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

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

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

Государственно-правовая
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Информационные правонарушения как угроза национальной безопасности»

Обучающийся Е.В. Артамонова
(Инициалы Фамилия) (личная подпись)

Руководитель доцент, к.ю.н. К.П. Федякин
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Актуальность темы исследования обусловлена тем, что на сегодняшний день в силу влияния недружественных стран число угроз информационной безопасности резко возросло, поэтому данная сфера требует особого внимания и разработки защитных мер, отвечающих актуальным реалиям. Отдельного внимания заслуживают вопросы обеспечения информационной безопасности несовершеннолетних в сети «Интернет». Поскольку использование несовершеннолетним интернет-ресурсов сопряжено с риском взаимодействия с опасным контентом (синий кит, продажи наркотиков, движение колумбайн и так далее).

Объект исследования – общественные отношения, складывающиеся по поводу правового регулирования информационной безопасности в Российской Федерации.

Предмет исследования – нормы российского законодательства, материалы периодической печати и судебной практики, благодаря которым можно целостно и всесторонне рассмотреть вопросы правового регулирования информационной безопасности в Российской Федерации, а также выявить характерные для него проблемные аспекты.

Цель исследования заключается в выявлении актуальных проблем, возникающих в процессе обеспечения информационной безопасности Российской Федерации.

Методологическую основу выпускного исследования составляют общенаучные и частнонаучные методы. В число общенаучных методов познания входят: синтез, анализ, сравнение, дедукция, индукция, диалектический метод. К числу используемых в настоящей работе частнонаучных методов относятся: формально-юридический метод, сравнительно-правовой метод.

Структурно работа состоит из введения, трех глав, заключения, а также списка используемой литературы и используемых источников.

Оглавление

Введение 4
Глава 1 Информационная безопасность как элемент системы национальной безопасности Российской Федерации 7
1.1 Понятие информационной безопасности 7
1.2 Значение информационной безопасности для современной Российской Федерации 17
Глава 2 Элементы правового регулирования информационной безопасности 23
2.1 Конституционно-правовые основы регулирования информационной безопасности 23
2.2 Организационные основы регулирования информационной безопасности 33
2.3 Особенности правового регулирования информационной безопасности в сети «Интернет» 40
Глава 3 Проблемы правового регулирования противодействия информационным правонарушениям в Российской Федерации 52
Заключение 61
Список используемой литературы и используемых источников 65

Введение

Одной из причин возникновения государства, которая впоследствии вошла в число его приоритетных задач, является защита от внутренних и внешних угроз. Со временем, в процессе развития общественных отношений и их усложнения различными элементами, число угроз, которые требовали внимания, также возросло. Это обстоятельство послужило причиной разработки специального комплекса, который включает в себя различные методы и средства противодействия внутренним и внешним угрозам государства. Разрабатываемый государством комплекс мер должен быть «гибким» и соответствовать актуальным реалиям современного мира. Так, исходя из нынешних условий, Российская Федерация должна отдавать приоритет не только военной безопасности, но и уделять должное внимание вопросам обеспечения информационной безопасности. Информация является важным инструментом воздействия на общество. Те или иные сведения при распространении могут дестабилизировать обстановку внутри государства, а также привести к другим неблагоприятным последствиям.

Актуальность темы исследования обусловлена тем, что на сегодняшний день в силу влияния недружественных стран число угроз информационной безопасности резко возросло, поэтому данная сфера требует особого внимания и разработки защитных мер, отвечающих актуальным реалиям. Отдельного внимания заслуживают вопросы обеспечения информационной безопасности несовершеннолетних в сети «Интернет». Поскольку использование несовершеннолетним интернет-ресурсов сопряжено с риском взаимодействия с опасным контентом (синий кит, продажи наркотиков, движение колумбайн и так далее).

Объект исследования – общественные отношения, складывающиеся по поводу правового регулирования информационной безопасности в Российской Федерации.

Предмет исследования – нормы российского законодательства, материалы периодической печати и судебной практики, благодаря которым можно целостно и всесторонне рассмотреть вопросы правового регулирования информационной безопасности в Российской Федерации, а также выявить характерные для него проблемные аспекты.

Цель исследования заключается в выявлении актуальных проблем, возникающих в процессе обеспечения информационной безопасности Российской Федерации.

Для достижения заявленной цели, нами были определены следующие задачи:

– рассмотреть понятие и признаки информационной безопасности;

– проанализировать значение информационной безопасности для современной Российской Федерации;

– изучить конституционно-правовые основы регулирования информационной безопасности;

– рассмотреть организационные основы регулирования информационной безопасности;

– раскрыть Особенности правового регулирования информационной безопасности в сети «Интернет»;

– выявить проблемы правового регулирования противодействия информационным правонарушениям в Российской Федерации.

Теоретическую основу исследования составляют работы следующих ученых юристов: М.Г. Адылханов, И.Р. С.В. Баринов, Е.В. Безручко, М.С. Власенко, М.К. Дзанагова, А.Н. Ибрагимова, Н.Е. Колобаева, С.В. Корнакова, В.А. Мазуров, К.А. Мамедова, О.М. Манжуева, Л.С. Михайлова, К.Д. Озимко, П.А. Олейникова, Л.Г. Павкина, С.А. Привалов, Т.Б. Савкина, М.С. Саликов, Ю.В. Слесарев, Л.К. Терещенко, Д.А. Тершуков, Ш.Г. Утарбеков, Г.И. Шахворостов, П.С. Швыряев, Т.М. Шогенов, О.А. Шубина.

Нормативную базу выпускного исследования составляют следующие акты: Конституция Российской Федерации, Гражданский кодекс Российской

Федерации (часть третья), Закон РФ «О государственной тайне», Закон РФ «О средствах массовой информации», Семейный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Федеральный закон «Об архивном деле в Российской Федерации», Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации», Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации», Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», Указ Президента РФ «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационнотелекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационнотелекоммуникационной сети «Интернет»).

Методологическую основу выпускного исследования составляют общенаучные и частнонаучные методы. В число общенаучных методов познания входят: синтез, анализ, сравнение, дедукция, индукция, диалектический метод. К числу используемых в настоящей работе частнонаучных методов относятся: формально-юридический метод, сравнительно-правовой метод.

Структурно работа состоит из введения, трех глав, заключения, а также списка используемой литературы и используемых источников.

Глава 1 Информационная безопасность как элемент системы национальной безопасности Российской Федерации

1.1 Понятие информационной безопасности

Одной из причин возникновения государства, которая впоследствии вошла в число его приоритетных задач, является защита от внутренних и внешних угроз. Со временем, в процессе развития общественных отношений и их усложнения различными элементами, число угроз, которые требовали внимания, также возросло. Это обстоятельство послужило причиной разработки специального комплекса, который включает в себя различные методы и средства противодействия внутренним и внешним угрозам государства. Разрабатываемый государством комплекс мер должен быть «гибким» и соответствовать актуальным реалиям современного мира. Так, исходя из нынешних условий, Российская Федерация должна отдавать приоритет не только военной безопасности, но и уделять должное внимание вопросам обеспечения информационной безопасности. Информация является важным инструментом воздействия на общество. Те или иные сведения при распространении могут дестабилизировать обстановку внутри государства, а также привести к другим неблагоприятным последствиям.

В современном мире информация является, своего рода, ценным ресурсом, который может использоваться в различных целях, в том числе и для регулирования поведения людей. Отдельная информация требует особой охраны, поскольку содержит в себе исключительно личные данные о конкретном человеке или значимые для государственной обороны сведения. В свою очередь, другая информация должна быть ограничена в распространении, ввиду своего негативного влияния и потенциальной угрозы тому или иному общественному институту. Именно этим продиктована необходимость государства принимать активное участие в процессах размещения, распространения, получения и защиты информации. В связи с

этим в российской нормативно-правовой базе нашло свое отражение понятие «информационная безопасность». Указанное определение имеет основополагающее значение в Доктрине информационной безопасности Российской Федерации. Указанный документ рассматривает понятие информационной безопасности следующим образом «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» [37].

Анализируя представленное определение можно в первую очередь отметить, что понятие «информационная безопасность» по своей структуре и содержанию весьма схоже с понятием «национальная безопасность». Стратегии национальной безопасности раскрывает второе понятие следующим образом: «состояние защищенности от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны» [40]. Объяснить такое положение вещей можно тем, что понятие «национальная безопасность» является родовым по отношению к понятию «информационная безопасность». Национальная безопасность включает в себя широкий перечень охраняемых законом общественных отношений, к числу которых можно отнести и охрану отдельных видов информации, а также защиту общества от вредоносной информации. В силу того, что информационная безопасность является структурным элементом национальной безопасности, легальные дефиниции указанных категорий имеют множество сходств. При этом необходимо отметить, что при определении информационной безопасности нормотворец отразил лишь

некоторые аспекты ее специфики, оставив без внимания отдельные сущностные признаки. В связи с этим мы считаем необходимым, для формирования целостного представления о категории информационная безопасность, обратиться к научным работам ученых-юристов, которые исследовали данный вопрос.

