

Института 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 «Проблемы правового регулирования информационной безопасности»

Обучающийся Б.В. Виноградов
(инициалы фамилия) (личная подпись)

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

2023

Аннотация

Актуальность темы выпускной квалификационной работы обусловлена интенсивным развитием информационной сферы в современной жизни и постоянным возрастанием информационных угроз. На сегодняшний день информационная сфера используется не только как один из способов улучшения жизни общества и расширения возможностей, но и как средство совершения преступлений, как современное орудие информационной войны.

Одним из важнейших средств обеспечения информационной безопасности выступает надлежащее правовое регулирование. Однако, на сегодняшний день можно отметить его отставание в данном вопросе. Цель исследования заключается комплексном исследовании правового регулирования информационной безопасности в Российской Федерации.

На основании обозначенной цели, можно определить следующие задачи исследования:

- изучить концептуальные и правовые основы понятия и содержания информационной безопасности;
- проанализировать систему правового регулирования информационной безопасности в РФ;
- изучить полномочия органов государственной власти в области обеспечения информационной безопасности;
- проанализировать понятие и классификацию угроз информационной безопасности;
- определить проблемы правового регулирования информационной безопасности;
- сформулировать основные направления совершенствования правового регулирования информационной безопасности в РФ.

Структура настоящего исследования состоит из введения, основной части разделённой на две главы, заключения и списка используемой литературы и используемых источников.

Оглавление

Введение

Актуальность темы исследования не вызывает сомнений, поскольку обусловлена интенсивным развитием информационной сферы в современных условиях. Информационная сфера на сегодняшний день оказывает серьезное воздействие на все отрасли общественных отношений. Вместе с тем, растет и число угроз в обозначенной области. На сегодняшний день информационная сфера используется не только как один из способов улучшения жизни общества и расширения возможностей, но и как средство совершения преступлений, как современное орудие информационной войны.

Последствия негативного воздействия информационных угроз могут быть очень разрушительны для общества. Одним из важнейших средств обеспечения информационной безопасности выступает надлежащее правовое регулирование. Однако, на сегодняшний день можно отметить его отставание в данном вопросе, что является недопустимым и оказывает негативное воздействие на обеспечение информационной безопасности. Правовое регулирование в обозначенной сфере характеризуется наличием пробелов, неточностей и отставанием в развитии. В свою очередь, необходимо отметить, что обеспечение информационной безопасности на сегодняшний день выходит за рамки одного государства, что также затрудняет правовое регулирование в данной сфере.

Учитывая темпы технологического прогресса и развития общественных отношений, нормативно-правовые акты своевременно должны обновляться, чтобы соответствовать современным реалиям, обеспечивать надежную охрану интересов граждан, организаций, государства в целом в сфере информации.

За последнее время вопрос правового регулирования информационной безопасности становился предметом диссертационных и монографических исследований таких учёных, как: Т.А. Полякова (2008 год, Правовое обеспечение информационной безопасности при построении информационного общества в России), А.Н. Жарова (2020 год, Теоретические

основания правового регулирования создания и использования информационной инфраструктуры Российской Федерации), С.А. Комаров (2019 год, Правовое регулирование обеспечения информационной безопасности и защиты персональных данных: монография), А.К. Жарова (2021 год, Правовое регулирование создания и использования информационной инфраструктуры в Российской Федерации. Монография), А.К. Дейнеко (2023 год, Публичное право в киберпространстве (публично-правовое регулирование информационных отношений). Монография).

Как видно, в последнее время, правовое регулирование информационной безопасности неоднократно подвергалось комплексным исследованиям. Однако, в виду интенсивного развития информационной сфере, правовое регулирование на сегодняшний день остается в отстающем положении, ряд вопросов остаются спорными и нерешенными.

Научная новизна исследования заключается в формулировании практических рекомендаций, направленных на совершенствование правового регулирования информационной безопасности в Российской Федерации.

Теоретическую основу исследования составили работы таких авторов, как: Е.В. Амосова, А.В. Бабаш, Е.К. Баранова, С.В. Баринов, Б.О. Баторов, А.Н. Болдырев, Т.А. Бражник, С.Р. Гостева, А.К. Дубень, А.К. Жарова, С.В. Иванов, М.Ф. Исаева, В.С. Козлов, Н.М. Колосова, В.Н. Лебедев, И.П. Михнев, С.В. Михнева, А.А. Стрельцов, А.В. Минбалеев, Н.В. Кроткова, С.В. Мухачев, К.Л. Костюченко, А.А. Харламова, М.А. Д.Д. Назарова, К.А. Наскидашвили, Т.А. Полякова, Г.Б. Романовский, М.А. Тишин, Ю.А. Трегубова, Ш.Г. Утарбеков, К.Н. Фадеева, А.Д. Цыплакова, В.А. Шестак, И.З. Шахсуварова, А.Ю. Яковлева-Чернышева, А.В. Дружинина и других авторов.

Объектом настоящего исследования является совокупность общественных отношений в сфере правового регулирования информационной безопасности Российской Федерации.

Предметом исследования выступают нормативно-правовые акты, материалы судебной практики, диссертационные и монографические

исследования, учебные издания и периодическая печать, посвященные исследованию правового регулирования информационной безопасности в Российской Федерации.

Цель исследования заключается в комплексном исследовании правового регулирования информационной безопасности в Российской Федерации.

На основании обозначенной цели, можно определить следующие задачи исследования:

- изучить концептуальные и правовые основы понятия и содержания информационной безопасности;
- проанализировать систему правового регулирования информационной безопасности в РФ;
- изучить полномочия органов государственной власти в области обеспечения информационной безопасности;
- проанализировать понятие и классификацию угроз информационной безопасности;
- определить проблемы правового регулирования информационной безопасности;
- сформулировать основные направления совершенствования правового регулирования информационной безопасности в РФ.

Нормативную основу исследования составили Конституция Российской Федерации, Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации», Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральный закон от

07.07.2003 № 126-ФЗ «О связи», Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи», Уголовный кодекс Российской Федерации и другие нормативно-правовые акты.

Структура настоящего исследования состоит из введения, основной части разделённой на две главы, заключения и списка используемой литературы и используемых источников.

Глава 1. Общая характеристика и правовое регулирование информационной безопасности в РФ

1.1 Концептуальные и правовые основы понятия и содержания информационной безопасности

Понятие информационной безопасности закреплено в Указе Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», согласно п.в, ч.2, ст. 1 указанного правового акта, «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» [46].

Как видно, данный правовой акт в основу понятия информационной безопасности закладывает словосочетание «состояние защищенности», объектами защиты от информационных угроз при этом выступают личность, общество и государство, что представляется очень правильным, поскольку информационная безопасность, действительно, складывается из безопасности личности, общества и государства. Безопасность государства не может быть обеспечена без обеспечения безопасности личности.

Для уяснения сущности определения легального понятия информационной безопасности проанализируем понятия, на которых оно основано. Так, под состоянием защищенности в современной доктрине предлагается понимать систему мер, направленных на предупреждение рисковых ситуаций, а также смягчение и ликвидацию их последствий. Под риском следует понимать вероятность наступления неблагоприятных условий, нарушение прав граждан, обусловленное внешними причинами[53, с. 71].

Защищенность должна обеспечиваться в соответствии с законом. То есть для защищенности необходимо использовать соответствующие формы и методы защиты прав.

Для обеспечения защищенности законодательством Российской Федерации предусматриваются различные формы и способы защиты. Традиционно под формой понимается способ наличия содержания, который непосредственно связан с ней и служащий его выражением, также под способом понимают определённые действия или совокупность действий, применяемые для осуществления какой-либо работы. В русском языке нет чёткого разграничения между способами и формами, кроме того из приведенного выше определения следует, что понятие форма определяют через способ. Понятие формы и способы непрерывно связанны между собой.

Некоторые учёные правоведы под формой защиты понимают определённые систематические действия произведённые уполномоченным на то лицом, совокупность внутренне согласованных организационных действий по защите охраняемых законом интересов и прав, осуществляемых в рамках одного правового режима [53, с. 71].

Любая форма защиты объединяет характерные и конкретные способы и соответствующие органы защиты. Традиционно в правовой доктрине выделяют две формы защиты: юридическая и неюридическая.

Юридическая форма защиты предусматривает возможность использования судебного порядка разрешения спора о защите прав. Согласно части 1 статьи 46 Конституции РФ каждый имеет право на защиту в судебном порядке [22].

Неюридическая форма защиты представляет собой совокупность применяемых мер, субъектом, уполномоченным самостоятельно и напрямую обращаться к органам за защитой своих прав, такой способ получил название, как самозащита.

Понятие информационной угрозы подробно будет рассмотрено в следующих параграфах работы, поэтому перейдем к рассмотрению объектов,

реализация которых, согласно легальному определению, не должна быть нарушена при надлежащем уровне обеспечения информационной безопасности - это конституционные права и свободы человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

Конституционные права и свободы человека и гражданина представляют собой важнейшие и незыблемые права и свободы, гарантируемые главным законом государства - Конституцией. Согласно данному правовому акту: «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются. Органы государственной власти и органы местного самоуправления, их должностные лица обязаны обеспечить каждому возможность ознакомления с документами и материалами, непосредственно затрагивающими его права и свободы, если иное не предусмотрено законом» [22].

Под уровнем жизни в современной доктрине понимается «обеспеченность населения необходимыми благами и степень удовлетворения индивидуальных потребностей человека в них. Качество жизни выражает меру индивидуальной доступности того, чем располагает общество (здоровье и здравоохранение, образование, отдых)» [8, с. 69]. Безусловно, нарушение информационной безопасности может приводить к ухудшению уровня и качества жизни человека, поскольку информационные угрозы, которые распространяются в средствах массовой информации и в телекоммуникационной сети «Интернет», на сегодняшний день вполне способны подорвать психическое здоровье человека и ухудшить качество его жизни.

Нарушение информационной безопасности может оказывать негативное влияние на суверенитет государства. Суверенитет представляет собой

важнейший признак государства, который состоит в возможности государственной власти самостоятельно реализовывать свою власть. На сегодняшний день актуальным стало понятие цифрового суверенитета, «реализация которого зависит от используемых государством цифровых технологий и их функциональных возможностей» [13, с. 28].

Построение личностных ориентиров зависит от многих факторов, где получение информации играет решающую роль. Обращение к работам нейроспециалистов показывает, что человеческий мозг потребляет все происходящее вовне, ничто не проходит бесследно (в том числе на подсознательном уровне). Это означает, что в наш век информационных технологий главенствующее значение приобретают формы коммуникаций, благодаря которым происходит передача соответствующей информации. Именно поэтому в оборот вводятся такие формулировки, как информационная война, информационная безопасность. Сейчас каналами передачи выступает цифровой мир, где строится ключевое информационное поле. А это мессенджеры, телеграм-каналы, социальные сети, чаты, имиджборды. Их особенность заключается и в том, что передача информации возможна вне пределов государственных границ и в режиме реального времени.

Кибермир отвоевывает у государства суверенные полномочия по идентификации личности. Во-первых, блокчейн пытается заменить выдачу традиционных удостоверений (паспортов, реестров) цифровыми аутентификаторами, которые в силу распространенности приобретают огромное значение (ники, аватары, IP-адрес, логины, пароли и т.д.). В виртуальном пространстве печатные документы менее пригодны, что минимизирует их использование в социальных отношениях. Во-вторых, уже есть опыт ряда стран по внедрению цифровой идентификации личности, параллельной различным удостоверениям, выдаваемым государственными органами. В этой части происходят ссылки на Швецию, где электронный документ BankID (внедренный банковскими организациями вне участия государства) применяется практически всем взрослым населением страны и

используется сейчас во взаимоотношениях с органами государственной власти для получения публичных услуг. С учетом того, что предоставление цифровых услуг - прерогатива коммерческих организаций, государство становится в зависимость от операторов связи, поставщиков софта, владельцев сетей [42, с. 27].

Децентрализация идет семимильными шагами, разнонаправленно размывая суверенные полномочия государства. Этот вектор развития носит последовательный характер, и, по-видимому, он необратим. В то же время идея контролируемого общества не снимается с повестки дня. Иной момент: государство постепенно утрачивает функции контролера. Ему приходится как минимум делить подобные функции, вовлекая в этот процесс нестандартных субъектов, где потребление и расходы, переведенные на электронные площадки, выступают самым удобным объектом [42, с. 28].

С помощью нарушения информационной безопасности также возможно создание угрозы для территориальной целостности Российской Федерации, поскольку с помощью распространения через интернет призывов к нарушению территориальной целостности вполне возможно оказание влияния на формирование в сознании общества необходимости провозглашения того или иного субъекта РФ. Очень непростая ситуация на сегодняшний день обстоит с республикой Крым и новыми территориями, вошедшими в состав нашего государства. В связи с этим распространение пропаганды относительно принадлежности данных регионов не к Российской Федерации, создает угрозу нарушению территориальной целостности.