Л.Г. Павкина рассматривает информационную безопасность следующим образом: «как состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям» [27, с. 263]. Анализируя представленное определение, можно сделать вывод, что основное внимание в нем уделяется именно охране общественных отношений. При этом в легальной дефиниции акцент смещен на защиту личности, общества и государства. Причем именно в такой последовательности, поскольку она отражает социальный и гуманистический характер нашего государства. Информационная безопасность преследует своей целью обеспечить защищенность интересов конкретных субъектов, а не обезличенных общественных отношений. В связи с этим, данное определение не отражает основополагающих признаков категории «информационная безопасность» и не позволяет нам более детально рассмотреть ее сущность.

О.А. Шубина рассматривает информационную безопасность как «получение максимальной информации о намерениях и потенциальных действиях своих оппонентов и минимальная утечка информации о своих планах» [49, с. 114]. Данное определение, на наш взгляд, носит скорее частный характер, поскольку не затрагивает вопросы информационной безопасности в интересующем нас контексте. Учитывая его специфику, оно скорее применимо больше для «информационной борьбы» между субъектами, которые осуществляют свою деятельность в одной сфере. Например, компании Apple и Samsung являются конкурентами на рынке техники (телефоны, планшеты и так далее), для них важно сохранить инкогнито информацию о делах внутри компании, но при этом также важно получить сведения о том, что происходит у их оппонента.

А.Н. Ибрагимова предлагает более широкое определение, которое рассматривает информационную безопасность в качестве «защищенности потребностей граждан, отдельных групп и социальных слоев, массовых объединений людей и населения в целом в качественной информации, которая необходима для функционирования их жизнедеятельности, образования и развития» [12, с. 95]. В первую очередь следует отметить, что автор данного определения весьма подробно рассматривает субъекты, в чьих интересах обеспечивается информационная безопасность. При этом без внимания остается государство, как один из основных субъектов защиты информации. На наш взгляд, уделяя особое внимание субъектам, автору стоило бы также подробно раскрыть, что информационная безопасность обеспечивается в интересах государственных органов и должностных лиц. Это позволило бы наиболее полно отразить весь субъективный состав, в контексте обеспечения информационной безопасности. Отдельно стоит обратить внимание, что автором используется категория «потребность», то есть, необходимость в обеспечении информационной безопасности. Что, на наш взгляд, является допустимым и оправданным в условиях цифровизации и роста числа источников информации.

Дополняя наше предыдущее замечание относительно субъектов, обладающих потребностью в информационной защищенности, стоит отметить, что, раскрывая такой субъект как «государство», нельзя ограничиваться только органами государственной власти и их должностными лицами. Мы должны принимать во внимание, что власть осуществляется не только на федеральном уровне и уровне субъектов Российской Федерации, но и на муниципальном уровне. Органы местного самоуправления и их должностные лица аналогично испытывают потребность в информационной защите, которую мы не при каких обстоятельствах не можем нивелировать.

В.А. Мазуров предлагает следующее определение информационной безопасности. «Информационная безопасность – защита информации и поддерживающей ее инфраструктуры с помощью совокупности программных,

аппаратно-программных средств и методов с целью недопущения причинения вреда владельцам этой информации или поддерживающей его инфраструктуре» [19, с. 59]. Автор уделяет внимание именно способам обеспечения информационной безопасности. Причем акцент делается именно на техническом аспекте данного вопроса. Это вполне уместно, так как в условиях развития технологий именно подобного рода способы и средства выходят на первый план, если рассматривать практическую сторону обеспечения информационной безопасности. Однако, данная работа имеет приоритетной целью рассмотрение информационной безопасности с точки зрения юриспруденции, поэтому мы не будем заострять внимание на технологическом аспекте данного вопроса.

Опираясь на рассмотренные нами определения, предложенные различными исследователями, можно отметить, что информационная безопасность может рассматриваться в двух ипостасях. Во-первых, информационная безопасность направлена на обеспечение сохранности информации от противоправного завладения, использования, распространения, если законом предусмотрена ее охрана. Примером таких сведений является государственная тайна, тайна усыновления, тайна частной жизни и так далее. Во-вторых, информационная безопасность подразумевает защиту населения от информации, которая может причинить вред человеку, обществу и государству. Говоря о вредоносной информации, имеются в виду сведения, которые потенциально могут нести опасность субъектам защиты информационной безопасности. В качестве примера можно указать на сведения, которые вводят в заблуждение граждан относительно специальной военной операции.

Анализ легальной дефиниции и ее доктринальных вариантов позволяет нам сделать вывод, что для категории «информационная безопасность» характерны следующие признаки:

– определяется состоянием защищенности;

– имеет своей целью защиту интересов личности, общества и государства;

– обеспечивает защиту от незаконного получения, распространения и передачи информации, которая охраняется законом;

– обеспечивает реализацию мероприятий, направленных на защиту охраняемых субъектов от вредоносной информации;

– обеспечивает охрану прав и свобод человека и гражданина;

– обеспечивает государственную защиту и охрану государственного суверенитета;

– имеет своей целью защиту и сохранение территориальной целостности;

– направлена на обеспечение устойчивого социально-экономического развития Российской Федерации.

По большей части указанные признаки находят свое отражение в легальном определении понятия «информационной безопасности». Поэтому мы делаем вывод, что на сегодняшний день отсутствует необходимость вносить в него какие-либо существенные коррективы.

Наряду с признаками информационной безопасности для уяснения сущности категории «информационная безопасность» следует рассмотреть принципы ее обеспечения, поскольку они также отражают ее сущность и особенности формирования. В указанной ранее Доктрине можно найти только упоминание принципов деятельности госорганов, направленной на обеспечение информационной безопасности. При этом информационная безопасность обеспечивается не только государственными органами, но и иными субъектами.

Большинство основополагающих начал, положений и идей, которые лежат в основе обеспечения информационной безопасности, мы можем найти в статье третьей Федерального закона «Об информации, информационных технологиях и о защите информации». В законе перечислены следующие принципы:

– «свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

– установление ограничений доступа к информации только федеральными законами;

– открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

– равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

– обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

– достоверность информации и своевременность ее предоставления;

– неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

– недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами» [44].

Анализируя перечисленные выше перечисленные принципы, можно обратить внимание, что практически каждый из них повторяет или более подробно раскрывает положения Конституции Российской Федерации в сфере информационной безопасности. Так, принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом был взят непосредственно из части четвертой статьи 29 Конституции Российской Федерации. В свою очередь принцип равноправия языков при создании информационных систем и их эксплуатации основан на том, что Российская Федерация является многонациональным государством.

Хотя государственным языком является русский язык, в отдельных субъектах наряду с ним используется свой национальный язык. Поэтому при создании информационных систем общего пользования, должны учитываться такие особенности и находить свое отражение при их создании.

В научной литературе можно встретить исследования, в которых авторы выделяют и другие принципы обеспечения информационной безопасности. В работе С.В. Баринова можно встретить упоминание принципа своевременности в вопросах обеспечения информационной безопасности. «На практике своевременность достигается путем разработки и четкого исполнения положений концепции и системы защиты объекта, на котором сконцентрированы технические средства, средства связи, информация, подлежащая защите. Система защиты включает в себя совокупность правовых, научно-технических, специальных и организационных мер» [2, с. 97]. Своевременность в контексте данной темы означают, что меры обеспечения информационной безопасности применяются незамедлительно и в соответствии с актуальными условиями. В качестве примера можно привести закрепление административной ответственности за дискредитацию вооруженных сил Российской Федерации. Соответствующая норма была закреплена в Кодексе об административных правонарушениях уже спустя месяц после того, как вооруженные силы приступили к началу выполнения специальной военной операции.

Ш.Г. Утарбеков в своей работе говорит о целесообразности выделения в качестве самостоятельного принципа обоснованность информационной безопасности [41, с. 34]. Сущность данного принципа можно охарактеризовать следующим образом. Меры, которые реализуются в рамках обеспечения информационной безопасности, должны быть эквивалентны потенциальному вреду, причиненному той или иной угрозой. Основным ориентиром в данном случае должны выступать права и свободы человека и гражданина, которые признаются высшей ценностью в российском государстве. При этом без внимания не должны оставаться и интересы общества в целом, а также

интересы самого государства. Таким образом, само по себе нарушение принципа обоснованности влечет за собой нарушение интересов личности, общества и государства. На практике реализация рассматриваемого принципа может выглядеть следующим образом. Например, в сети начинается активное распространение материалов, которое пропагандирует аморальное поведение и уходу от традиционных ценностей. Потенциально это может привести к морально-нравственному разложению молодых людей, которые находят в этих материалах ориентиры для определения модели поведения. В этой ситуации в первую очередь принимается решение о реализации программы, направленной на приобщение молодежи к традиционным семейным ценностям, поддерживаемым в Российской Федерации. Поскольку эффект от этих мероприятий недостаточный, а угроза остается на прежнем уровне, принимается решение о внедрение запрета на распространение материалов, которые пропагандируют поддержку движения ЛГБТ. Так как первичные меры не возымели эффекта, орган власти провел анализ и принял решение, что частичное ограничение права на свободу доступа и распространения отдельной информации соразмерно потенциальной угрозе.

М.К. Дзанагова и М.М. Бетеева выделяют принцип прогноза информационной безопасности [8, с. 273]. Реализация указанного принципа определяется тем, что субъекты обеспечения информационной безопасности осуществляют постоянный мониторинг, целью которого является обнаружение потенциальных угроз. После этого производится анализ всех имеющихся обстоятельств, по результатам которого прогнозируются возможные развития событий. На основе прогноза готовятся планы «поведения» уполномоченных субъектов в той или иной ситуации. В результате чего, угроза может быть устранена уже на начальном этапе, соответственно, охраняемым субъектам не будет нанесено никакого вреда, либо такой вред будет сведен к минимуму. В ходе реализации мероприятий, направленных на прогнозирование вероятного развития событий используется отечественный и зарубежный опыт обеспечения информационной

безопасности, а также предложения, заявленные специалистами, учеными и деятелями в данной сфере.

В качестве отдельного самостоятельного принципа допустимо обозначить принцип распределения обязанностей в сфере обеспечения информационной безопасности. Его сущность определяется тем, «что обязанности по обеспечению информационной безопасности должны быть распределены между некоторыми субъектами, при этом их роли должны быть в целом равнозначными. Более того, распределяя полномочия, необходимо предоставлять таким субъектам только те привилегии (права в рассматриваемой сфере), которые необходимы им для реализации возложенных задач. Концентрация полномочий у одного субъекта повышает возможность допущения ошибок, поскольку он принимает решение единолично и не согласует их с другими субъектами деятельности» [20, с. 18].

Завершая обсуждение по теме данного параграфа, нами были сделаны следующие выводы. Во-первых, информационная безопасность рассматривается как «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». Легальное определение, на наш взгляд, содержит в себе все основополагающие признаки, поэтому не требует каких-либо существенных корректировок. Во-вторых, нами было отмечено, что информационная безопасность может рассматриваться в двух ипостасях. С одной стороны, информационная безопасность направлена на обеспечение сохранности информации от противоправного завладения, использования, распространения, если законом предусмотрена ее охрана. Примером таких сведений является государственная тайна, тайна усыновления, тайна частной жизни и так далее. С другой стороны, информационная безопасность

подразумевает защиту населения от информации, которая может причинить вред человеку, обществу и государству. Говоря о вредоносной информации, имеются в виду сведения, которые потенциально могут нести опасность субъектам защиты информационной безопасности. В-третьих, система принципов обеспечения информационной безопасности характеризуется разнообразными структурными элементами, направленность которых не ограничивается одной только защитой от явных угроз. В ней также можно выделить принципы формирования системы анализа и прогнозирования, а также механизмов глубокой защиты.

1.2 Значение информационной безопасности для современной Российской Федерации

На сегодняшний день обеспечение информационной безопасности имеет особое значение для Российской Федерации. Этому способствуют различные обстоятельства, среди которых можно выделить два наиболее значительных. Во-первых, Российская Федерация является современным государством, которое стремится апробировать технологические разработки в различные сферы жизни общества (электронные талоны в больницу, личный кабинет на сайте государственных услуг с возможностью записаться на прием в государственные органы в режиме онлайн и так далее). Подобная политика постепенной цифровизации создает необходимость разработки эффективных механизмов защиты и охраны личных данных о гражданах. Однако на сегодняшний день нельзя сказать о том, что работа в этом направлении окончена, поскольку в новостях с определенной периодичностью появляются сведения об утечки баз данных с персональными данными в общее пользование или незаконное владение третьих лиц. Во-вторых, существенное влияние на необходимость принимать активное участие в регулировании процессов получения, распространения и размещения информации оказывает обостренный конфликт со странами НАТО и Евросоюза. Со стороны

недружественно настроенных государств ведутся активные попытки дестабилизировать обстановку внутри государства и нарушить основы конституционного строя путем информационного воздействия на население.

Следует отметить, что в доктрине информационной безопасности Российской Федерации перечислен ряд угроз, что, на наш взгляд, подчеркивает важность вопроса обеспечения информационной безопасности в нашем государстве. Одной из таких угроз является применение механизмов информационного воздействия в рамках осуществления деятельности террористическими и экстремистскими образованиями. При помощи информационного воздействия подобного рода организации могут создавать социальное напряжение, разжигать религиозную вражду, пропагандировать экстремистские идеалы, вербовать людей для террористической деятельности. Для подобной деятельности, как правило, используются различные площадки: социальные сети и мессенджеры (ВКонтакте, Facebook, Instagram, WhatsApp, Viber, Telegram). Наибольшая вероятность оказаться в поле информационного воздействия террористических и экстремистских организаций у представителей молодежи. Исследователи отмечают, что «целевой аудиторией являются в основном молодые люди, с 16 до 35 лет, которые имеют личные проблемы» [29, с. 389]. Поскольку социальные сети и мессенджеры плотно вошли в жизнь большинства граждан, вопросы обеспечения информационной безопасности, в частности, регулирование информационного потока, как в самой сети «Интернет», так и непосредственно в самих социальных сетях, приобретает высокую степень актуальности и значимости.

Определяя значимость информационной безопасности для современной Российской Федерации, следует обратиться к отдельным статистическим данным. Так, в 2019 году число преступление с использованием информационных технологий составляло 294,5 тысячи. В 2020 году этот показатель составил уже 510 тысяч преступлений, а в 2021 году возрос практически до 518 тысяч [23]. Исследователи в области киберпреступности

отмечают, что такие преступления «характеризуются высокой латентностью и низкой раскрываемостью, в том числе из-за возможности дистанционного совершения данных преступлений. Общая раскрываемость данной категории дел составляет в среднем 20% ежегодно» [47, с. 187]. Высокий показатель преступлений, совершаемых с использованием информационных технологий, в совокупности с низким показателями раскрываемости свидетельствуют о том, что на сегодняшний день еще не разработаны эффективные механизмы предупреждения и раскрытия таких преступлений. Указанное обстоятельство в очередной раз свидетельствует о значимости развития механизмов обеспечения информационной безопасности в современной России.

Говорить о значение информационной безопасности можно и по той причине, что законодатель наделяет граждан широким перечнем прав и свобод в информационной сфере. Отдельные права и свободы закрепляются в нормах основного закона. Поскольку Российская Федерация является демократическим государством, основным приоритетом которого является человек, его права и свободы, законодатель стремится предоставить гражданам максимальный объем возможностей. При этом соблюдает необходимый баланс между возможностями и ограничениями. Важной задачей здесь является практическая составляющая реализации прав и свобод, а также реальная возможность привлечь нарушителя к установленной законом ответственности. Однако проблемы имеют место быть не только на практике, но и на уровне правового регулирования. В ряде нормативно-правовых актов имеются пробелы и коллизии. Более подробно мы рассмотрим данный вопрос в следующей главе.

«Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран» [34, с. 8]. Особенно остро

данная проблема проявляется в условиях ухода иностранных компаний с отечественного рынка. В том случае, если ситуация не изменится, то последствия начнут проявляться в ближайшее время, поскольку на разработку отечественного программного обеспечения и технического оборудования потребуется куда больше времени, чем потенциально имеется в запасе. Отсутствие должного программного и технического обеспечения может создать ряд уязвимостей, при помощи которых злоумышленники смогут противоправными способами получать доступ к охраняемой законом информации.

Говоря о недостаточном уровне развития отечественного программного и технического обеспечения, стоит обратить внимание, что отдельная часть специалистов в сфере IT покинули территорию Российской Федерации и выполняют свою работу удаленно с территории других государств. При этом важно понимать, что технически доступ к информации в различных сферах жизни российского общества осуществляется через зарубежных провайдеров, что потенциально создает угрозу информационной безопасности. На наш взгляд, данный вопрос требует особого внимания, поскольку на сегодняшний день отсутствует запрет на доступ к отечественному сетевому окружению при удаленной работе за пределами территории Российской Федерации. При этом многие иностранные компании релоцировали своих сотрудников в другие страны, поскольку зарубежные клиенты, находящиеся в недружественных странах, по той же причине ограничили удаленный доступ к своему сетевому окружению из Российской Федерации.

Значимость информационной безопасности в системе обеспечения национальной безопасности определяется также и тем, что информационные технологии имеют высокую динамику развития. Именно это обстоятельство требует от системы обеспечения информационной безопасности гибкости и соответствию актуальным реалиям. Появление новых угроз требует быстрого реагирования и разработки мер (как технических, так и правовых) для их предупреждения и противодействия. Кроме того, стоит обратить внимание,

что в стране наблюдается реальное отсутствие квалифицированных кадров, причем не только в сфере IT, но и среди сотрудников правоохранительных органов. Именно это обстоятельство и является причиной низкой раскрываемости преступлений с использованием информационных технологий. Развитие информационной безопасности должно включать в себя, в том числе и проведение академических мероприятий, направленных, во-первых, на повышение информационной грамотности среди населения, а также повышения квалификации сотрудников, задействованных во всех учреждениях, обеспечивающих стабильность системы информационной безопасности.