Еще одним объектом, реализация которого может быть нарушена в результате создания информационных угроз, является устойчивое социально-экономическое развитие. Для развитого демократического правового государства характерно отсутствие политико-административных форм и методов воздействия на экономику страны, на поведение субъектов экономических отношений. Государство регулирует их только при помощи

экономических методов, прежде всего, разрабатывая специальные долгосрочные государственные программы по развитию экономики.

Необходимо отметить, что государство принимает непосредственное участие в некоторых наиболее важных отраслях экономики, таких как энергетика, атомная, оборонная промышленность, космонавтика, машиностроение, авиация, связь, чаще всего, государство в указанных случаях, осуществляет непосредственное управление, выступая в качестве собственника или держателя акций. Это создает определенную стабильность и гарантию безопасности для функционирования данных организаций и для общества в целом [15].

На сегодняшний день справедливо можно отнести Российскую Федерацию к числу стран с развитой экономикой. Безусловной является важная роль крупных объединений промышленных и финансовых предприятий в экономике мировых держав. Однако ряд ученых отмечают некоторую сложность в адаптации крупных групп производственных компаний к изменяющимся рыночным условиям в условиях трансформации экономики и введения различных экономических санкций со стороны иностранных государств в отношении России в последнее время. Так, на территории Крыма невозможно найти ни отделений крупных банков, действующих в России и в международном пространстве, ни операторов сотовой связи. Это связано с угрозой приостановления деятельности данных предприятий в зарубежных странах.

Таким образом, легальное определение информационной безопасности частично дублирует определение национальной безопасности, что позволяет говорить о том, что информационная безопасность выступает элементом национальной. Основными объектами защиты информационной безопасности закон называет личность, общество и государство. Целью обеспечения национальной безопасности выступают 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.

В современной доктрине понятие информационной безопасности определяется по-разному. Так, По мнению С.В. Иванов, под информационной безопасностью понимает «состояние высокой степени защищенности, при котором гарантируется реализация прав и свобод человека и гражданина в информационной сфере и максимально снижен риск негативного воздействия внутренних и внешних угроз» [14, с. 50]. Как видно из данного определения понятие информационной безопасности также определяется через категорию защищенности. Однако в данном случае, речь идет только о безопасности личности и не уделяется вниманию безопасности государства. Думается, что информационная безопасность сегодня является вопросом не только государственного масштаба, но и выходит за его пределы. Благодаря свойствам и способностям информационной сферы в современном мире, она может оказывать общемировое воздействие.

С.В. Баринов под информационной безопасностью понимает «состояния защищенности, при котором отсутствует риск, связанный с причинением информацией вреда здоровью и (или) физическому, психическому, духовному, нравственному развитию человека» [3, с. 102]. В данном определении автор описывает информационную безопасность личности, перечисляя вред, который может нанести информационная угроза человеку [26].

Под информационной безопасностью Б.Е. Кенжетаев понимает «защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры» [18, с. 37].

Т.А. Полякова и А.А. Стрельцова, информационную безопасность определяют, как «состояние защищенности национальных интересов РФ в

информационной сфере, которые складываются из комплекса сбалансированных интересов личности, общества и государства, от внутренних и внешних угроз, что не противоречит принципу обеспечения национальной безопасности в информационной области, указанному в Стратегии национальной безопасности» [35, С. 230]. Авторы данного определения делают акцент на безопасности государства, игнорируя при этом информационную безопасность личности, что также является объектом защиты, согласно Конституции и Стратегии национальной безопасности.

Д.Д. Назарова под информационной безопасностью предлагает понимать «состояние защищенности информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера (информационных угроз, угроз информационной безопасности), которые могут нанести неприемлемый ущерб субъектам информационных отношений» [31, с. 349].

К.Н. Фадеева трактует информационную безопасность как «совокупность средств обеспечения информационного суверенитета страны, защиту информационной сферы от внешних и внутренних информационных угроз. Эта безопасность должна включать в себя эффективное противодействие совокупности информационных угроз» [53, с. 36]. Относительно данного определения, представляется целесообразным отметить, что в данном случае не учитывается безопасность личности и общества, речь идет только о государственной безопасности в информационной сфере.

А.В. Бабаш и Е.К. Баранова определили, что «информационная безопасность – это составляющая национальной безопасности, процесс управления угрозами и опасностями, государственными и негосударственными институтами, отдельными гражданами, при котором обеспечивается информационный суверенитет Российской Федерации» [2, с. 47]. Указанное определение рассматривает информационную безопасность как часть национальной, поскольку официальные определения практически дублируют друг друга. Данные авторы обращают внимания, что

информационные угрозы сегодня представляют собой угрозы национальной безопасности, что представляется справедливым. Однако, рассматривать информационную безопасность, как процесс представляется не совсем корректным.

И.З. Шахсуварова дает следующее определение информационной безопасности – «это комплексная система, цель функционирования которой – защита объектов (информация, знания, информационные системы), принадлежащих финансово-хозяйственной, политической, военной, технологической сфер деятельности, от разного рода угроз (несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения) с применением программных, технических, методических, информационных и правовых средств, использующих отдельные лица или специализированные подразделения и специалисты государственных органов» [64, с. 213]. Данное определение представляется, в определенной степени, ограниченным, поскольку перечисляет конкретно сферы защиты и виды угроз. При этом, информация сегодня касается практически всех без исключения сфер деятельности, а угрозы выходят за пределы несанкционированного доступа, использования, раскрытия, нарушения, модификации или уничтожения информации. Кроме того, объектами защиты И.З. Шахсуварова называет саму информацию, в то время, как наиболее корректно говорить о личности, обществе и государстве [64, с. 213]. Думается, что данное определение более приемлемо непосредственно для компьютерной информации.

Как видно из анализа теоретических определений понятия информационной безопасности, большинство авторов берут за основу законодательное определение информационной безопасности как состояния защищенности от информационных угроз. Однако ряд авторов предлагают определять исследуемую категорию как систему мер защиты, как процесс управления информационными угрозами. Ряд авторов, в своих определениях не уделяет достаточного внимания безопасности личности и общества,

останавливаясь только на безопасности государства, рассматривая информационную безопасность, как часть национальной безопасности, однако без безопасности личности и общества невозможно существование безопасности государства.

Нельзя оставить без внимания тот факт, что проанализированные определения понятия информационной безопасности не раскрывали сам термин «информационная». Также, как и легальное определение, исследуемого понятия, они ограничивались указанием на защиту от информационных угроз. В свою очередь, при определении понятия информационных угроз, законодатель также не раскрывает термин «информационные». Для определения данного понятия необходимо обратиться к Федеральному закону № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который под информацией понимает «сведения (сообщения, данные) независимо от формы их представления» [54].

На основании вышеизложенного представляется целесообразным дополнить легальное определение данными из ФЗ № 149, чтобы оно выглядело следующим образом: «информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних угроз в сфере распространения сведений, сообщений и данных, 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».

Таким образом, проанализировав понятие информационной безопасности в доктрине и в современном праве, можно отметить, что легальное определение информационной безопасности частично дублирует определение национальной безопасности, что позволяет говорить о том, что информационная безопасность выступает элементом национальной.

Основными объектами защиты информационной безопасности закон называет личность, общество и государство. Целью обеспечения национальной безопасности выступают 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.

Как видно из анализа теоретических определений понятия информационной безопасности, большинство авторов берут за основу законодательное определение информационной безопасности как состояния защищенности информационных угроз. Однако ряд авторов предлагают определять исследуемую категорию как систему мер защиты, как процесс управления информационными угрозами. Ряд авторов, в своих определениях не уделяет достаточного внимания безопасности личности и общества, останавливаясь только на безопасности государства, рассматривая информационную безопасность, как часть национальной безопасности, однако без безопасности личности и общества невозможно существование безопасности государства.

Нельзя оставить без внимания тот факт, что проанализированные определения понятия информационной безопасности не раскрывали сам термин «информационная». Также, как и легальное определение, исследуемого понятия, они ограничивались указанием на защиту от информационных угроз. В свою очередь, при определении понятия информационных угроз, законодатель также не раскрывает термин «информационные». Для определения данного понятия необходимо обратиться к Федеральному закону № 149-ФЗ «Об информации, информационных технологиях и о защите информации», который под информацией понимает «сведения (сообщения, данные) независимо от формы их представления» [54].

На основании вышеизложенного представляется целесообразным дополнить легальное определение данными из ФЗ № 149, чтобы оно выглядело следующим образом: «информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних угроз в сфере распространения сведений, сообщений и данных, 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».

1.2 Система правового регулирования информационной безопасности в Российской Федерации

Согласно Указу Президента РФ № 646, одними из средств обеспечения информационной безопасности, помимо организационных и технических, являются также правовые средства [46].

Правовое регулирование информационной безопасности формировалось в два этапа. Его основы были заложены еще в середине 90-х годов. Основополагающим нормативно-правовым актом в тот период времени быа Конституция РФ, которая закрепляла основные права и свободы человека и гражданина, касающиеся свободы поиска, получения, передачи, производства и распространения информации любым законным способом [22].

Нормативно-правовыми актами, реализующими информационное обеспечение инновационных технологий, являлись федеральные законы, принятые в 1995 году: «О связи» [61], «Об информации, информатизации и защите информации» [62]. В последнем указанном акте давалось, а именно в ст. 2, определение информации, под которой понимались «сведения о лицах, предметах, фактах, событиях, явлениях и процессах, независимо от формы их

представления». Указанные законы регламентировали правовые отношения в сфере обмена информацией и обработки информации с использованием новых технологий. Данные федеральные законы давали юридическое понятие различным компонентам информационной технологии как объектам правовой охраны, определяли категории доступа к информации ограниченного доступа, устанавливали права и обязанности лица, которое владеет объектами правовой охраны.

Важную роль в обеспечении информационной безопасности сыграл Указ Президента РФ 03.04.1995 г. № 334 от «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также представления услуг в области шифрования информации» [47].

Указ запрещал пользоваться государственным органам, организациям и предприятиям шифровальными и криптографическими системами, техническими средствами хранения, обработки и передачи информации, которые не имеют сертификата. Так же, согласно Указу, требуется: усилить прокурорский надзор за соблюдением законодательства в сфере разработки производства, реализации и эксплуатации шифровальных средств и предоставления услуг в области шифрования информации; создать федеральный центр защиты экономической информации [47].

Итак, до 1997 года в России не была создана эффективная правовая система защиты информации, в связи с тем, что отсутствовала одна из важных составляющих - уголовно-правовые средства защиты.

Второй этап развития законодательства в сфере безопасности информации начинается с введением в УК РФ главы 28, которая закрепляет преступления в сфере компьютерной информации, включая в себя три состава преступления, объединенных единым объектом посягательства - общественные отношения, связанные с использованием компьютерной информации [45].

9 сентября 2000 года была утверждена Президентом РФ «Доктрина

информационной Безопасности Российской Федерации». В данной Доктрине закреплялись виды и источники угроз информационной безопасности РФ, организационные основы системы обеспечения информационной безопасности РФ, методы обеспечения информационной безопасности РФ в различных сферах жизни общества и иные положения. На данный момент действует Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 05.12.2016 №646 [46]. Она содержит в себе практически аналогичные положения, но уже более соответствующие современным реалиям.

Исследование современного этапа развития правового регулирования информационной безопасности необходимо начинать с главного закона Российской Федерации - Конституции, которая содержит ряд статей, посвященных информационной безопасности. Так, ч.2 ст. 23 закрепляет право каждого на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ст. 24 закрепляет, что «сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются». Ч. 4 ст. 29 устанавливает, что «каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом». Ст. 42 закрепляет право каждого на достоверную информацию [22].

Следующим правовым актом, с помощью которого осуществляется правовое регулирование информационной безопасности, является Федеральный закон от №149-ФЗ «Об информации, информационных технологиях и о защите информации» , который закрепляет понятие информации, информационных технологий, информационных систем. Согласно данному правовому акту, «информация представляет собой сведения (сообщения, данные) независимо от формы их представления; информационные технологии - процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов» [54].

Под информационной системой следует понимать «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [54].

ФЗ №149 также закрепляет виды информации, распространение которой запрещается сюда, относится информация, которая «направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти или вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность» [54].

Федеральный закон «Об информации» устанавливает правила распространения информации в социальных сетях. Ст. 10.6 устанавливает запрет на распространение информации, порочащей честь и достоинство кого-либо, информации о способах, методах разработки, изготовления и использования наркотических средств, информации о способах совершения самоубийства, а также призывов к совершению самоубийства [54].

Указанный правовой акт также закрепляет порядок ограничения доступа к информации, устанавливает основы защиты информации. Защита информации, согласно данному Федеральному закону, представляет собой «принятие правовых, организационных и технических мер, направленных на:

- обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;
- соблюдение конфиденциальности информации ограниченного доступа;
- реализацию права на доступ к информации» [54].

Обладатель информации, оператор информационной системы в случаях, согласно ФЗ № 149, обязаны обеспечить:

- «предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;
- своевременное обнаружение фактов несанкционированного доступа к информации;
- предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;
- недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;
- возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;
- постоянный контроль за обеспечением уровня защищенности информации;
- нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации» [54].