Совокупность указанных обстоятельств позволяет нам сделать вывод, что информационная безопасность в условиях актуальной действительности имеет важное значение для Российской Федерации, поскольку угрозы, характерные для данного сектора, охватывают своим негативным влиянием все сферы жизни общества и несут угрозы интересам личности, общества и государства.

Завершая обсуждение по теме данной главы, нами были сделаны следующие выводы. Во-первых, информационная безопасность рассматривается как «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». Легальное определение, на наш взгляд, содержит в себе все основополагающие признаки, поэтому не требует каких-либо существенных корректировок. Во-вторых, нами было отмечено, что информационная безопасность может рассматриваться в двух ипостасях. С одной стороны, информационная безопасность направлена на обеспечение сохранности информации от противоправного завладения, использования,

распространения, если законом предусмотрена ее охрана. Примером таких сведений является государственная тайна, тайна усыновления, тайна частной жизни и так далее. С другой стороны, информационная безопасность подразумевает защиту населения от информации, которая может причинить вред человеку, обществу и государству. Говоря о вредоносной информации, имеются в виду сведения, которые потенциально могут нести опасность субъектам защиты информационной безопасности. В-третьих, система принципов обеспечения информационной безопасности характеризуется разнообразными структурными элементами, направленность которых не ограничивается одной только защитой от явных угроз. В ней также можно выделить принципы формирования системы анализа и прогнозирования, а также механизмов глубокой защиты. В-четвертых, значение информационной безопасности в Российской Федерации определяется наличием рядом проблемных аспектов, к их числу мы можем отнести: высокий показатель преступлений с использованием информационных технологий и их низкая раскрываемость, использование социальных сетей и мессенджеров террористическими и экстремистскими организациями в ходе осуществления своей деятельности, отсутствие должного уровня развития отечественного программного и технического обеспечения.

Глава 2 Элементы правового регулирования информационной безопасности

2.1 Конституционно-правовые основы регулирования информационной безопасности

Правовые нормы, направленные на обеспечение информационной безопасности, содержатся в нормативно-правовых актах различных уровней. При этом основа всей системы обеспечения информационной безопасности заложена в нормах Конституции Российской Федерации. Рассмотрим каждую из норм, содержащих элементы правового статуса в сфере информационной безопасности, в отдельности с целью выявления проблемных аспектов на стадии ее формирования.

В первую очередь необходимо проанализировать положения статьи 29 Конституции Российской Федерации, а именно часть четвертую. Ее содержание определено следующим положением: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» [16]. Хотя законодатель провозглашает свободу получения и распространения информации, сразу делается оговорка о ее относительности. Соответственно, мы можем сделать вывод, что свобода и распространение информации является не абсолютным правом и в отдельных случаях может ограничиваться законодателем. В этой сфере важную роль играет понятие государственной тайны. Его законодательная дефиниция определена в статье второй Закона Российской Федерации «О государственной тайне». Выглядит оно следующим образом. «Государственная тайна - защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации» [10]. Законодатель строит определение при помощи перечисления

основных категорий сведений, которые подлежат государственной охране в силу своей значимости для обеспечения безопасности общества и государства. Более подробно перечень сведений, отнесенных к категории «государственная тайна», рассматривается в статье пятой рассматриваемого нормативно-правового акта. Так, к числу засекреченных данных в области внешней политики и экономики законодатель относит сведения: о внешнеполитической деятельности, если распространение такой информации может стать угрозой для безопасности государства, о финансовых взаимоотношениях с другими государствами, если такая информация может нести угрозу безопасности государства. Хотя институт государственной тайны служит в качестве инструмента для ограничения права на свободу доступа и распространения в целях обеспечения национальной безопасности, законодатель счел необходимым отдельные категории сведений сделать «неприкосновенными». То есть, отдельная информация не может быть отнесена к категории государственной тайны не при каких обстоятельствах. Перечень такой информации предусмотрен статьей седьмой рассматриваемого закона. К категории «государственная тайна» не могут быть отнесены сведения следующего содержания:

– «о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;

– о состоянии здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;

– о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;

– о фактах нарушения прав и свобод человека и гражданина;

– о состоянии здоровья высших должностных лиц Российской Федерации;

– о фактах нарушения законности органами государственной власти и их должностными лицами;

– составляющие информацию о состоянии окружающей среды (экологическую информацию)» [10].

Анализируя список сведений, которые не могут быть отнесены к государственной тайне, мы делаем следующий вывод. Обозначенная информация непосредственно затрагивает сферу интересов граждан, поэтому факт ее сокрытия, подразумевает нарушение прав и свобод граждан. В этой связи законодатель закрепляет различные меры ответственности за сокрытие информации, которая не подлежит засекречиванию. Нарушитель может быть привлечен к дисциплинарной, административной или уголовной ответственности за содеянное. Мера ответственности зависит от того, какой реальный или потенциальный вред был причинён (мог быть причинен) личности, обществу или государству.

Отдельно стоит заметить, что законодатель запрещает скрывать информацию о льготах, предоставляемых государством. При буквальном толковании данной нормы, можно прийти к выводу, что речь идет только о привилегиях, компенсациях, социальных гарантиях, которые предоставляются органами государственной власти или органами власти субъектов. Таким образом, без внимания остаются льготы, которые предоставляются гражданам за счет средств из бюджета муниципального образования, поскольку муниципальная власть не входит в понятие государственной власти. Для устранения данной неточности в тексте закона, мы предлагаем дополнить абзац 4-ый статьи 7-ой Закона Российской Федерации «О государственной тайне» так, чтобы по смыслу ее новой редакции было очевидно, что запрещается относить к категории государственная тайна льготы, предоставляемые государством и муниципальными образованиями.

Другое положение основного закона, которое регулирует сферу информационных правоотношений, предусмотрено статьей 23. В ней

законодатель закрепил право каждого на личную и семейную тайну. Сразу же стоит обратить внимание, что легальное определение употребляемых понятий не содержится в отечественном законодательстве. Равно как и отсутствуют его признаки и сущностные критерии, благодаря которым можно отнести ту или иную информацию к категории «личная тайна» и «семейная тайна». Анализируя данную норму при помощи системного толкования, стоит обратить внимание на часть 3-ю статьи 25 Федерального закона «Об архивном деле в Российской Федерации». В ней закреплено, что «ограничение на доступ к архивным документам, содержащим сведения о личной и семейной тайне гражданина, его частной жизни, а также сведения, создающие угрозу для его безопасности, устанавливается на срок 75 лет со дня создания указанных документов» [42]. Хотя закон и устанавливает запрет, он оставляет вопросы толкования данной нормы сотрудникам архива. Поскольку какой-либо единый подход к данному вопросу отсутствует, такое толкование может быть расширительным, создавая возможность для злоупотребления данной нормой в личных интересах. Отсутствие единых критериев к понятию личной и семейной тайны способствует дестабилизации единообразия правоприменительной практики. На практике это выражается в том, что в одних обстоятельствах идентичные сведения могут признаваться личной или семейной тайной, а в других могут считаться общедоступными.

Конституционным Судом предпринимались попытки разъяснить смысл понятия «частная жизнь». «Право на неприкосновенность частной жизни означает предоставленную человеку и гарантированную государством возможность контролировать информацию о самом себе, препятствовать разглашению сведений личного, интимного характера. В понятие частная жизнь включается та область жизнедеятельности человека, которая относится к отдельному лицу, касается только его и не подлежит контролю со стороны общества и государства, если она носит непротивоправный характер» [26]. Суд весьма поверхностно раскрыл критерии, которые позволяют нам оценить те или иные сведения и сделать вывод относительно их отнесения к категории

частная жизнь. Единственное, что Суд определил достаточно четко, это тот факт, что информация о совершенных противоправных деяниях не может быть отнесено к сведениям о частной жизни.

Возвращаясь к понятиям личной и семейной тайны, мы можем предположить, что это собирательные понятия, которые включают в себя информацию личного и семейного характера. Здесь стоит добавить, что, по сути, семейная тайная является частью личной тайны, поскольку информация о семье является личной. Так, право не свидетельствовать против своего супруга и близких родственников является личным право каждого, независимо от гражданства и прочих условий. Поэтому не совсем понятно, почему законодатель выделил в качестве отдельных категорий личную и семейную тайну. Возможно, это обусловлено как раз тем обстоятельством, что родственные и семейные отношения являются конституционно-правовым основанием для свидетельского иммунитета. Мы, безусловно, можем отнести к личной тайне сведения, составляющие врачебную тайну [45] или тайну совершения завещания [6]. К семейной тайне мы можем отнести тайну усыновления [32].

Упомянутые в Конституции понятия «личная тайна» и «семейная тайна» должны не просто провозглашаться в положениях основного закона, но и в дальнейшем конкретизироваться в положениях других нормативно-правовых актов. Так, ранее рассмотренное нами право на свободу распространения и ознакомления с информацией достаточно детально находит свое отражение в положениях нормативно-правовых актов различных уровней: устанавливаются механизмы ограничения права, гарантии его реализации и так далее. Для устранения указанной проблемы мы видим возможным раскрыть основные критерии отнесения информации к категориям личная и семейная тайна. В этом случае станет возможным не просто ссылаться на наличие такого понятия в законодательстве, а мотивировать то или иное решение о допуске или отказе в допуске к информации, ссылаясь на конкретные критерии. Это позволит решить ряд проблем, в том числе и

рассмотренную нами выше, связанную с неправильным толкованием понятий личная тайна и семейная и последующий неправомерный отказ в доступе к информации или, напротив, неправомерный доступ к получению информации.

Помимо прав и свобод в сфере информационной безопасности основной закон страны содержит отдельные обязанности. В статье 24 Конституции предусмотрена обязанность органов государственной власти и местного самоуправления обеспечить возможность ознакомиться с документами и материалами, затрагивающими его права и свободы. При этом мы осознаем, что обязанность также, как и корреспондирующее ей право не является абсолютной. Так, отдельная информация, например, в сфере государственной обороны, прямо или косвенно затрагивает права и свободы граждан. Но нужно понимать, поскольку они входят в категорию охраняемых законом сведений, соответствующая обязанность не будет распространяться на государственные органы.

Следует обратить внимание на статью 28 Конституции, в которой закреплена свобода вероисповедания. Формально она относится к категории личных прав и свобод, но все же гарантирует право каждого распространять информацию об исповедуемых религиозных убеждениях. Однако, распространение сведений ограничивается законом. Речь идет о религиозных убеждениях, которые проповедуют постулаты, которые идут в разрез с традиционными ценностями и положениями законодательства. Например, однополые браки, насилие, расовое превосходство и так далее. Информация о таких убеждениях не подпадает под реализацию права на свободное распространение информации и в отдельных случаях подлежит ответственности, например, по статье 282 Уголовного кодекса [36]. В связи с этим мы рекомендуем представить статью 28 Конституции в следующей редакции: «Каждому гарантируется свобода совести, свобода вероисповедания, включая право исповедовать индивидуально или совместно с другими любую религию или не исповедовать никакой. Каждый имеет право свободно выбирать, иметь и распространять религиозные и иные убеждения и

действовать в соответствии с ними, если это не противоречит законодательству Российской Федерации».

Особую значимость в обеспечении информационной безопасности имеют механизмы цензурирования. Цензура выступает своего рода универсальным инструментом ограничения распространения информации, но в тоже время является тоталитарным явлением, противоречащим самой сущности демократизма. В этой связи важно рассмотреть положения статьи 29 основного закона. В части 5-ой указанной статьи закреплено два важных положения. Во-первых, гарантия свободы массовой информации. Во-вторых, запрет на цензуру. В условиях информационного противодействия вопросы цензуры имеют особенно актуальный характер, поскольку определенные темы и высказывания подлежат ограничению, что вызывает дискуссии на данную тему. С точки зрения закона, легальное определение понятия цензура представляется следующим образом: «Цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей» [11]. Анализируя данное определение, можно отметить, что в нем нет никаких указаний относительно опосредованного воздействия на законную деятельность СМИ. Такое воздействие может совершаться при помощи анонимных угроз, намеков и других способов. Например, на руководителя средства массовой информации может неформально надавить сотрудник органа власти, аргументируя тем, что распространение той или иной информации нанесет ущерб репутации органа государственной власти, за отказ сотрудничать, могут последовать обещания о создании проблем с законом. В связи с этим мы выступаем за дополнение законодательного понятия цензура. На наш взгляд, требуется указать, что

цензурой, в том числе, является опосредованное требование об удалении или не публикации информации в средствах массовой информации.

С.А. Привалов в своем исследовании, посвященном ограничению распространении информации, заявляет о наличии негласной цензуры. В подтверждение заявленной позиции автор приводит примеры, когда СМИ, публикующие новости оппозиционных движений, потеряли свой статус ввиду не совсем понятных причин. Как правило, в качестве основания, лежащего в основе решения, лежит формулировка «призыв к незаконному участию в массовых мероприятиях» [28, с. 17]. Можно согласиться с тем обстоятельством, что издания и лидеры мнений, которые выступали против политики государственной власти подвергались блокировке в российском интернете, признавались иностранными агентами, а также подвергались другим мерам государственного принуждения. Однако, на наш взгляд, не совсем корректно называть это цензурой. В описанных случаях органы власти действуют в рамках своей компетенции и в соответствии с юридическими нормами. С точки зрения действующего законодательства, такие действия не могут квалифицироваться в качестве цензуры. Нельзя не согласиться с тем обстоятельством, что органы власти влияют на распространение информации, при этом важно оценить контекст таких действий. В условиях информационного противостояния, когда на население оказывается основное давление при помощи информации, а СМИ с высокой вероятностью могут быть подвержены влиянию недружественных государств, органы власти могут предпринимать действия, которые направлены на ограничение источников распространения информации, которые могут оказать дестабилизирующее воздействие на общество. Поэтому, на наш взгляд, воздействие органов власти оправдано, отвечает актуальным реалиям, поэтому говорить о негласной цензуре неуместно.

В числе прочих конституционных гарантий, некоторые исследователи, отдельно выделяют право на обращение граждан, право на получение достоверной информации об окружающей среде, свидетельский иммунитет

супругов и близких родственников [22, с. 19]. Анализируя данную группу прав, в целом можно согласиться с данной позицией. Важно понимать, что конституционные права могут иметь различные сущностные признаки, а само их разделение на несколько групп имеет условный характер. Право на обращение граждан может служить инструментом для достижения определенных целей в информационной сфере. Так, подавая обращение, гражданин может запросить предоставить ему доступ к определенной информации, которая прямо или косвенно затрагивает его права и свободы. Такой информацией могут стать, например, сведения о благоустройстве города, о социальном такси, городские планы и так далее. Поскольку право на обращение реализуется при условии соблюдения государственной и иной охраняемой законом тайны, мы можем отнести его к числу основ обеспечения информационной безопасности в Российской Федерации.

Другое приведенное выше право на достоверную информацию об окружающей среде, также может быть отнесено к числу основ обеспечения информационной безопасности. С его помощью определяется порядок доступа граждан к сведениям, связанным с состоянием окружающей среды непосредственно в стране, в конкретном субъекте или муниципалитете. Данная информация не может стать государственной тайной, поскольку законодатель внес данные сведения в специальный перечень данных, которые не при каких обстоятельствах не могут подлежать засекречиванию.

Свидетельский иммунитет родственников и супругов также может быть отнесен нами к основам обеспечения информационной безопасности. Следует также отметить, что он непосредственно связан с ранее рассмотренными нами понятиями личной и семейной тайны. Здесь стоит обратить внимание на следующее обстоятельство. Хотя Пленум Верховного Суда установил, что предметом тайны частной жизни не может выступать информация о совершенных правонарушениях, законодатель оставляет право разглашения той или иной информации, полученной в результате родства или семейной связи с возможным правонарушителем, за свидетелем этих событий. Дело в

том, что противоправными действия могут быть признаны только по решению суда и в отдельных случаях по решению уполномоченных лиц, до этого момента указанная информация охраняется личной или семейной тайной для соответствующего круга лиц.

Еще одной конституционно-правовой основой обеспечения информационной безопасности является ответственность за сокрытие данных, которые так или иначе создают угрозу жизни или здоровью гражданина (часть 3 статьи 41 Конституции). Содержание данного положения позволяет нам сделать вывод, что граждане обладают правом получать информацию об обстоятельствах, которые потенциально могут причинить вред их жизни или здоровью. Положение, предусмотренной частью 3 статьи 41 Конституции, находит свое развитие в статье 237 Уголовного кодекса. Максимальная санкция за сокрытие информации, которая привела к тому, что человеку был причинен вред или наступили иные тяжкие последствия, предусматривает наказание в виде лишения свободы сроком до пяти лет. Более детально вопросы ответственности за нарушения в сфере обеспечения информационной безопасности будут рассмотрены нами в следующем параграфе.

Подводя промежуточные итоги по теме данного параграфа, мы можем сделать следующие выводы касательно конституционно-правовых основ обеспечения информационной безопасности.

Во-первых, основной закон государства содержит в себе широкий перечень положений, так или иначе, связанных с вопросами обеспечения информационной безопасности в Российской Федерации.

Во-вторых, при буквальном толковании абзаца 4-го статьи 7-ой Закона Российской Федерации «О государственной тайне», можно прийти к выводу, что речь идет только о привилегиях, компенсациях, социальных гарантиях, которые предоставляются органами государственной власти или органами власти субъектов. Таким образом, без внимания остаются льготы, которые предоставляются гражданам за счет средств из бюджета муниципального образования, поскольку муниципальная власть не входит в понятие

государственной власти. Для устранения данной неточности в тексте закона, мы предлагаем дополнить абзац 4-ый статьи 7-ой Закона Российской Федерации «О государственной тайне» так, чтобы по смыслу ее новой редакции было очевидно, что запрещается относить к категории государственная тайна льготы, предоставляемые государством и муниципальными образованиями.