Следующим правовым актом, играющим важнейшую роль в правовом регулировании информационной безопасности, является Указ Президента РФ № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Данный правовой акт, как уже отмечалось, содержит само понятие информационной безопасности, понятие угроз информационной безопасности, обеспечения информационной безопасности, закрепляет систему и средства обеспечения информационной безопасности и иные понятия, имеющие значение для уяснения сущности информационной безопасности в Российской Федерации [46].

Доктрина информационной безопасности определяет «стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации» [46]. К примеру, «стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности» [46].

«Стратегической целью обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры» [46].

«Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

- противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;
- пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных

технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

– повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

– повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

– повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

– повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

– обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет

повышения защищенности соответствующих информационных технологий;

- совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;
- повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;
- нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей» [46].

Так как информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства, федеральные законы, регламентирующие информационную безопасность, издаются в различных сферах жизни общества. Например, Федеральный закон «Об электронной подписи» [55], который регулирует отношения в области использования электронных подписей при совершении различных сделок, оказании государственных услуг, исполнении государственных функций, с целью удостоверения личности лица и недопущения нарушения несанкционированного доступа к определённой информации; Федеральный закон «О противодействии экстремистской деятельности», который закрепляет ограничения по распространению информации, содержащей признаки экстремистской направленности, и иные федеральные законы [56].

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» также имеет важнейшее значение для правового регулирования информационной безопасности в Российской Федерации. Данный правовой акт «регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры

Российской Федерации в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак» [58].

Важнейшее значение в обеспечении информационной безопасности играют нормы административного и уголовного права, которые предусматривают наказание за нарушение информационной безопасности. КоАП РФ содержит ряд составов правонарушений, которые заключаются в распространении небезопасной информации. В частности, сюда относятся распространение пропаганды наркотиков, психотропных веществ, закиси азота, иных веществ, способных причинить вред здоровью, пропаганды нетрадиционных сексуальных отношений, педофилии или смены пола. За совершение данных деяний предусмотрена административная ответственность [19].

Кроме того, КоАП РФ содержит отдельную, посвященную правонарушениям в сфере информации. Глава 13 КоАП РФ предусматривает административную ответственность за нарушение правил защиты информации, за незаконную деятельность в сфере защиты информации, за разглашении информации с ограниченным доступом, за неисполнение обязанностей организатором распространения информации в сети «Интернет», неисполнение обязанностей, предусмотренных законодательством о деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации [19].

Административная ответственность за правонарушения в сфере информационной безопасности, в основном, представлена в виде небольшого штрафа, что представляется несоразмерным вреду, который причиняется рядом правонарушений в сфере безопасности информации.

За наиболее серьезные деяния в сфере безопасности информации законодательством Российской Федерации предусмотрена уголовная ответственность. Уголовный кодекс содержит главу, посвященную преступлениям в сфере компьютерной информации, а также отдельные

составы, которые так или иначе связаны с нарушением информационной безопасности. В науке, чаще всего, при характеристике преступлений в сфере информационной безопасности, используется термин «преступление в сфере информационно-телекоммуникационных технологий». Ряд авторов вообще считают некорректным выделение понятия данного вида преступлений, полагая достаточным говорить об отдельных аспектах информационной преступности. Другие авторы считают необходимым выделения отдельного понятия и признаков преступлений в сфере информационных технологий, объясняя это широким распространением данных преступлений и серьезным ущербом, причиняемым совершением преступлений в данной сфере [34, с. 53].

Прежде всего, необходимо отметить, что преступления, совершаемые в сфере информации, не ограничиваются главой УК РФ, включающей преступления против компьютерной информации. Распространение небезопасной информации с помощью интернета, к примеру, имеет место при множестве иных преступных деяний на сегодняшний день, в частности, в сфере оборота наркотических средств; контрабанде запрещенных к обороту товаров; преступлениях, нарушающих авторские права; вербовке лиц для совершения терактов [28].

УК РФ выделяет 5 видов преступлений в сфере компьютерной информации, в соответствии со ст. 272, 273, 274, 274.1. и 274.2. Преступление, закрепленное в ст. 272 называется «неправомерный доступ к компьютерной информации». В примечании к данной статье дано определение понятия компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [45]. Понятия сообщений, данных, электрических сигналов раскрываются в ФЗ «Об информации» [54].

Под неправомерным доступом следует понимать совершение определенных действий, направленных на получение возможности ознакомиться и (или) воспользоваться компьютерной информацией. Эти действия могут выражаться в использовании специальных программ или

технических возможностей для взлома установленных защитных систем и проникновении в компьютер или иную информационную систему под видом законного пользователя, не имея на это прав и законных оснований [38, с. 3].

Преступлением данные действия будут только при наступлении определенных последствий, указанных в законе, а именно: уничтожение, блокирование, модификацию или копирование данной информации.

Следующим видом преступлений в сфере компьютерной информации являются деяния, предусмотренные ст. 273 УК РФ - создание, использование и распространение вредоносных программ. Важным моментом является то, что для привлечения к ответственности по ст. 273 УК РФ не требуется наступление каких-либо последствий [45]. Достаточно даже одного факта создания такой программы, который будет выражен в написании подобной вредоносной программе на любом носителе, даже на бумаге с использованием полного алгоритма вредоносных действий.

Необходимо отметить, что составы преступлений, предусмотренных ст. 272 и 273 имеют некоторую схожесть. Так, в обоих случаях, совершение преступления сопряжено с неправомерным доступом к компьютерной информации и ведет к уничтожению, блокированию, модификации либо копированию информации, а также взламывает средства защиты данной информации. К примеру созданная вредоносная программа может использоваться для доступа и копирования информации. В данном случае будет сложно установить по какой именно статье следует квалифицировать данное деяние. Разграничения указанных составов можно проводить по предмету преступления. Так, в случае со ст. 272 - предметом преступления будет выступать только охраняемая законом информация, а в случае со ст. 273 - это может быть абсолютно любая информация. Разграничивать данные составы следует также по наличию последствий, так, состав, предусмотренный ст. 272 является материальным - является обязательным наступление последствий в виде уничтожения, блокирования, модификации

либо копирования. Для квалификации деяния по ст. 273 наличия последствий не требуется.

Следующим видом преступлений в сфере компьютерной информации уголовный закон называет нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей - ст. 274 УК РФ [45]. Нарушение указанных правил может иметь достаточно серьезные последствия, поскольку в современном мире компьютерная информация и информационно-телекоммуникационные сети играют важную роль. Сбои в работе указанных систем могут повлечь огромные материальные потери для общества и государства. К примеру, нередки случаи, когда перебои в интернете при снятии клиентом банка наличных через соответствующий терминал могут привести к невыполнению данной операции, но списание средств при этом будет осуществлено [34, с. 52]. В свою, очередь, для изучения правил, указанных в рассматриваемой норме, следует обращаться к другим нормативно-техническим актам и специальным инструкциям, таким как ФЗ «О связи», инструкции конкретного компьютерного предприятия.

Субъектом указанного состава всегда является должностное лицо, на которое его должностными обязанностями возложена обязанность надлежащего обращения с соответствующей информацией и специальными данными [30].

Преступление, предусмотренное ст. 274.2 УК РФ «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования», является совсем новым, закрепленным в Уголовном кодексе в 2022 году. Данное деяние было криминализировано в связи с необходимостью защиты безопасности сети «Интернет», поскольку участились случаи «взлома», хакерские атаки различных значимых платформ в связи с началом РФ военной операции [45].

В п.б. ч. 2 ст. 228.1 УК РФ сбыт наркотических и психотропных веществ с помощь сети «Интернет» является квалифицированным составом. В ст. 242 УК РФ «Незаконные изготовление и оборот порнографических материалов или предметов», использование сети «Интернет» также выступает квалифицирующим обстоятельством и закрепляется в ч. 2 данной статьи [45].

С января 2021 года в УК РФ был внесен дополнительный квалификационный признак в ст. 354.1 УК РФ (реабилитация нацизма). Он приравнивает нарушения по этой статье, которые совершены с использованием интернета, к нарушениям с использованием СМИ [45].

Достаточно резонансными делами были многочисленные доведения до самоубийства с использованием социальных сетей. Подростки, вступавшие в так называемые «группы смерти» («Синий кит», «Разбуди меня в 4.20» и др.), выполняли определенные задания, последним из которых было совершение суицида. В УК РФ использование интернета для доведения до самоубийства выступает в качестве квалифицирующего обстоятельства и закрепляется в п. «д» ч.2 ст. 110 УК РФ. Ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства закрепляется в ч.2 ст.110.2 УК РФ и предусматривает до 15 лет лишения свободы [45].

Таким образом, можно отметить, что законодательство Российской Федерации о безопасности в сфере информации начало формироваться еще с 1991 года. На первом этапе отмечается издание различных нормативно-правовых актов, которые включают в себя отдельные направления по обеспечению информационной безопасности. Второй же этап ознаменован принятием Доктрины информационной безопасности, Федерального закона «Об информации, информационных технологиях и о защите информации», Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» и закреплении в Уголовном кодексе Российской Федерации, основные общественно-опасные деяния в сфере информации. В последующем требуется развитие данного направления с

целью предупреждения и пресечения посягательств на данную сферу жизни общества.

1.3 Полномочия органов государственной власти в области обеспечения информационной безопасности

Ключевую роль в области обеспечения информационной безопасности играют органы государственной власти, которые ограничивают распространение вредоносной информации и пропаганды, обеспечивают сохранность информации, защищают информацию от несанкционированного доступа. Согласно ст. 12 ФЗ «Об информации, информационных технологиях и защите информации», «государственное регулирование в сфере применения информационных технологий предусматривает:

- регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных законом;
- развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;
- создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети «Интернет» и иных подобных информационно-телекоммуникационных сетей;
- обеспечение информационной безопасности детей» [54].

«Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

- участвуют в разработке и реализации целевых программ применения информационных технологий;

– создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации» [54].

Важнейшую роль в обеспечении информационной безопасности играет Президент РФ. В современной доктрине отмечается постоянно возрастающее значение роли президента как в процессе информатизации, так и в обеспечении безопасности информации [21, с. 18].

Президент в соответствии с Конституцией Российской Федерации является главой государства. Он является представителем государственной власти, который стоит выше, чем три другие ветви государственной власти, а именно: законодательная, судебная, исполнительная. При этом президент не относится ни к одной из указанных ветвей власти.

На президента Российской Федерации возложены в соответствии с законодательством определённые полномочия, а также функции по взаимодействию с нижестоящими ветвями власти. Кроме того, президент участвует в процессе организации деятельности федеральных органов государственной власти, но при этом не имеет статуса главы ни одной из указанных ветвей [48].

В соответствии с Конституцией Российской Федерации, Президент России обладает широким кругом полномочий, которые позволяют ему оказывать влияние на работу всех государственных механизмов, а также политику, реализуемую государством [22]. Например, необходимо отметить, важную роль президента с точки зрения организации деятельности исполнительной власти, которая реализуется через формирование системы органов исполнительной власти и осуществления контроля над практическим осуществлением полномочий этих органов.

Президент своим Указом № 646 утвердил важнейшую в сфере информационной безопасности Доктрину, которая не только формулирует основные информационные угрозы, но и обосновывает направления

обеспечения информационной безопасности. Согласно данной Доктрине, «Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами. Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами. Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации» [46].

Согласно Доктрине информационной безопасности, «организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности» [46].

«Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

– законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать,

получать, передавать, производить и распространять информацию любым законным способом;

- конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;
- соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;
- достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;
- соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации» [46].

«Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

- обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;
- оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;
- планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;
- организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-

технического, информационно-аналитического, кадрового и экономического обеспечения;

– выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области» [46].

Как видно, Президент РФ не только утверждает нормативные документы, регулирующие основы информационной безопасности, но и осуществляет контроль за деятельностью органов, исполняющих данные акты, защищает права граждан на обеспечение их безопасности в информационной сфере, определяет направления политики в обозначенной области [49].

Следующим государственным органом, который имеет важное значение в обеспечении информационной безопасности, является Федеральная Служба Безопасности (далее - ФСБ РФ), в рамках которой были созданы специальные отделы, занимающиеся информационной безопасностью государства. К примеру, Центр информационной безопасности призван заниматься расследованием преступлений в сфере информационной безопасности, в частности, связанных с незаконным распространением персональных данных. Центр по компьютерным инцидентам отслеживает различные компьютерные атаки на критическую инфраструктуру российского государства [29, с. 132].

Федеральная Служба Охраны Президента защищает информацию, составляющую государственную тайну от несанкционированного доступа, в том числе, иностранных разведывательных служб, обеспечивает безопасную специальную связь президенту.

Важные функции по обеспечению информационной безопасности возложены на Министерство цифрового развития, связи и массовых

коммуникаций Российской Федерации (Минцифры). Данное ведомство координирует функционирование информационных ресурсов в нашем государстве, таких как информационно-телекоммуникационная сеть «Интернет», телевидение и радиовещание, регулирует связь и вопросы биометрии.