В-третьих, в ходе исследования нами было обращено внимание, что упомянутые в Конституции понятия «личная тайна» и «семейная тайна» должны не просто провозглашаться в положениях основного закона, но и в дальнейшем конкретизироваться в положениях других нормативно-правовых актов. Для устранения указанной проблемы мы видим возможным раскрыть основные критерии отнесения информации к категориям личная и семейная тайна. В этом случае станет возможным не просто ссылаться на наличие такого понятия в законодательстве, а мотивировать то или иное решение о допуске или отказе в допуске к информации, ссылаясь на конкретные критерии. Это позволит решить ряд проблем, в том числе и рассмотренную нами выше, связанную с неправильным толкованием понятий личная тайна и семейная и последующий неправомерный отказ в доступе к информации или, напротив, неправомерный доступ к получению информации.

2.2 Организационные основы регулирования информационной безопасности

Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности. 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. Другими словами, в процессе осуществления информационной

безопасности принимают участие все органы власти законодательной, исполнительной и судебной власти всех уровней, также задействованы органы, которые не входят не в одну из ветвей власти, например, прокуратура и органы местного самоуправления. Помимо государственно-властных субъектов в процессе обеспечения информационной безопасности задействован общественный потенциал в лице активных граждан и их объединений. Только совместная деятельность позволяет выявлять угрозы еще на раннем этапе и оперативно их устранять.

«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» [37].

Стоит обратить внимание, что деятельность тех или иных упомянутых субъектов может быть полностью не направлена на обеспечение информационной безопасности, при этом их отдельные полномочия могут быть реализованы в данной сфере в части охраны особо важной информации, а также ограничения распространения вредоносной для государства, общества

и личности информации. Так, Государственная Дума и Совет Федерации занимаются подготовкой и принятием законов, регулирующих все основные отношения в обществе. Соответственно, они разрабатывают в том числе и законопроекты в сфере обеспечения информационной безопасности. В полномочия органов исполнительной власти субъектов входят вопросы по разработке и принятию основных начал реализации мероприятий, направленных на обеспечение информационной безопасности в рамках конкретного субъекта. Разумеется, концепции субъекта могут развивать положения, предусмотренные федеральной концепции, но не могут вступать с ней в противоречия.

Отдельно стоит обратить внимание, что среди субъектов отсутствует упоминание Президента Российской Федерации. При этом в его компетенцию входят полномочия в сфере обеспечения информационной безопасности. В качестве примера приведем статью 6-ю Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». В ней указано, что «Президент Российской Федерации определяет основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры» [43]. Кроме того, в полномочия президента входит подписание всех федеральных законов, в том числе и в рассматриваемой сфере, а также утверждение Доктрины информационной безопасности. В связи с этим не совсем понятно, по какой причине Президент не входит в рассмотренный выше перечень организационных основ. Поэтому мы видим возможным с целью обеспечения целостности организационных основ в сфере обеспечения информационной безопасности включить в список организационных основ Президента Российской Федерации, так как, он обладает широкими полномочиями в регулировании вопросов в сфере информационной безопасности.

Деятельность субъектов в сфере обеспечения информационной безопасности основывается на следующих основных началах, положениях, идеях:

– «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» [37].

Анализируя представленный перечень принципов обеспечения информационной безопасности, необходимо отметить следующее. Первые три пункта олицетворяют собой принципы законности, равенства всех перед законом, а также свободу информации. Учитывая специфику и узкую направленность Доктрины, не совсем понятно, по какой логике законодатель отдельно отмечает два общеправовых принципа, которые, равно как и другие принципы данной группы, распространяют свое действие на сферу обеспечения информационной безопасности. В этом случае, на наш взгляд, указание общеправовых принципов в Доктрине не требуется. В свою очередь принцип свободы информации, хотя и провозглашается основным законом и может рассматриваться в качестве общеправового, он отражает специфику данной сферы.

Принцип конструктивного взаимодействия подразумевает, что уполномоченные субъекты осуществляют свои полномочия в сфере информационной безопасности не отстраненно друг от друга, а в условиях совместной работы. Это продиктовано необходимостью решения вопросов, затрагивающих компетенцию нескольких органов власти, разработки новых методов регулирования отношений в сфере информационной безопасности, а также разрешения спорных ситуаций. Следует отметить, что Доктрина подразумевает взаимодействие между госорганами, объединениями и гражданами. При этом без внимания остаются органы местного самоуправления, которые законодателем включены в список организационных основ. Как уже было отмечено ранее, органы местного самоуправления не могут быть отнесены к государственным органам, поэтому, мы считаем, что следует дополнить рассматриваемый нами принцип и представить его следующим образом: «конструктивное взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности».

Принцип соблюдения баланса является несколько абстрактным, поскольку баланс или равновесие является субъективной величиной. Назначение данного принципа заключается в том, чтобы при обеспечении информационной безопасности уполномоченные субъекты не злоупотребляли средствами, характерными для метода принуждения. Другой вопрос здесь заключается в том, что следует понимать в качестве потребности граждан в свободном обмене информации. Поскольку данное понятие нигде не раскрыто, весьма сложно определить, где находится такой баланс. Наличие такой абстрактной категории не обеспечивает должного баланса интересов, ограничивая тем самым право на свободу распространения информации.

Рассматривая тему организационных основ системы информационной безопасности, следует уделить внимание средствам обеспечения информационной безопасности. Доктрина позволяет выделить следующие специфические средства: правовые, организационно-технические и

экономические. Экономические меры направлены на определение порядка финансирования механизмов обеспечения информационной безопасности, а также страхования информационных рисков. Сюда входит разработка новых технологий для защиты охраняемых законом сведений и ограничения вредоносной информации.

Технические меры, в свою очередь, можно разделить на программные и аппаратные механизмы. Они отражают этап реализации правовых норм в реальной жизни. Например, руководствуясь правовой нормой, суд принял решение заблокировать сайт на территории Российской Федерации. В этом случае для практической реализации решения суда требуется программное обеспечение, которое позволит произвести такую блокировку. Можно предположить, что только при помощи технических средств можно построить действенную систему обеспечения информационной безопасности, поскольку именно они лежат в основе практической реализации всех мероприятий. Однако, такое суждение не является верным, поскольку эффективная система имеет место быть только в том случае, когда все уникальные по своей сути меры, выполняют определенный функционал в рамках достижения единой цели – обеспечения информационной безопасности.

Правовые меры представляют собой юридические нормы, которые регулируют вопросы в информационной сфере. Правовые средства можно разделить в зависимости от места нормы в иерархии. Так, можно выделить конституционные нормы, нормы федеральных законов, нормы подзаконных актов. Также мы можем разделить правовые средства на регулятивные и охранительные. Первые используются для урегулирования отношений в сфере распространения и получения доступа к информации, вторые предупреждения, пресечения правонарушений в сфере информационной безопасности, а также для привлечения к ответственности за совершение таких правонарушений.

«Отдельные авторы выделяют в качестве отдельной категории морально-этические меры обеспечения информационной безопасности.

Морально-этические меры задают правила обращения с информацией и накладывают определенную степень ответственности за их несоблюдение. Различают два направления: создание и поддержание в обществе негативного отношения к нарушениям и нарушителям по отношению к информационной безопасности, в том числе и карательного характера. Второе заключается в координации действий, направленных на повышение уровня образованности и информированности общества в области информационной безопасности» [21, с. 46]. Мы разделяем позицию автора по данному вопросу. Подобный подход имеет место быть в сфере противодействия коррупции, где морально-этические меры применяются с целью снижения факторов, способствующих совершению правонарушений. Развитие правовой культуры в целом способно снизить число совершаемых правонарушений в обществе. Если это положение характерно для общего, то мы можем применить его и к частному (сфере обеспечения информационной безопасности). За последние несколько лет уполномоченные субъекты прибегали к использованию морально-этических мер относительно часто. Так, в период распространения коронавирусной инфекции государственные информационные ресурсы пытались распространять информацию о ложных сообщениях, которые могли ввести население в заблуждение и несли угрозу обществу. Сейчас аналогичную картину мы можем наблюдать в вопросе распространения ложной информации о ходе проведения специальной военной операции. Мы положительно оцениваем применение морально-этических мер в сфере обеспечения информационной безопасности, поскольку в актуальных условиях особенно важно повысить уровень правовой культуры граждан и закрепить в их сознании установку о губительном влиянии распространения недостоверной информации, а также совершения других правонарушений, которые могут причинить вред и так находящейся под угрозой информационной сфере. Подобные нарушения могут вызвать панику и иные неблагоприятные для общества последствия.

Подводя промежуточные итоги по теме данного параграфа, мы можем сделать следующие выводы касательно организационных основ обеспечения информационной безопасности.

Во-первых, мы видим возможным с целью обеспечения целостности организационных основ в сфере обеспечения информационной безопасности включить в список организационных основ Президента Российской Федерации, так как, он обладает широкими полномочиями в регулировании вопросов в сфере информационной безопасности.

Во-вторых, отдельно нами было обращено внимание на то, что Доктрина подразумевает взаимодействие между госорганами, объединениями и гражданами. При этом без внимания остаются органы местного самоуправления, которые законодателем включены в список организационных основ. Как уже было отмечено ранее, органы местного самоуправления не могут быть отнесены к государственным органам, поэтому, мы считаем, что следует дополнить рассматриваемый нами принцип и представить его следующим образом: «конструктивное взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности».

В-третьих, Мы положительно оцениваем применение морально-этических мер в сфере обеспечения информационной безопасности, поскольку в актуальных условиях особенно важно повысить уровень правовой культуры граждан и закрепить в их сознании установку о губительном влиянии распространения недостоверной информации, а также совершения других правонарушений, которые могут причинить вред и так находящейся под угрозой информационной сфере. Подобные нарушения могут вызвать панику и иные неблагоприятные для общества последствия.

2.3 Особенности правового регулирования информационной безопасности в сети «Интернет»

На сегодняшний день особенно остро стоит вопрос обеспечение информационной безопасности в сети «Интернет». Дело в том, что на сегодняшний день использование интернета стало неотъемлемой частью жизни большинства членов общества. Обращаясь к статистическим данным, мы видим, что в среднем каждый человек проводит в сети «Интернет» порядка семи часов. Интернет используется в различных целях, например, для развлечений, для поиска информации, для общения и так далее [50]. С учетом того обстоятельства, что в среднем человеку требуется восемь часов для сна, то по представленным данным человек проводит половину времени своего бодрствования в интернет-пространстве. Это обстоятельство указывает на то, что государству необходимо уделить пристальное внимание вопросам обеспечения информационной безопасности в сети «Интернет».

Государство осознает роль интернета в жизни общества, поэтому предпринимает попытки по регулированию отношений в сети «Интернет». Так, порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационнотелекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационнотелекоммуникационной сети «Интернет», утвержден Указом Президента РФ от 22 мая 2015 г. №260 «О некоторых вопросах информационной безопасности Российской Федерации». Согласно которому, «подключение информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет», осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств, а их защита обеспечивается в соответствии с законодательством Российской Федерации» [39].

Кроме того, для обеспечения информационной безопасности в сети «Интернет» установлены следующие правила:

– «подключение информационных систем, информационнотелекоммуникационных сетей и средств вычислительной

техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну, либо информации, обладателями которой являются государственные органы и которая содержит сведения, составляющие служебную тайну, к информационно-телекоммуникационным сетям, позволяющим осуществлять передачу информации через государственную границу Российской Федерации, в том числе к международной компьютерной сети не допускается;

− средства защиты, которыми пользуются государственные органы, в обязательном порядке должны пройти сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю;

− размещение технических средств, подключаемых к информационно-телекоммуникационным сетям международного информационного обмена, в помещениях, предназначенных для ведения переговоров, в ходе которых обсуждаются вопросы, содержащие сведения, составляющие государственную тайну, осуществляется только при наличии сертификата, разрешающего эксплуатацию таких технических средств в указанных помещениях» [38].

Следует обратить внимание, что правовому регулированию в сети «Интернет» характерен ряд проблемных аспектов. Анализ научных работ по данному вопросу позволил выявить наиболее часто выделяемые проблемы, характерные данной сфере регулирования:

– «распространение экстремистских материалов в сети» [48, с. 161];

– «проблемы, связанные с защитой прав интеллектуальной собственности в сети» [30, с. 10];

– «проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя)» [31, с. 383];

– проблема защиты персональных данных граждан;

– проблема распространения сведения о наркотических веществах, в частности их продажи;

– противоправное распространение порнографических материалов, в том числе материалов с участием несовершеннолетних;

– активное распространение мошенничества в сети «Интернет».

Относительно распространения экстремистских материалов следует обратить внимание на следующее обстоятельство. В отдельных случаях правоохранительные органы проявляют чрезмерную бдительность для ограничения их распространения. Так, правоприменительная практика знает ряд случаев, когда по статье 282 Уголовного кодекса к ответственности привлекались лица за лайки и репосты записей в социальных сетях. Так, Евгений Корт был приговорен к году в колонии поселения, поскольку в социальной сети «Вконтакте» в альбоме сохраненные фотографии разместил фото Максима Марцинкевича, который являлся националистом и лидером запрещенной организации [13]. В другом случае Дмитрий Третьяков переслал сообщение с канала в беседу из нескольких человек. В посте содержались рассуждения относительно митингах в Российской Федерации, которые судебная психолого-лингвистической экспертиза было оценила, как призывы к насильственным и деструктивным действиям [25, с. 95]. Весьма размытые законодательные формулировки понятия «экстремизм» позволяют за действия в социальных сетях обвинить лицо, например, в публичном оправдании терроризма, возбуждении расовой, религиозной, социальной розни, пропаганде расового превосходства и так далее. На наш взгляд, сложившаяся практика позволяет использовать борьбу с экстремизмом для карательных и показательных нужд. Особенно явно это прослеживается в том, что зачастую к ответственности привлекается конкретное лицо из числа многих, кто лайкнул или переслал информацию. В отдельных случаях даже автор распространяемой информации не привлекается к ответственности. В связи с этим мы предлагаем следующие рекомендации по совершенствованию правового регулирования противодействия распространения экстремистских

материалов. Во-первых, необходимо более подробно разъяснять объективную сторону преступлений, предусмотренных статьями 280, 280.1, 282 Уголовного кодекса, в том числе разъяснить практику применения данных норм в отношении действий в социальных сетях. Во-вторых, требуется смягчение уголовной ответственности за такие действия, поскольку их общественная опасность несоразмерна назначаемым наказаниям. В-третьих, в первую очередь необходимо привлекать авторов распространяемой информации, которая признана содержащей элементы экстремистских высказываний, а уже только после этого лиц, которые ее распространяют.

В качестве инструмента предотвращения распространения вредоносной информации в сети «Интернет» чаще всего применяется блокировка. Для блокировки той или иной информации (конкретного ресурса) необходимо подать административное исковое заявление. Суд оценивает доводы заявителя и принимает решение об отказе в удовлетворении требований или о блокировке информации, которая не соответствует требованиям отечественного законодательства. После вступления решения в законную силу оно направляется в Роскомнадзор. Роскомнадзор, руководствуясь судебным решением, вносит запись в реестр и уведомляет владельца ресурса о необходимости удалить конкретную информацию. После этого в установленный срок владелец ресурса должен удалить вредоносную информацию, если он этого не сделает, то его ресурс может быть заблокирован на территории Российской Федерации. Здесь стоит обратить внимание, что блокировка не всегда эффективна, поскольку для доступа к заблокированной информации или ресурсу могут быть использованы программы, которые находятся в открытом доступе. Также владелец ресурса может создать сайт «зеркало», который имеет аналогичное содержание, но располагается по другому адресу. В этой связи стоит рассмотреть возможность запретить использование VPN сервисов на территории Российской Федерации с целью предотвращения доступа к запрещенной информации.

Отдельно необходимо обратить внимание на вопросы обеспечения безопасности несовершеннолетних в сети «Интернет». Зачастую использование несовершеннолетним интернет-ресурсов сопряжено с риском взаимодействия с нежелательным контентом [18, с. 102]. Речь идет не только о контенте, который предназначен исключительно для совершеннолетней аудитории, но и о материале, который может привести к самоубийству, совершению террористического акта или иным общественно-опасным последствиям. Данный вопрос уже неоднократно обсуждался среди учеными-юристами. Например, Н.Е. Колобаева говорит о том, что использование сети «Интернет» является одним из условий социализации в современных реалиях [15, с. 15]. Мы разделяем позицию автора, так как, ресурсы сети «Интернет» в современных реалиях используются для расширения кругозора и социального взаимодействия. Проблема здесь заключается в том, что культура пользования информацией у несовершеннолетних находится на низком уровне или вовсе отсутствует, поэтому они не фильтруют потребляемую информацию. М.С. Власенко предлагает «для обеспечения безопасности несовершеннолетних блокировать продвижение на рынок интернет-услуг ресурсов, в которых исключен доступ к нелегальной и вредной информации» [5, с. 100]. Данная точка зрения является несколько спорной, на наш взгляд. Информация, которая противоречит отечественному законодательству, должна априори блокироваться сразу после ее выявления. Выделяя два понятия «нелегальная информация» и «вредная информация», автор фактически разделяет их между собой и исключает возможность их отождествления. Вредоносная информация, скорее всего, подразумевает совокупность данных, в результате ознакомления с которыми психике несовершеннолетнего может быть причинен вред. Оценивая предложение автора с данной точки зрения, можно сделать вывод, что оно противоречит свободе распространения информации, поскольку ограничивает право совершеннолетних граждан на доступ к такому контенту.