Подконтрольной Минцифры выступает Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) России. На сегодняшний день Роскомнадзор выполняет особо важные функции, что связано с тем, что на данный момент ведется настоящая информационная война. Роскомнадзор блокирует размещение фейковой информации в интернете и телевидении, запрещает передачи, угрожающие информационной безопасности государства. Огромное количество неправдивой информации сегодня размещается в интернет ресурсах, эта информация направлена на подрыв доверия граждан к государственной власти. С началом специальной военной операции имело место огромное количество призывов в социальных сетях к протестам против власти российского государства. Это угрожало безопасности Российской Федерации, что говорит о важности своевременного блокирования подобной информации и привлечения распространителей к ответственности [52].

Прокуратура РФ также выполняет функции обеспечения информационной безопасности. Она представляет собой централизованную совокупность органов, которые осуществляют надзорные и контрольные функции над исполнением законов РФ и положений Конституции РФ.

С момента образования следственного комитета он был включён в состав органов прокуратуры. Однако позднее был выделен в отдельный орган, и получил самостоятельный статус Федерального государственного органа, действующего на основании законодательства Российской Федерации, с полномочиями в области уголовного судопроизводства.

Специальные отделы в системе Министерства Внутренних дел также уполномочены заниматься расследованием преступлений в сфере компьютерной информации и информационных технологий.

Безусловно, нельзя оставить без внимания роль судебных органов власти в обеспечении информационной безопасности. Конституция Российской Федерации в статье 46 гарантирует каждому гражданину право на судебную защиту [22]. Судебная власть рассматривает дела о нарушении прав граждан в сфере информационной безопасности.

Судебный порядок защиты предполагает подачу искового заявления на нарушение его прав, а в некоторых случаях судебный порядок рассмотрения дела проходит в порядке уголовного судопроизводства. Согласно ч. 3 ст. 118 Конституции судебную систему составляют Конституционный Суд Российской Федерации, Верховный Суд Российской Федерации, федеральные суды общей юрисдикции, арбитражные суды, мировые судьи субъектов Российской Федерации [22].

Так, одним из наиболее распространенных способов защиты прав в случае нарушения информационных прав граждан, является восстановление нарушенного права или восстановление положения, которое имело место до того, как было нарушено право. Применение этого способа уместно только в случаях, когда это восстановление возможно. К примеру, в отношении распространения неправдивых, порочащих сведений, с помощью использования СМИ, необходимо последующее опровержение путем опубликования в СМИ.

Рассмотрим пример из судебной практики. Так, ООО «Брянскгражданпроект» обратилось с иском в арбитражный суд Брянской области с иском к редакции ООО «Брянский рабочий» о защите деловой репутации и взыскании с ответчика 400 000 рублей [40].

Из обстоятельств дела следовало, что СМИ опубликовали материал, на основании которого истец обвинялся в незаконных денежных

операциях и притворных сделках. Репутация истца очень сильно пострадала ввиду данной публикации. В результате ООО понесло значительные убытки.

Для доказательств своей правоты, истцом была предоставлена вся необходимая документация суду, подтверждающая законность совершаемых обществом сделок. Таким образом, было установлено, что сведения, опубликованные ответчиком, не соответствовали действительности.

В результате этого, на ответчик судом было возложено обязательство написать опровержение и опубликовать его, а также выплатить ООО денежную компенсацию [40].

Важную роль в обеспечении информационной безопасности играют государственные органы законодательной власти, которые создают законы, регулирующие отношения в сфере информационно безопасности. Деятельность государственных органов и деятельность граждан должна основываться на букве закона. В Доктрине информационной безопасности отмечается, что деятельность государственных органов в сфере информационной безопасности должна основываться на принципе законности. В правовом государстве закон должен быть превыше всего. Кроме того, одним из проявлений принципа законности в РФ также можно назвать верховенство Конституции, которая закрепляет важнейшие начала основ государственного устройства и прав и свобод человека. Все законодательные акты опираться на Конституцию и не могут противоречить положениям, закрепленным в ней. При возникновении противоречий того или иного правового акта Конституции, данные положения или весь закон будут признаны неконституционными и должны будут подлежать изменениям [59].

Важнейшим показателем законности в государстве является уровень соблюдения законов. Но нельзя забывать о том, что в данном процессе важнейшую роль играет сам закон, то, насколько он совершенен, адекватен современным общественным отношениям, имеются ли в нем пробелы и коллизии. Одной из важнейших проблем современного права является наличие пробелов. Как уже было отмечено в работе, право не всегда успевает

за изменяющимися и появляющимися вновь общественными отношениями. На практике как правило, сначала возникают общественные отношения и только спустя определенное время это отражается в правовой норме. наличие пробелов в различных правовых нормах, что должно своевременно выявляться и устраняться. Особенно, это важно для уголовно-правовых норм, которые не могут применяться по аналогии. Если то или иное деяние не закреплено в качестве преступления в УК РФ, лицо нельзя привлечь к уголовной ответственности.

Законодательная функция – одна из ключевых и наиболее объемных по своему значению и содержанию функций государственного управления. Результатом ее реализации является формирование правовой системы государства, обеспечивающее с помощью законодательства правовое регулирование публичных отношений, возникающих в процессе развития общества и страны и объективно требующих государственного регулирования в форме законодательных постановлений.

Законодательная деятельность существует в синергетическом взаимодействии с государством, являясь формой выполнения его функций, и обществом, в рамках которого реализуется продукт законодательной деятельности – закон. Правительство является автономной социальной системой, направленной на управление обществом.

Спецификой законотворческой деятельности в демократическом правовом государстве является то, что выработка и принятие нормативно правовых решений, их формальное закрепление осуществляется здесь коллегиальными усилиями парламента, что обеспечивает достижение необходимого правового консенсуса.

В отличие от парламента, правительство выступает так называемым институтом оперативного управления, особенно значимым структурно-функциональным элементом в системе государственного управления, обеспечивающим практическое исполнение, реализацию законодательных решений. Следовательно, если институт народных представителей – это

управление посредством закона, то институт оперативного управления – это управление в соответствии с законом, на основании закона, выработанного и принятого представительным органом власти. Иными словами, институт оперативного управления – это институт подзаконного управления, субъекты которого, как правило, не имеют права осуществлять законотворческие функции. Однако в современных условиях эта схема достаточно модифицирована, поэтому исполнительная власть, в частности правительство, оказывают значительное влияние на принятие законов парламентом и даже иногда получают собственные законодательные полномочия под надзором законодательного органа. Поэтому законодательная функция государственного управления реализуется парламентом вместе с правительством (либо другими органами исполнительной власти).

Изменения последних лет привели к появлению такой категории, как система единой публичной власти. Поправки, внесенные в Конституцию РФ в 2020 году, определили место органов местного самоуправления в единой системе публичной власти наряду с органами государственной власти [22].

Публичная власть формируется из представителей народа и наделена полномочиями выражать волю этого народа. Толковый словарь определяет слово «публичный» как «общественный, находящийся в распоряжении общества, устроенный для общества, не частный».

Понятие публичная власть включено в тексты официальных нормативных актов, как на федеральном, так и на региональном уровне. Кроме того, в 2020 году данный термин был официально внесён в Конституцию Российской Федерации, несмотря на отсутствие полноценного, юридически закрепленного термина «публичная власть» [22].

В 2020 году, на основании поправок, которые были одобрены для внесения в Конституцию РФ, в статье 132 появилось понятие «системы единой публичной власти», к которой относятся органы государственной власти и органы местного самоуправления [22].

Единая система публичной власти включает в себя совокупность органов государственной власти, органов государственной власти субъектов РФ, а также других государственных органов, органов местного самоуправления, деятельность которых направлена на соблюдение и защиту прав и свобод граждан, в том числе в сфере информационной безопасности.

В современных условиях серьезной угрозой информационной безопасности являются кибератаки. В 2021–2022 гг. отмечается резкий рост кибератак, совершаемых как на частный сектор, так и на органы публичной власти. По данным «Лаборатории Касперского», число кибер-инцидентов на органы публичной власти в России увеличилось в 10 раз. Практически на 150% возросло число случаев утечки конфиденциальной информации [63, с. 29]. Должностные лица в органах публичной власти отмечают, что за последние годы риски как случайных, так и умышленных утечек информации возросли.

При этом одной из основных форм системного воздействия на кибератаки считается профилактика. Выражается она прежде всего в информационно-аналитической работе и координации усилий субъектов профилактики. Для совершенствования ее мер Указом Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» было предписано создание специализированных штабов по обеспечению кибербезопасности во всех субъектах Российской Федерации, что и было исполнено к 7 сентября 2022 г. [50]. Основной задачей таких штабов является повышение защищенности информационных систем, постоянный мониторинг и взаимодействие с Национальным координационным центром по компьютерным инцидентам. Однако отметим, что проведение заседаний в различных субъектах России разнится и не имеет какой-либо регламентации по срокам: в Омской области - не реже 1 раза в год, в Архангельской области - не реже 1 раза в месяц [63, с. 29].

Таким образом, можно сделать вывод относительно того, что органы государственной власти имеют решающее значение в обеспечении

информационной безопасности. Закон не устанавливает какого-либо отдельного государственного органа, отвечающего за информационную безопасность, эта обязанность возложена всю структуру государственных органов. Находясь во взаимодействии друг с другом, выполняя при этом, каждый свои функции, различные органы государственной власти обеспечивают информационную безопасность в государстве. Важную роль в обеспечении информационной безопасности играют такие государственные органы, как Государственная Дума, Правительство РФ, ФСБ, ФСО, МВД, Минцифры, Роскомнадзор, Прокуратура, суды, органы публичной власти субъектов федерации и другие органы [60].

Особая роль в обеспечении информационной безопасности отведена президенту, который не только утверждает нормативные документы, регулирующие основы информационной безопасности, но и осуществляет контроль за деятельностью органов, исполняющих данные акты, защищает права граждан на обеспечение их безопасности в информационной сфере, определяет направления политики в обозначенной области.

Глава 2 Актуальные вопросы правового регулирования информационной безопасности в Российской Федерации

2.1 Понятие и классификация угроз информационной безопасности

Понятие и основные угрозы информационной безопасности закреплены в Доктрине информационной безопасности. Так, под угрозой информационной безопасности данный правовой акт понимает «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [46].

Основные угрозы информационной безопасности заключаются в следующем. Прежде всего этого, применение информационно-технических средств воздействия иностранными государствами, которые направлены на подрыв безопасности информационной инфраструктуры Российской Федерации в военных целях. Кроме того органы разведывательных служб иностранных государств осуществляют попытки несанкционированного доступа к информации, касающейся деятельности стратегических и научных предприятий Российской Федерации.

Следующей угрозой информационной безопасности Доктрина называет «расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий» [46]. Современные реалии показывают, как в той или иной местности периодически происходят столкновения представителей различных народов на религиозной почве — это

и израиле-палестинский конфликт, который вызывает волнения в других странах. К примеру, недавний протест в Дагестане, когда митингующие напали на аэропорт с целью отыскания там граждан Израиля. Все это результат информационного воздействия на сознание людей.

«Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности» [46]. Результатом данной деятельности является искаженное представление действительности в средствах массовой информации, поскольку российской стороне не дают возможности высказаться. В итоге, многие российские граждане, находясь на территории зарубежных государств, сталкиваются с дискриминацией по национальному признаку.

«Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей» [46]. Воздействие на молодежь в данных целях является очень разрушительным по своему последствию, поскольку молодое поколение находится только на стадии формирования ориентиров и приоритетов и в большей степени подвержено воздействию со стороны. Пропаганда нетрадиционных отношений, неуважения к старшему поколению, негативного отношения к собственному государству губительно воздействует на современную молодежь. В результате, никто не хочет защищать государство, которое ведет неправильную политику.

Зачастую, информационная пропаганда западных государств говорит о том, что Российская Федерация является государством-агрессором, в то время, как остальные страны доброжелательно настроены по отношению к России. Кроме того, внедряется идея о том, что огромные средства, которые тратятся страной на обеспечение армии и безопасности целесообразнее было

бы потратить на повышение уровня благосостояния простого населения. В результате таких воздействий, у молодого поколения формируется отрицательное отношение к своему государству.

Военная операция на Украине повлекла за собой внедрение огромного количества ложной информации о действиях РФ, о событиях проведения военной операции, о характере причинения вреда российской стороной конфликта. Были обнаружены информационные центры, деятельность которых заключалась в осуществлении вбросов ложной информации в социальные сети для искажения реальной картины военной операции, а также для формирования у российского населения протестов против действующей власти в стране, а у зарубежного населения - неприязни к русскому народу и российскому государству.

Особенно неприемлемым является искажение зарубежными государствами роли России в победе во Второй мировой войне. Важнейшим шагом на пути сохранения национальных ценностей Российской Федерации стало введение уголовной ответственности за реабилитацию нацизма. Искажение истории и уничижение памяти ветеранов Великой Отечественной войны не должны быть допустимы в современном мире. Однако, на практике, все чаще встречаются случаи реабилитации нацизма, признания нацистов героями. Интернет в данных преступных действиях выступает вспомогательным элементом и позволяет распространять нацистскую идеологию, сведения, порочащие ВОВ.

Одним из подобных случаях была попытка зарегистрировать лидера нацистов в качестве участника бессмертного полка, который проводился онлайн в 2020 году. В Данном преступном действии «Интернет» был использован в качестве способа совершения преступления. В 2021 году в ст. 354.1 УК РФ была внесена часть 4, закрепляющая ответственность за распространение выражающих явное неуважение к обществу сведений о днях воинской славы и памятных датах России, связанных с защитой Отечества, а равно осквернение символов воинской славы России, оскорбление памяти

защитников Отечества либо унижение чести и достоинства ветерана Великой Отечественной войны, совершенные публично с использованием сети «Интернет» [46].

Следующей угрозой Доктрина называет то, что «различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры» [46].

Важной основой террористической деятельности является ее материально-финансовое обеспечение, которое на современном этапе достигло достаточно высокого уровня. Террористические группировки сегодня имеют серьезное материальное обеспечение, что дает им широкие возможности для осуществления их деятельности. Зачастую такие группировки используют криптовалюту, операции с которой использовать сложнее. Данный вид валюты на сегодняшний день является недостаточно урегулированным в правовом поле. В частности, не урегулирован вопрос налогообложения данной валюты, затруднены каналы отслеживания операций, совершаемых с криптовалютой ввиду возможности совершения анонимных операций, а также отсутствия необходимого центра администрирования совершения подобных операций. Все это создает благоприятные условия для оказания финансовой поддержки террористической деятельности с помощью интернета и использования электронной валюты.

Следующей угрозой информационной безопасности являются возрастающие «масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с

нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее» [46].

Таким образом, основные угрозу информационной безопасности, представленные в Доктрине информационной безопасности, можно кратко сформулировать следующим образом:

- информационно-техническое воздействие иностранных государств на критическую инфраструктуру РФ в военных целях;
- информационное воздействие зарубежных спецслужб в целях дестабилизации внутриполитической обстановки внутри РФ;
- информационное воздействие на сознание российских граждан с целью разложения их культурно-нравственных ценностей и ориентиров;
- информационное воздействие с целью разжигания межнациональной ненависти и вражды;
- интенсивный рост преступности в сфере компьютерной информации.

Состояние информационной безопасности в сфере обороны Доктрина характеризует, как усиление информационного воздействия, направленного на подрыв суверенитета и территориальной целостности страны. Кроме того, отмечается «увеличение масштабов и рост скоординированности компьютерных атак на объекты критической информационной инфраструктуры Российской Федерации» [46].

Относительно информационной безопасности в экономической сфере Доктрина отмечает отставание развития современных российских технологий, зависимость их от иностранных компонентов, программного обеспечения [46].

«Состояние информационной безопасности в области науки, технологий

и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы» [46].

«Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве» [46].

В современной доктрине выделяют иные классификации угроз информационной безопасности. В частности, К.А. Наскидашвили угрозы информационной безопасности подразделяет на следующие элементы:

– «нежелательный контент;
– несанкционированный доступ;
– утечки информации;
– потеря данных;
– мошенничество;
– кибервойны;
– кибертерроризм» [32, с. 187].

При этом под нежелательным контентом автор понимает распространение сведений, запрещенных законом. Несанкционированный доступ представляет собой получение информации, на которую субъект не имеет права. Утечка информации происходит в результате технических неисправностей либо нарушениях правил хранения информации. Потеря

данных выражается в несовершенстве информационных баз, в результате которых происходит утрачивание определенной информации.

Информационное мошенничество стало частью современного мира, оно выражается в краже данных банковских карт, взломах личных кабинетов банков пользователей и др.. Одним из распространенных видов преступлений является так называемое телефонное мошенничество, когда человеку звонят лица, представляющиеся сотрудниками безопасности банка и просят сообщить данные банковской карты, в последствии списывая с нее все денежные средства. Широкая волна списания денежных средств с банковских карт коснулась сайтов продаж - «Авито» и «Юла». Мошенники отправляли продавцам электронную форму для списания средств, под видом формы получения денег продавцом. Заполняя данную форму, у продавца также списывались денежные средств.

Мошенничество с помощью использования сети «Интернет» достигает невероятных масштабов, однако достоверной статистики по количеству данных преступлений на сегодняшний день нет, поскольку отслеживать такие преступления достаточно сложно, в свою очередь, очень малая часть потерпевших обращается в правоохранительные органы [4, с. 104].

Кибервойны заключаются в распространении информации, которая приводит к разжиганию межнациональных конфликтов. Терроризм также перенесся в виртуальную сферу и представляет собой серьезную угрозу безопасности общества и государства.

А.Н. Болдырев выделяет естественные и искусственные угрозы информационной безопасности. Естественные происходят случайным образом, не зависимо от воли человека, а искусственные - создаются самим обществом [5, с. 137].

В.К. Тишин выделяет следующие информационные угрозы:

– «распространение идей и концепций, направленных на разжигание национальной, социально-политической, религиозной вражды;

- призывы к нарушению суверенитета и территориальной целостности государства;
- опасность кибератак на важнейшие информационно-технические системы страны (военные системы управления и связи, ВПК, транспортные системы и другие);
- нарушение прав в информационной сфере (например, авторского);
- террористическая активность в информационном пространстве;
- разведывательно-подрывная деятельность иностранных спецслужб;
- разглашение секретной информации (составляющих государственную тайну сведений и прочей конфиденциальной информации, значимой для обеспечения национальных интересов);
- дискредитация политики России и авторитета отдельных российских государственных деятелей;
- ограничение прав граждан на доступ к информации (если это не предусмотрено законом);
- распространение в СМИ культа жестокости и насилия;
- неразвитость информационной инфраструктуры и рынка высокотехнологической продукции;
- научно-техническая отсталость страны» [43, с. 182].

Как видно, автор в качестве угроз информационной безопасности также называет неразвитость информационной инфраструктуры и научно-техническую отсталость государства. Это представляется вполне обоснованным и хотя, не закреплено в качестве угрозы в Доктрине информационной безопасности, все же является таковой.

Л.С. Резниченко отмечает, что основными источниками угроз в сфере информационной безопасности выступают:

- недружественные государства, спецслужбы которых осуществляют кибератаки на государственные платформы, вмешиваются в деятельность структур, связанных с экономической деятельностью государства и т.д.;
- террористические организации, которые осуществляют кибератаки с целью подорвать национальную систему безопасности;
- организованные преступные группировки, которые осуществляют атаки на банковские системы с целью хищения денежных средств;
- «хактивисты – индивидуальные хакеры, обычно они руководствуются личной выгодой, местью, финансовой выгодой или политической деятельностью» [39, с. 83];
- внутренние злоумышленники - сотрудники, которые имеют доступ к базам данных и используют их в незаконных целях.

Л.С. Резниченко отмечает, что не стоит недооценивать опасность исходящую от внутренних злоумышленников, поскольку «они могут иметь доступ к чувствительной информации и ресурсам, которые находятся за пределами доступа внешних злоумышленников» [39, с. 83]. Это особенно опасно в современной обстановке. Так, одним достаточно частых преступных деяний, является на сегодняшний день продажа данных клиентской базы сотрудниками сотовой связи. В результате подобных действий, гражданам РФ после начала специальной военной операции поступали многочисленные звонки с угрозами либо с целью мошенничества.

А.К. Дубень выделяет еще одну угрозу информационной безопасности РФ - это утечка квалифицированных кадров. Достаточно большое количество молодых специалистов уезжают работать в другие государства в виду того, что там более достойная оплата их труда. Кроме того, государства Европы и США представляют специалистам в сфере информационных технологий более широкие возможности для работы и развития, что нельзя сказать про РФ, поскольку в результате санкций, наше государство столкнулось с

многочисленными трудностями, в том числе, это коснулось программного обеспечения, которое приобреталось за рубежом. Отрасль информационных технологий сегодня вынуждена заниматься разработкой собственных программ и средств защиты информации [11, с. 150].

Таким образом, понятие и основные угрозы информационной безопасности закреплены в Доктрине информационной безопасности. Так, под угрозой информационной безопасности данный правовой акт понимает «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [46].

Основные угрозы информационной безопасности, представленные в Доктрине информационной безопасности, можно кратко сформулировать следующим образом:

- информационно-техническое воздействие иностранных государств на критическую инфраструктуру РФ в военных целях;
- информационное воздействие зарубежных спецслужб в целях дестабилизации внутриполитической обстановки внутри РФ;
- информационное воздействие на сознание российских граждан с целью разложения их культурно-нравственных ценностей и ориентиров;
- информационное воздействие с целью разжигания межнациональной ненависти и вражды;
- интенсивный рост преступности в сфере компьютерной информации.

Современная доктрина выделяет, как правило иную классификацию угроз: ряд авторов в качестве таковых называет неразвитость информационной инфраструктуры и научно-техническую отсталость государства; другие отмечают в качестве угрозы утечку квалифицированных кадров информационной сферы в другие государства.

2.2 Проблемы правового регулирования информационной безопасности

Приступая к исследованию проблем правового регулирования информационной безопасности, необходимо обратить внимание на достаточно большой массив нормативно-правовых актов, регулирующих общественные отношения в обозначенной сфере. В качестве основных можно выделить Конституцию РФ, Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О безопасности критической информационной структуры Российской Федерации», Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации», Указ Президента РФ «О некоторых вопросах информационной безопасности Российской Федерации», Уголовный кодекс РФ, Кодекс об Административных правонарушениях РФ и другие.

Такое значительное количество различных законов и подзаконных актов, регулирующих вопросы, касающиеся тех или иных аспектов информационной безопасности, с одной стороны, оправдано тем, что информация сегодня проникла практически во все сферы нашей жизни, и каждая сфера нуждается в отдельном регулировании. С другой стороны, в современной доктрине отмечается, что ни один из правовых актов не носит комплексного характера и не регулирует напрямую общественные отношения в сфере информационной безопасности [24, с. 145]. Кроме того, такой массив нормативно-правовых актов затрудняет практическое применение правового регулирования информационной безопасности. Для установления одних и тех же вопросов необходимо обращаться к различным правовым актам. Более того, можно говорить об отсутствии системности в правовом регулировании информационной безопасности.

К примеру, Доктрина информационной безопасности содержит определения понятия информационной безопасности, угроз информационной

безопасности, обеспечения информационной безопасности, информационной инфраструктуры. А для уяснения понятия информации необходимо обращаться к ФЗ «Об информации». Для квалификации правонарушений в сфере информационной безопасности также необходимо обращаться к указанным правовым актам. Представляется более правильным сосредоточение понятийного аппарата информационной безопасности в одном правовом акте.

Еще одним проблемным моментом правового регулирования информационной безопасности является специфичность терминологии, используемой в данной сфере. Для того, чтобы правильно применять нормы законов в сфере информационной безопасности, правоприменителю нужно обладать не только юридическими знаниями, но знаниями в сфере информационных технологий. Для уяснения сущности некоторых понятий правоприменителю в ряде случаев необходимо обращаться к другим источникам либо привлекать экспертов в данной области. Более того, законодательного закрепления многих понятий и явлений, используемых на практике, нет (отсутствуют понятия подлинника и копии). Соответственно, следователю либо судье приходится расшифровывать данные понятия с помощью различных источников, которые могут носить субъективный характер.

Такое положение вещей представляется неприемлемым, поскольку право должно отличаться точностью и не допускать субъективизма. Таким образом, необходимым представляется закрепление и определение понятий, используемых в сфере применения информационных технологий в соответствующем законодательстве. Это позволит минимизировать разночтения в применении специализированных понятий.

Е.В. Амосова отмечает непроработанность понятийного аппарата в сфере правового регулирования информационной безопасности, в частности, неоднозначность понятия информации, неопределенность природы ее носителя, сложность стоимостной оценки информации [1, с. 145].

Т.А. Полякова также подчеркивает непроработанность правового регулирования информационной безопасности. Автор подчеркивает необходимость глубокого научного осмысления законодательства в обозначенной сфере; подробного обоснования внедрения зарубежного опыта в современное отечественное право, а также установление ответственность за качество разрабатываемых проектов законодательных актов [36, с. 82].

В.С. Козлов отмечает, что «Федеральный закон «Об информации, информационных технологиях и о защите информации», который, казалось бы, принят специально для регулирования вопросов информационной безопасности в ее различных проявлениях (как на общегосударственном уровне, так и на уровне локальном – относительно граждан, юридических лиц, их объединений), термины «информационная безопасность» и «безопасность информации» вообще не использует, говоря лишь о механизмах защиты информации. Таким образом, названный Федеральный закон требует включения терминов «информационная безопасность Российской Федерации» и «безопасность информации», поскольку они являются основополагающими и понятиеобразующими для самого закона и для системы информационной безопасности и обеспечения такой безопасности на территории России» [20, с. 111].

Ю.А. Трегубова отмечает наличие пробелов в сфере лицензирования внепланового контроля за организациями, которые используют в своей деятельности шифровальные средства для защиты информации. Автор отмечает, что «Таковыми являются кредитно-банковские организации. Например, в ПАО Сбербанк функционирует центр информационной безопасности «SOC - Security Operation Center», который занимается разработкой и контролем всей информационной системы, создавая новые механизмы шифрования данных, тем самым повышая уровень ее защиты. Анализ нормативной базы по данному вопросу выявил наличие пробелов в действующем законодательстве. Так, п. 10 ст. 19 Федерального закона № 99-ФЗ «О лицензировании отдельных видов деятельности» содержит такие

положения, касающиеся внеплановых проверок, как: наличие ходатайства лицензиата о проведении проверки; поступление в лицензирующий орган обращений граждан, СМИ о фактах грубого нарушения закона и т.п. С юридической точки зрения правоохранительные органы не вправе проводить внеплановые проверки с целью выявления нарушения закона, о которых стало известно из различных источников. В связи с этим необходимо дополнить положения рассматриваемого закона положением о дозволении проведения внеплановых проверок сотрудниками ОВД» [44, с. 94].

Немаловажной проблемой является отсутствие должного уровня ответственности за нарушение сохранности персональных данных. Административная ответственность, которая предусмотрена ст. 13.11 КоАП РФ, ничтожно мала. Так, «за невыполнение оператором при обработке персональных данных без использования средств автоматизации обязанности по соблюдению условий, обеспечивающих в соответствии с законодательством Российской Федерации в области персональных данных сохранность персональных данных при хранении материальных носителей персональных данных и исключающих несанкционированный к ним доступ, если это повлекло неправомерный или случайный доступ к персональным данным, их уничтожение, изменение, блокирование, копирование, предоставление, распространение либо иные неправомерные действия в отношении персональных данных, при отсутствии признаков уголовно наказуемого деяния влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до четырех тысяч рублей; на должностных лиц - от восьми тысяч до двадцати тысяч рублей; на индивидуальных предпринимателей - от двадцати тысяч до сорока тысяч рублей; на юридических лиц - от пятидесяти тысяч до ста тысяч рублей» [19]. Такой размер штрафа не заставит оператора относиться серьезно к сохранности персональных данных.

Еще одной проблемой правового регулирования информационной безопасности является его отставание, поскольку информационные

технологии развиваются сегодня очень интенсивно. Т.Н. Михеева отмечает, что на сегодняшний день право находится в серьезно отстающей позиции по отношению к общественным отношениям в сфере информационных технологий [27, с. 115].

А.А. Горелов отмечает, что внедрение цифровых технологий в современные правоотношения серьезным образом изменяет их, и обуславливает необходимость создания специальной правовой базы, регулирующей данные отношения [9, с. 38].

М.Ю. Осипов говорит о необходимости осмысления юристами основ информационных технологий и указывает на необходимость диалога между представителями юридической и ряда технических наук для повышения уровня правового регулирования в сфере информационных технологий [33, с. 184].

Т.Н. Михеева и Н.А. Бессонов в своем исследовании обосновывают, что процесс развития информационных технологий значительно опережает их правовое регулирование. В качестве примера авторы приводят отсутствие надлежащего правового регулирования международной торговли через Интернет, отсутствие правовых норм, закрепляющих ответственность банков за ненадлежащее обеспечение безопасности хранения информации; отсутствие подготовленных технических специалистов в органах внутренних дел, неурегулированность налогообложения криптовалюты и др. Данные авторы также указывают на необходимость создания полноценной правовой базы, регулирующей все информационные сферы [27, с. 81].

А.Ю. Яковлева-Чернышова говорит о необходимости пересмотра всего правового регулирования сферы информационных и цифровых технологий, которые по мнению автора совершенно не адаптированы к изменившемся правоотношениям в данной сфере. Необходим пересмотр уже имеющегося правового регулирования и создание новых правовых актов, отвечающих потребностям и особенностям современных отношений в данной сфере [65, с. 52].

В современной доктрине также отмечается, не совсем корректное употребление тех или иных терминов. К примеру, Т.А. Бражник указывает на некорректность понятия «информационная безопасность», закрепленного в Доктрине информационной безопасности. Автор отмечает, что данное понятие не включает в себя информационную безопасность личности, поскольку «толкование информационной безопасности личности как состояние защищенности от внешних и внутренних угроз в текущих нормативных источниках неоднородно и поэтому используется преимущественно в технической сфере. Очевидно, что информационная безопасность личности предполагает также наличие определенной свободы личности в информационной среде, в том числе свободы на реализацию конституционных и информационных прав, однако обеспечение такой свободы должно гарантироваться правовыми и социальными методами» [6, с. 189].

Вопросы вызывает и определение понятия информационной угрозы, закрепленного в Доктрине информационной безопасности, поскольку данное понятие определяет угрозу, как «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере» [46]. Как видно из данного определения, оно не включает в себя понятия угрозы информационной безопасности личности. Однако в тексте Доктрины, при описании угроз, упоминается о разрушающем воздействии информации на сознание молодого поколения в целях размывания духовно-нравственных ценностей.

Также вызывает вопросы понятие «уничтожение компьютерной информации», содержащиеся в уголовно-правовых нормах. Так, ряд авторов считают спорной такую ситуацию, когда имеет место частичное уничтожение информации, которая в последующем может быть восстановлена. Данные авторы полагают, что целесообразнее было дополнить данную дефиницию и указывать «полное уничтожение», что будет означать невозвратность утраченной информации [41, с. 87]. Думается, что такая точка зрения не

совсем корректна, поскольку более справедливым будет привлечение к ответственности лица за любое уничтожение информации, т.е. если умысел лица был направлен на уничтожение информации, не должно иметь значения, утрачена данная информация полностью или частично.

Сложность в квалификации преступлений в сфере компьютерной информации отмечается при наличии ситуации, когда был похищен носитель информации (флешка, CD-диск). По сути, данный носитель не представляет материальной ценности, однако информация, хранящаяся на нем может иметь существенную ценность для ее законного владельца. Кроме того, дальнейший неправомерный доступ к этой информации очень трудно установим. За хищение в виду малозначительности данное лицо тоже нельзя будет привлечь к уголовной ответственности. В свою очередь, подобное деяние может повлечь серьезные последствия.

Ряд авторов предлагают ввести ст. 272.1, которая бы закрепляла ответственность за незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации [12, с. 25].

Анализ судебной практики показывает, что зачастую преступления, предусмотренные ст. 272 и 273, сопряжены с деяниями, нарушающими авторские и смежные права. Однако при квалификации деяния по таким статьям, как 146, 165 УК РФ, необходимо наличие ущерба в достаточно крупном размере. На практике, такие деяния чаще всего остаются безнаказанными, поскольку установить крупный ущерб данных преступлений очень сложно [17]. Таким образом, необходимым представляется снижение значения вреда, нанесенного преступлениями, закрепленными в вышеуказанных статьях. Это позволит сократить количество данных преступлений ввиду отсутствия у правонарушителей чувства безнаказанности.

Существенной проблемой, трудно поддающейся устранению, является отсутствие механизма защиты интеллектуальной собственности в ходе

электронной торговли, поскольку именно область трансграничной торговли наиболее подвержены высоким рискам в сфере лицензирования товаров [25, с. 68].

Необходимо отметить, что для совершения преступлений в сфере безопасности информации, преступники зачастую используют интернет. Наиболее распространены из них: преступления в сфере компьютерной информации, мошенничество с использованием электронных средств платежа, сбыт наркотических средств с использованием сети «Интернет», доведение до самоубийства, незаконные изготовление и оборот порнографических материалов или предметов и др. Как видно, ряд составов закрепляют использование интернета в качестве квалифицирующего обстоятельства. Однако, несмотря на введение такого способа совершения преступлений, как использование сети «Интернет» в отдельные статьи УК РФ, право в целом находится в отстающем положении в отношении цифровых отношений на сегодняшний день, что обуславливает необходимость постоянного совершенствование уголовного закона, который не может применяться по аналогии и должен соответствовать уровню развития общественных отношений, за нарушение которых предусматривает ответственность.

Таким образом, анализ проблем правового регулирования информационной безопасности позволяет говорить о наличии ряда проблемных моментов. К ним можно отнести:

- большое количество нормативных актов, регулирующих отдельные аспекты информационной безопасности, ни один из которых не носит комплексного характера и не регулирует напрямую общественные отношения в сфере информационной безопасности;
- неопределенность понятия информации, используемое в нормативно-правовых актах;

- дублирование некоторых понятий в различных правовых актах (понятие «информации» - ФЗ «Об информации» и Доктрина информационной безопасности);
- специфичность терминологии, используемой в данной сфере, создает у правоприменителя необходимость обладать не только юридическими знаниями, но знаниями в сфере информационных технологий, для уяснения сущности некоторых понятий необходимо обращаться к другим источникам либо привлекать экспертов в данной области;
- непроработанность нормативно-правовой базы, наличие пробелов, в частности в сфере лицензирования;
- отставание нормативно-правового регулирования в сфере информационной безопасности от интенсивно развивающихся общественных отношений в данной сфере;
- недостаточно серьезные меры административной и уголовной ответственности, предусмотренные за правонарушения в сфере информационной безопасности.

2.3 Основные направления совершенствования правового регулирования информационной безопасности в Российской Федерации

Прежде всего совершенствование правового регулирования информационной безопасности представляется необходимым начать с издания единого федерального закона, который был бы посвящен основным аспектам информационной безопасности в РФ, закреплял весь понятийно-категориальный аппарат в обозначенной сфере.

Кроме того, необходимо конкретизировать понятие информации, поскольку, в современной доктрине отмечается, что понятие, закрепленное в Доктрине, не охватывает всей сущности обозначенного явления. В связи с

этим, современными авторами предлагается определять информацию, как «сведения, знания, сообщения, сигналы и данные об окружающем мире и протекающих в нём процессах, которые воспринимаются и передаются в любой форме (материальной и нематериальной) человеком или специальным устройством» [23, с. 157]. По данному поводу можно отметить, что наиболее целесообразно разделять понятие цифровой информации и информации, которая передается иными способами, к примеру вербальным путем.

ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию», понятие информационной безопасности определяет, как «состояние защищенности детей, при котором отсутствует риск, связанный с причинением информацией вреда их здоровью и (или) физическому, психическому, духовному, нравственному развитию» [57]. В свою очередь, понятие информационной безопасности, закрепленное в Доктрине, не отражает возможность причинения вреда здоровью человека. В связи с этим, представляется необходимым дополнение понятия информационной безопасности либо закрепление понятия информационной безопасности детей в Доктрине.

Как уже было отмечено в работе, понятие угрозы информационной безопасности, закрепленное в Доктрине, не подразумевает возможности существования информационной угрозы для личности, хотя далее по тексту доктрины, при описании угроз отмечается разрушающее воздействие информации на сознание личности. Поэтому, целесообразным представляется дополнить определение угрозы национальной безопасности.

Также необходимо своевременное закрепление в законе появляющихся новых терминов и явлений в сфере информационной безопасности, не получивших адекватное отражение в правовых нормах. Это позволит минимизировать разночтения в применении специализированных понятий.

Е.В. Амосова предлагает совершенствование правового регулирования информационной безопасности с помощью следующих направлений:

- «доработка понятийного аппарата в сфере информационного права;
- правовое закрепление свободы получения и распространения информации субъектами общественных отношений в интересах формирования гражданского общества;
- обеспечение надежной защиты информационного потенциала Российской Федерации от неправомерного его использования;
- доработка системы контроля за экспортом из страны интеллектуальной продукции и информационных банков данных;
- развитие взаимодействия систем информационного обеспечения для эффективного использования информационных ресурсов страны;
- доработка системы нормативно-правовых актов, регулирующих отношения собственности и соблюдения баланса интересов субъектов общественных отношений в области обладания и применения информационных ресурсов;
- формирование общего информационного пространства стран СНГ в интересах эффективности взаимодействия в реализации общих интересов;
- принятие на международном уровне решений о безусловном запрете на использование информационного оружия в мирное время» [1, с. 146].

М.А. Тишин также предлагает «провести оптимизацию правового, научно-технического, методического и организационного сопровождения системы обеспечения информационной безопасности России. Среди правовых мероприятий особенно актуальной для нас остается защита интеллектуальной собственности» [43, с. 187].

Следующим направлением совершенствования правового регулирования в сфере информационной безопасности является

необходимость закрепления ответственности банков за сохранность информации. Одним из распространенных видов преступлений в сфере информации является незаконное списание денежных средств, когда такие действия связаны с несанкционированным доступом к программам. К сожалению, приходится констатировать отсутствие на сегодняшний момент точных статистических данных, позволяющих отразить масштаб данных преступных деяний. Это обусловлено сложностями выявления преступлений, совершаемых данным способом, а также отсутствием ведения отдельного учета денежных списаний через интернет-ресурсы [10, с. 104].

Еще одним обозначенным проблемным моментом является отсутствие законодательного закрепления обязанности провайдеров и владельцев серверов сохранения электронной информации. Сейчас имеет место ситуация, когда удаленный доступ позволяет лицу удалить всю контактную доказательную информацию с любого компьютера, находясь практически в любой точке мира, еще до вынесения судом определенного постановления. Более того, на практике отмечаются случаи, когда провайдеры игнорируют требования правоохранительных органов на предоставление определенной информации о том или ином домене [7, с.24].

Все это обуславливает необходимость законодательного закрепления ответственности провайдеров, обязанности их сохранения электронной информации, которая может являться доказательственной базой по тому или иному преступлению и предоставления по требованию правоохранительных органов.

Таким образом, на сегодняшний день в силу значительной распространенности применения информационных технологий для оказания различных услуг, а также наличия рисков совершения незаконных операций через интернет, важно урегулировать порядок деятельности организаций, в частности банков, по применению электронных ресурсов, порядок использования их клиентами, а также ответственность банков за ненадлежащий уровень сохранности конфиденциальной информации о

клиентах.

На сегодняшний день имеет место значительное количество интернет-магазинов, которые принимают к оплате банковские карты, не проверяя и не подтверждая операции с помощью запросов в адрес банков. В силу этого существует возможность использования такого отсутствия необходимости подтверждения банковских операций с целью совершения незаконных списаний денежных средств со счета, например, посредством выяснения реквизитов карты или иных данных клиента [16, с. 71]. Обязанность дополнительного подтверждения списания денежных средств необходимо закрепить на законодательном уровне.

В работе отмечалось недостаточно суровое наказание, предусмотренное нормами КоАП РФ и УК РФ за совершение правонарушений в сфере информационной безопасности. Если проанализировать наказание, предусмотренное за совершение преступления, где «Интернет» используется в качестве способа совершения, то практически во всех проанализированных статьях предусмотрено наказание в виде лишения свободы. Максимальное наказание за преступления данной группы предусмотрено п. «д» ч.2 ст. 110 УК РФ и ч.2. ст. 110.2 УК РФ - до пятнадцати лет лишения свободы [45]. Объектом преступления в данном случае выступает жизнь человека. Распространение информации с помощью интернета, в случаях доведения до самоубийства, облегчает доступ к потерпевшему. Через интернет могут поступать различного рода угрозы и оказываться воздействие, которое без интернета было бы сложно реализуемым.

Необходимо отметить, что несмотря на то, что в большинстве случаев интернет как способ совершения преступления выступает как квалифицирующий признак, на практике данный способ не всегда означает обязательное повышение степени общественной опасности. Так, распространение сведений, составляющих коммерческую тайну, с использованием электронной почты либо аккаунта в социальной сети не

становится более опасным для общества, чем в случае непосредственного распространения информации самим субъектом преступления.

Ряд ученых обосновывают необходимость внесения в уголовный закон такого дополнительного наказания, которое бы препятствовало преступнику осуществлять свою дальнейшую деятельность с использованием сети «Интернет» [41, с. 90]. Такое наказание предлагается назвать ограничением права на цифровое присутствие. Такое предложение представляется достаточно обоснованным и актуальным на сегодняшний день, однако сложно реализуемым, поскольку на данный момент имеет место огромное количество вакансий удаленной работы через «Интернет», где лицо может трудиться неофициально. Каким образом, будет возможно отслеживание соблюдения данного вида наказания, не совсем понятно.

Встречаются в современной правовой доктрине и такие мнения, согласно которым следует закрепить использование сети «Интернет» как отягчающее обстоятельство. Такое предложение представляется не уместным, поскольку в ряде случаев, как уже было отмечено ранее в работе, использование данной сети не повышает степень общественной опасности деяния, а лишь облегчает совершение преступления.

Обязательными основаниями для закрепления в качестве отягчающего обстоятельства использования сети «Интернет» можно назвать обоснование этого международными нормами, а также тот факт, что ввиду распространенности данного вида преступности создаются серьезные угрозы для безопасности общественных отношений.

В работе отмечалось, что в последнее время актуальной угрозой информационной безопасности стали участившиеся кибератаки. В свою очередь, одним из направлений профилактики кибератак является проведение оценки состояния систем защиты информационных систем, а также проведение специализированных учений. Так, согласно Постановлению Правительства Российской Федерации от 13 мая 2022 г. № 860 «О проведении эксперимента по повышению уровня защищенности государственных

информационных систем федеральных органов исполнительной власти и подведомственных им учреждений» на федеральном уровне запланировано проведение соответствующих мероприятий в период с 16 мая 2022 г. по 30 марта 2023 г. [37]. При этом существенным пробелом является отсутствие подобного на уровне субъектов и на местном уровне.

Одним из немногих примеров, где уже были проведены контрольные мероприятия, может служить Республика Алтай. При этом был выявлен ряд недостатков в принятом оперативным штабом решении [63, с. 30]. Во-первых, отсутствует обоснование более короткого срока проведения оценки состояния защищенности информационных систем и выявления уязвимостей, чем на федеральном уровне (с 16 мая 2022 г. по 16 сентября 2022 г.) [63, с. 30].

Во-вторых, возникают вопросы относительно формы и перечня проведенных работ и корректности отчетов о результатах проверки с учетом того, что техническое задание на выполнение соответствующих работ, разработанное Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации, было опубликовано после их начала (3 июня 2022 г.). При этом на основании результатов подобных отчетов планируется создать единый реестр недопустимых событий в сфере информационной безопасности [63, с. 30] В этой связи возникает вопрос, как наиболее эффективно использовать результаты проверок, проведенных не в соответствии с техническим заданием, и учитывать ли их вообще.

К сожалению, на сегодняшний день не осуществляется анализ состояния кибербезопасности на уровне органов местного самоуправления. Это повышает уязвимость информационных систем. Кроме того, на сегодняшний день нет актуальной правовой базы, которая регулировала бы вопросы взаимодействия между государственными органами на всех уровнях с целью обмена информацией относительно киберугроз и опытом борьбы с ними. Отсутствует и единая платформа для обмена подобной информацией.

В науке отмечается, что на местном уровне публичной власти отсутствует и практика создания систем отчетности, мониторинга и

взаимодействия с другими субъектами профилактики [63, с. 31]. Несмотря на то, что в соответствии с Указом Президента Российской Федерации от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [51]. Федеральная служба безопасности Российской Федерации разработала систему «ГосСОПКА», она не подходит для обмена опытом, по мнению экспертов [63, с. 30]. Данная система в большей степени рассчитана на сбор и хранение информации об обнаруженных угрозах или выявленных инцидентах, о которых субъекты критической информационной инфраструктуры обязаны уведомлять в течение 24 часов [63, с. 31].

Б.О. Баторов отмечает, что, на сегодняшний день является достаточно актуальным вопросом необходимость корректировки нормативно-правового регулирования информационной безопасности, касающегося деятельности МВД. Автор указывает на то, что многие ведомственные акты в сфере информационной безопасности содержат отсылки к утратившим силу законам. В связи с этим автором предлагается закрепить в нормативно-правовых актах необходимость ежегодного проведения проверок «ведомственных нормативных актов в полное соответствие с действующим законодательством, а также его поддержание в актуальном состоянии» [4, с. 126].

С данным предложением следует согласиться, поскольку в нормативно-правовых актах на сегодняшний день не отражена обязанность производить постоянный мониторинг нормативно-правовой базы, посвященной информационной безопасности, в том числе, на соответствие внутренних документов, регламентирующих деятельность органов МВД федеральному законодательству.

Кроме того, представляется необходимым закрепить в современных федеральных программах проведение обязательных мероприятий, направленных на совершенствование нормативно-правовой базы в сфере

информационной безопасности, что является крайне важным в виду интенсивного развития общественных отношений в обозначенной сфере.

Т.А. Полякова для совершенствования правового регулирования в сфере информационной безопасности предлагает «проведение научных исследований в области права, связанных с разработкой понятия и системы информации ограниченного доступа, поскольку родовых критериев такого вида информации сегодня недостаточно они носят только общие черты, включая и требование конфиденциальности» [36, с. 72].

Проведение научных исследований с целью совершенствования нормативно-правового регулирования информационной безопасности представляется крайне важным, поскольку это позволяет не только выявлять проблемы текущей нормативно-правовой базы и устранять пробелы в законодательстве, но и делает возможным разработку рекомендаций, направленных на повышение эффективности правовых норм.

Таким образом, в целях совершенствования правовых норм, регулирующих информационную безопасность можно сформулировать следующие предложения:

- издание единого федерального закона, который был бы посвящен основным аспектам информационной безопасности в РФ, закреплял весь понятийно-категориальный аппарат в обозначенной сфере;
- конкретизация понятия информации, закрепление понятия цифровой информации;
- дополнение определения понятия угрозы информационной безопасности указанием на возможность вредоносного воздействия информации на личность;
- ужесточение ответственности за нарушение сохранности персональных данных;
- закрепление в правовых нормах обязательного проведения оценки состояния систем защиты информационных систем на уровне субъектов и на местном уровне;

– закрепление в нормативно-правовых актах обязанности ежегодного проведения проверок ведомственных нормативных актов в сфере информационной безопасности на предмет их соответствия актуальному законодательству;
– проведение постоянных научных исследований и научного осмысления нормативно-правового регулирования информационной безопасности с целью совершенствования законодательства.

Заключение

Проанализировав понятие информационной безопасности в доктрине и в современном праве, можно отметить, что легальное определение информационной безопасности частично дублирует определение национальной безопасности, что позволяет говорить о том, что информационная безопасность выступает элементом национальной.

Основными объектами защиты информационной безопасности закон называет личность, общество и государство. Целью обеспечения национальной безопасности выступают 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.

Как видно из анализа теоретических определений понятия информационной безопасности, большинство авторов берут за основу законодательное определение информационной безопасности как состояния защищенности от информационных угроз. Однако ряд авторов предлагают определять исследуемую категорию как систему мер защиты, как процесс управления информационными угрозами. Ряд авторов, в своих определениях не уделяет достаточного внимания безопасности личности и общества, останавливаясь только на безопасности государства, рассматривая информационную безопасность, как часть национальной безопасности, однако без безопасности личности и общества невозможно существование безопасности государства.

Нельзя оставить без внимания тот факт, что проанализированные определения понятия информационной безопасности не раскрывали сам термин «информационная». Также, как и легальное определение, исследуемого понятия, они ограничивались указанием на защиту от информационных угроз. В свою очередь, при определении понятия

информационных угроз, законодатель также не раскрывает термин «информационные». Для определения данного понятия необходимо обратиться к Федеральному закону «Об информации, информационных технологиях и о защите информации», который под информацией понимает «сведения (сообщения, данные) независимо от формы их представления».

На основании вышеизложенного представляется целесообразным дополнить легальное определение информационной безопасности, чтобы оно выглядело следующим образом: «информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних угроз в сфере распространения сведений, сообщений и данных, 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».

Необходимо отметить, что нормативно-правовое регулирование информационной безопасности на сегодняшний день представляено могочисленных количеством законодательных актов, таких как Доктрина информационной безопасности, Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию и закреплением в КоАП РФ и УК РФ основных общественно-опасных деяний в сфере информации.

Можно сделать вывод относительно того, что органы государственной власти имеют решающее значение в обеспечении информационной безопасности. Закон не устанавливает какого-либо отдельного государственного органа, отвечающего за информационную безопасность, эта обязанность возложена всю структуру государственных органов. Находясь во взаимодействии друг с другом, выполняя при этом, каждый свои функции,

различные органы государственной власти обеспечивают информационную безопасность в государстве. Важную роль в обеспечении информационной безопасности играют такие государственные органы, как Государственная Дума, Правительство РФ, ФСБ, ФСО, МВД, Минцифры, Роскомнадзор, Прокуратура, суды, органы публичной власти субъектов федерации и др.

Особая роль в обеспечении информационной безопасности отведена президенту, который не только утверждает нормативные документы, регулирующие основы информационной безопасности, но и осуществляет контроль за деятельностью органов, исполняющих данные акты, защищает права граждан на обеспечение их безопасности в информационной сфере, определяет направления политики в обозначенной области.

Понятие и основные угрозы информационной безопасности закреплены в Доктрине информационной безопасности. Основные угрозы информационной безопасности, представленные в Доктрине информационной безопасности, можно кратко сформулировать следующим образом:

- информационно-техническое воздействие иностранных государств на критическую инфраструктуру РФ в военных целях;
- информационное воздействие зарубежных спецслужб в целях дестабилизации внутриполитической обстановки внутри РФ;
- информационное воздействие на сознание российских граждан с целью разложения их культурно-нравственных ценностей и ориентиров;
- информационное воздействие с целью разжигания межнациональной ненависти и вражды;
- интенсивный рост преступности в сфере компьютерной информации.

Современная доктрина выделяет, как правило иную классификацию угроз: ряд авторов в качестве таковых называет неразвитость информационной инфраструктуры и научно-техническую отсталость

государства; другие отмечают в качестве угрозы утечку квалифицированных кадров информационной сферы в другие государства.

Анализ проблем правового регулирования информационной безопасности позволяет говорить о наличии ряда проблемных моментов. К ним можно отнести:

- большое количество нормативных актов, регулирующих отдельные аспекты информационной безопасности, ни один из которых не носит комплексного характера и не регулирует напрямую общественные отношения в сфере информационной безопасности;
- дублирование некоторых понятий в различных правовых актах (понятие «информации» - ФЗ «Об информации» и Доктрина информационной безопасности);
- специфичность терминологии, используемой в данной сфере, создает у правоприменителя необходимость обладать не только юридическими знаниями, но знаниями в сфере информационных технологий, для уяснения сущности некоторых понятий необходимо обращаться к другим источникам либо привлекать экспертов в данной области;
- отсутствие законодательного закрепления многих понятий и явлений, используемых на практике (отсутствуют понятия подлинника и копии);
- непроработанность нормативно-правовой базы, наличие пробелов, в частности в сфере лицензирования;
- отставание нормативно-правового регулирования в сфере информационной безопасности от интенсивно развивающихся общественных отношений в данной сфере;

– недостаточно серьезные меры административной и уголовной ответственности, предусмотренные за правонарушения в сфере информационной безопасности.

В целях совершенствования правовых норм, регулирующих информационную безопасность можно сформулировать следующие предложения:

– издание единого федерального закона, который был бы посвящен основным аспектам информационной безопасности в РФ, закреплял весь понятийно-категориальный аппарат в обозначенной сфере;
– конкретизация понятия информации, закрепление понятия цифровой информации;
– дополнение определения понятия угрозы информационной безопасности указанием на возможность вредоносного воздействия информации на личность;
– ужесточение ответственности за нарушение сохранности персональных данных;
– закрепление в правовых нормах обязательного проведения оценки состояния систем защиты информационных систем на уровне субъектов и на местном уровне;
– закрепление в нормативно-правовых актах обязанности ежегодного проведения проверок ведомственных нормативных актов в сфере информационной безопасности на предмет их соответствия актуальному законодательству;
– проведение постоянных научных исследований и научного осмысления нормативно-правового регулирования информационной безопасности с целью совершенствования законодательства.

Список используемой литературы и используемых источников

1. Амосова Е.В. Актуальные проблемы правового регулирования информационной безопасности в Российской Федерации // Наука и Просвещение. 2022. С. 144-147.
2. Бабаш А.В., Баранова Е.К. Актуальные вопросы защиты информации: монография. М.: Риор: Инфра-М. 2017. 111 с.
3. Баринов С.В. О правовом определении понятия «информационная безопасность личности» // Актуальные проблемы российского права. 2016. № 4. С. 97 - 105.
4. Баторов Б.О. Некоторые проблемы нормативно-правового регулирования защиты информации в органах внутренних дел Российской Федерации и пути их разрешения // Труды Академии управления МВД России. 2022. №2 (62). С. 121-127.
5. Болдырев А.Н. Информационная безопасность. Виды угроз информационной безопасности // Сборник материалов III Республиканской студенческой научно-практической конференции. Элиста. Московский государственный гуманитарно-экономический университет. 2021. С. 137-140.
6. Бражник Т.А. Отдельные аспекты правового регулирования информационной безопасности личности // Вестник ВГУ. Серия: Право. 2019. №3 (38). С. 182-189.
7. Володина С.И. Электронное досье по уголовному делу в эпоху цифровизации // Адвокатская практика. 2021. № 2. С. 23 - 27.
8. Гостева, С.Р. Достойные качество и уровень жизни граждан - важное условие обеспечения национальной безопасности России // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2011. № 1(7). С. 69-78.
9. Горелов А.А. Цифровизация в юридической практике // Трудовое право. 2021. № 9. С. 37 - 40.

10. Долгиева М.М. Квалификация преступлений, совершаемых в сфере компьютерной информации в отношении криптовалюты // Современное право. 2018. № 11. С. 103 - 108.

11. Дубень А.К. Отдельные аспекты правового регулирования информационной безопасности // Национальная безопасность / nota bene. 2022. №6. С. 145-151.

12. Евдокимов К.Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации // Российский следователь. 2015. № 10. С. 24 - 29.

13. Жарова А.К. Обеспечение информационного суверенитета Российской Федерации // Юрист. 2021. № 11. С. 28 - 33.

14. Иванов С.В. Правовое регулирование информационной безопасности личности в Российской Федерации // Вестник Екатерининского института. 2014. № 1 (25). С. 49- 50.

15. Исаева М.Ф. О внутренних угрозах информационной безопасности // Международный научно-исследовательский журнал. 2019. № 5-1(83). С. 26-28.

16. Каверин В. Повышение эффективности через цифровизацию // Банковское обозрение. 2021. № 6. С. 70 - 72.

17. Кенжетаев Б.Е. Информационная безопасность: понятие, сущность, содержание // Вестник Торайгыров университета. Гуманитарная серия. 2020. № 4. С. 36-45.

18. Кассационное определение Судебной коллегии по уголовным делам Верховного Суда Российской Федерации от 23.07.2020 № 83-УД20-4 [Электронный ресурс]. - URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1062723477004936629502444415. (дата обращения: 15.10.2023).

19. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 04.08.2023) // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 1.

20. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) // официальный интернет-портал правовой информации http://www.pravo.gov.ru.

21. Козлов В.С. Информационная безопасность и безопасность информации в Российской Федерации: проблемы правового регулирования // Сборник научных трудов. Хакасский государственный университет им. Н.Ф. Катанова. 2023. С. 111-112.

22. Колосова Н.М., Колосов К.М. Президент Российской Федерации как гарант информационной безопасности личности // Журнал российского права. 2020. №4. С. 17-27.

23. Кулжабаева Ж.О., Костяная Ю.С. К вопросу о понятии информации // Вестник Института законодательства и правовой информации Республики Казахстан. 2020. №3 (61). С.150-158.

24. Лебедев, В. Н. Проблемы нормативного правового регулирования информационной безопасности в Российской Федерации и федеральных органах исполнительной власти // Сборник статей Международной научно-практической конференции. 2019. С. 144-148.

25. Лебедев А.С. Проблемы правового регулирования трансграничной электронной торговли в Евразийском экономическом союзе // Евразийская интеграция: экономика, право, политика. 2020. № 2(32). С. 65-71.

26. Михеева Т.Н. К вопросу о правовых основах цифровизации в Российской Федерации // Вестник Университета имени О.Е. Кутафина. 2019. №9 (61). с.114-122.

27. Михеева Т.Н, Бессонов Н.К. Конституционно-правовое регулирование информатизации и цифровизации в России // Образование и право. 2021. №5. С.80-83.

28. Михнев И.П., Михнева С.В. Полномочия федеральных органов государственной власти Российской Федерации в области обеспечения

безопасности критической информационной инфраструктуры // Вестник Алтайской академии экономики и права. 2019. № 1-2. С. 202-208.

29. Мухачев С.В., Костюченко К.Л., Харламова А.А. Государственные органы обеспечения информационной безопасности в период становления современной российской государственности // Вестник Уральского юридического института МВД России. 2022. №4 (36). С. 129-135.

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

31. Назарова Д.Д. Доктринальные подходы к определению понятия «информационная безопасность»: проблемы интерпретации // Актуальные вопросы развития современной цифровой среды: сборник статей по материалам научно-технической конференции молодых ученых, Москва, 14–16 апреля 2021 года. – Волгоград: Издательский дом «Сириус»). 2021. – С. 343-351.

32. Наскидашвили, К.А. Информационная безопасность. Виды угроз информационной безопасности // Вестник студенческого научного общества ГОУ ВПО «Донецкий национальный университет». 2020. Т. 1, № 12. С. 187-189.

33. Осипов М.Ю. К вопросу о методологическом потенциале современных концепций права в контексте повышения эффективности правового регулирования цифровых технологий // VI Московский юридический форум «Российская правовая система в условиях четвертой промышленной революции» Конференция «Эффективность правового регулирования цифровых технологий» . М. 2019 г. С. 184-184.

34. Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. №1. С. 52-62.

35. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для бакалавриата и магистратуры. Москва: Издательство Юрайт, 2018. 325 с.

36. Полякова, Т. А. Новые векторы развития информационного права в условиях цивилизационного кризиса и цифровой трансформации / Т.А. Полякова, А. В. Минбалеев, Н. В. Кроткова // Государство и право. 2020. № 5. С. 75-87.

37. Постановление Правительства РФ от 13.05.2022 № 860 (ред. от 24.03.2023) «О проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений» (вместе с «Положением о проведении эксперимента по повышению уровня защищенности государственных информационных систем федеральных органов исполнительной власти и подведомственных им учреждений»)// «Собрание законодательства РФ», 23.05.2022, № 21, ст. 3439.

38. Рафиков И.Н., Алышев Ю.В. Преступления в сфере компьютерной информации // E-Scio. 2020. №2 (41). С. 1-6.

39. Резниченко Л.С. Современные и перспективные угрозы информационной безопасности // Электронный сетевой политематический журнал «Научные труды КубГТУ». 2023. № 3. С. 80-92.

40. Решение арбитражного суда Брянской области по делу №А09-2030/2019 от 16.12.2019 // https://rospravosudie.com/act-opredelenie-a09-2030-2019-zenin-f-e-as-bryanskoj-oblasti-16-12-2009-5645324/.

41. Решетников А.Ю., Русскевич Е.А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации // Уголовное право. 2018. № 2. С. 86 - 95.

42. Романовский Г.Б., Романовская О.В. О цифровом суверенитете // Конституционное и муниципальное право. 2022. № 9. С. 25 - 31.

43. Тишин М.А. Угрозы информационной безопасности российской федерации // Filo Ariadne. 2018. № 4(12). С. 180-189.

44. Трегубова Ю.А. Некоторые проблемы правового обеспечения информационной безопасности в России / Ю. А. Трегубова, Т. В. Ерохина // Право и общество в условиях глобализации: перспективы развития: сборник научных трудов международной научно-практической конференции. № 5. 2017. С. 93-95.

45. Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 04.08.2023) // «Собрание законодательства РФ», 17.06.1996, № 25, ст. 2954.

46. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» //»Собрание законодательства РФ», 12.12.2016, № 50, ст. 7074.

47. Указ Президента РФ от 3 апреля 1995 г. № 334 «О мерах по соблюдению законности в области разработки производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации» // Собрание законодательства РФ. - 1995. - № 15. - Ст. 1285.

48. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»//»Собрание законодательства РФ», 02.05.2022, № 18, ст. 3058.

49. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» // «Собрание законодательства РФ», 25.05.2015, № 21, ст. 3092.

50. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»// «Собрание законодательства РФ», 02.05.2022, № 18, ст. 3058.

51. Указ Президента РФ от 15.01.2013 № 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»// «Собрание законодательства РФ», 21.01.2013, № 3, ст. 178.

52. Утарбеков Ш.Г. Понятие и место информационной безопасности в национальной безопасности России // Вестник Челябинского государственного университета. Серия: Право. 2021. Т. 6, № 3. С. 34-35.

53. Фадеева К.Н. Информационная безопасность: учебное пособие. – Чебоксары: Чувашский государственный педагогический университет им. И.Я. Яковлева, 2019. 164 с.

54. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 31.07.2023) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.10.2023) // «Собрание законодательства РФ», 31.07.2006, № 31 (1 ч.), ст. 3448.

55. Федеральный закон от 06.04.2011 № 63-ФЗ (ред. от 04.08.2023) «Об электронной подписи» (с изм. и доп., вступ. в силу с 01.09.2023) // «Собрание законодательства РФ», 11.04.2011, № 15, ст. 2036.

56. Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 28.12.2022) «О противодействии экстремистской деятельности» (с изм. и доп., вступ. в силу с 15.07.2023) // «Собрание законодательства РФ», 29.07.2002, № 30, ст. 3031.

57. Федеральный закон от 29.12.2010 № 436-ФЗ (ред. от 28.04.2023) «О защите детей от информации, причиняющей вред их здоровью и развитию»// «Собрание законодательства РФ», 03.01.2011 № 1, ст. 48.

58. Федеральный закон от 26.07.2017 № 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации» // «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4736.

59. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 06.02.2023) «О персональных данных»// «Собрание законодательства РФ», 31.07.2006. № 31 (1 ч.). ст. 3451.

60. Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 04.08.2023) «О связи»// «Собрание законодательства РФ», 14.07.2003, № 28, ст. 2895.

61. Федеральный закон от 16.02.1995 № 15-ФЗ (ред. от 17.07.1999) «О связи» [Электронный ресурс] // СПС КонсультантПлюс (утратил силу).

62. Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации» [Электронный ресурс] //СПС КонсультантПлюс (утратил силу).

63. Цыплакова А.Д., Шестак В.А. Участие местных органов публичной власти в совершенствовании мер профилактики кибератак в России // Государственная власть и местное самоуправление. 2023. № 2. С. 28 - 31.

64. Шахсуварова, И.З. Информационная безопасность: теоретические основы понятия // Аллея науки. 2022. Т. 1, № 7(70). С. 209-214.

65. Яковлева-Чернышева А.Ю., Дружинина А.В. правовое регулирование процессов цифровизации в России: гражданско-правовой аспект // Юридические исследования. 2021. №8. С. 51-62.