Для решения обозначенной проблемы мы видим перспективными следующие способы ее решения. Во-первых, требуется внедрение в школьную программу профильных уроков информационной грамотности. Это может быть отдельный курс, либо часть дисциплины «информатика». В рамках таких курсов необходимо объяснить несовершеннолетним, какие наиболее частые угрозы встречаются в сети «Интернет» и какого алгоритма действий необходимо придерживаться в случае их обнаружения. Вполне возможно провести отдельные занятия в рамках родительских собраний, поскольку на них в большей степени возложена обязанность по контролю за деятельностью несовершеннолетних. Отсутствие достаточной вовлеченности с их стороны благоприятно способствует увеличению влияния вредоносной информации. Большинство современных девайсов имеют механизмы родительского контроля, но, как правило, они просто не используются или со временем легко обходятся.

Помимо уже предложенных рекомендаций, направленных на совершенствование механизмов обеспечения безопасности несовершеннолетних в сети «Интернет», мы видим перспективным внедрение в оборот специальных сим-карт для несовершеннолетних. Доступ в интернет с таких сим-карт будет ограничен в такой степени, чтобы несовершеннолетний не мог попасть на сайты, содержащие вредоносную информацию. Однако, такой способ не сможет ограничить доступ к вредоносной информации, размещенной в разрешенных социальных сетях. К их числу мы можем отнести следующие площадки: Телеграмм, Одноклассники, Вконтакте, Тик-ток. Ранее в Совете Федерации высказывали предложения о запрете на посещение социальных сетей лицами, которые не достигли возраста 14 лет [7]. Мы отрицательно оцениваем такое радикальное предложение, поскольку социальные сети зачастую используются для взаимодействия с родителями и решения организационных вопросов на учебе. В большинстве учебных заведений у каждого класса есть своя беседа в одной из наиболее популярных социальных сетей, где ученики могут взаимодействовать с классным

руководителем и другими преподаватели во внеучебное время. При этом сама идея регистрации при помощи документов видится перспективной. Так, при регистрации профиля в социальной сети ВКонтакте (органы государственной власти наиболее лояльно относятся к данной социальной сети) у пользователя могут потребовать подтверждение личности при помощи документов. Если пользователь отказывается предоставить документы, то его профиль получает ограниченный функционал, в частности, посещать отдельные сообщества, просматривать видео, читать посты, если на них имеется отметка о возрастном ограничении. Такое решение видится нам перспективным при разработке мер обеспечения информационной безопасности несовершеннолетних в сети «Интернет».

Отдельно можно отметить, что в приложении «Вконтакте» для операционной системы IOS изначально недоступны страницы сообществ и страниц пользователей, которые содержат возрастной контент. Кроме того, в этой версии отсутствует возможность отключения безопасного поиска при просмотре видео. С одной стороны данная версия приложения может быть взята за основу при разработке «детской» версии приложения, с другой стороны возникает вопрос о законности таких ограничений с точки зрения отечественного законодательства.

Отдельно стоит обратить внимание на влияние специальных подразделений недружественно настроенных государств. В условиях проведения СВО вредное воздействие от такого информационного влияния. Наиболее активное воздействие в сети «Интернет» оказывает ЦИПсО. Это специализированное подразделение, целью которого является психологическое воздействие для создания паники и волнений среди населения. В результате проведенных информационных атак в южных территориях Российской Федерации фиксировались массовые беспорядки, а также территорию страны покинуло большое число лиц мужского пола. В этой связи важно проводить работу с населением, например, при помощи размещения на официальных ресурсах сводок с правдивой информацией о

происходящих событиях. Кроме того, таким образом можно противодействовать ложной информации, которая набирает популярность в интернете и активно распространяется среди граждан. Это позволит снизить негативное воздействие и стабилизировать сферу информационной безопасности в Российской Федерации.

Завершая обсуждение по теме данной главы, мы можем сделать следующие выводы.

Во-первых, основной закон государства содержит в себе широкий перечень положений, так или иначе, связанных с вопросами обеспечения информационной безопасности в Российской Федерации.

Во-вторых, при буквальном толковании абзаца 4-го статьи 7-ой Закона Российской Федерации «О государственной тайне», можно прийти к выводу, что речь идет только о привилегиях, компенсациях, социальных гарантиях, которые предоставляются органами государственной власти или органами власти субъектов. Таким образом, без внимания остаются льготы, которые предоставляются гражданам за счет средств из бюджета муниципального образования, поскольку муниципальная власть не входит в понятие государственной власти. Для устранения данной неточности в тексте закона, мы предлагаем дополнить абзац 4-ый статьи 7-ой Закона Российской Федерации «О государственной тайне» так, чтобы по смыслу ее новой редакции было очевидно, что запрещается относить к категории государственная тайна льготы, предоставляемые государством и муниципальными образованиями.

В-третьих, в ходе исследования нами было обращено внимание, что упомянутые в Конституции понятия «личная тайна» и «семейная тайна» должны не просто провозглашаться в положениях основного закона, но и в дальнейшем конкретизироваться в положениях других нормативно-правовых актов. Для устранения указанной проблемы мы видим возможным раскрыть основные критерии отнесения информации к категориям личная и семейная тайна. В этом случае станет возможным не просто ссылаться на наличие

такого понятия в законодательстве, а мотивировать то или иное решение о допуске или отказе в допуске к информации, ссылаясь на конкретные критерии. Это позволит решить ряд проблем, в том числе и рассмотренную нами выше, связанную с неправильным толкованием понятий личная тайна и семейная и последующий неправомерный отказ в доступе к информации или, напротив, неправомерный доступ к получению информации.

В-четвертых, мы видим возможным с целью обеспечения целостности организационных основ в сфере обеспечения информационной безопасности включить в список организационных основ Президента Российской Федерации, так как, он обладает широкими полномочиями в регулировании вопросов в сфере информационной безопасности.

В-пятых, отдельно нами было обращено внимание на то, что Доктрина подразумевает взаимодействие между госорганами, объединениями и гражданами. При этом без внимания остаются органы местного самоуправления, которые законодателем включены в список организационных основ. Как уже было отмечено ранее, органы местного самоуправления не могут быть отнесены к государственным органам, поэтому, мы считаем, что следует дополнить рассматриваемый нами принцип и представить его следующим образом: «конструктивное взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности».

В-шестых, мы положительно оцениваем применение морально-этических мер в сфере обеспечения информационной безопасности, поскольку в актуальных условиях особенно важно повысить уровень правовой культуры граждан и закрепить в их сознании установку о губительном влиянии распространения недостоверной информации, а также совершения других правонарушений, которые могут причинить вред и так находящейся под угрозой информационной сфере. Подобные нарушения могут вызвать панику и иные неблагоприятные для общества последствия.

Для обеспечения информационной безопасности несовершеннолетних в сети «Интернет» мы видим перспективными следующие способы ее решения. Во-первых, требуется внедрение в школьную программу профильных уроков информационной грамотности. Это может быть отдельный курс, либо часть дисциплины «информатика». В рамках таких курсов необходимо объяснить несовершеннолетним, какие наиболее частые угрозы встречаются в сети «Интернет» и какого алгоритма действий необходимо придерживаться в случае их обнаружения. Вполне возможно провести отдельные занятия в рамках родительских собраний, поскольку на них в большей степени возложена обязанность по контролю за деятельностью несовершеннолетних. Отсутствие достаточной вовлеченности с их стороны благоприятно способствует увеличению влияния вредоносной информации. Большинство современных девайсов имеют механизмы родительского контроля, но, как правило, они просто не используются или со временем легко обходятся.

Мы предлагаем следующие рекомендации по совершенствованию правового регулирования противодействия распространения экстремистских материалов в сети «Интернет». Во-первых, необходимо более подробно разъяснять объективную сторону преступлений, предусмотренных статьями 280, 280.1, 282 Уголовного кодекса, в том числе разъяснить практику применения данных норм в отношении действий в социальных сетях. Во-вторых, требуется смягчение уголовной ответственности за такие действия, поскольку их общественная опасность несоразмерна назначаемым наказаниям. В-третьих, в первую очередь необходимо привлекать авторов распространяемой информации, которая признана содержащей элементы экстремистских высказываний, а уже только после этого лиц, которые ее распространяют.

Отдельно нами было обращено внимание на влияние специальных подразделений недружественно настроенных государств. В частности в результате проводимых информационных атак в южных территориях Российской Федерации фиксировались массовые беспорядки, а также

территорию страны покинуло большое число лиц мужского пола. В этой связи важно проводить работу с населением, например, при помощи размещения на официальных ресурсах сводок с правдивой информацией о происходящих событиях. Кроме того, таким образом можно противодействовать ложной информации, которая набирает популярность в интернете и активно распространяется среди граждан. Это позволит снизить негативное воздействие и стабилизировать сферу информационной безопасности в Российской Федерации.

Глава 3 Проблемы правового регулирования противодействия информационным правонарушениям в Российской Федерации

Сфере информационной безопасности характерен ряд проблемных аспектов, которые создают угрозу личности, обществу и государству. В данной главе мы рассмотрим актуальные проблемы обеспечения информационной безопасности.

«Как показала практика работы правоохранительных органов, использование на предприятиях специальных технических средств, предназначенных для негласного получения информации создает угрозу информационной безопасности, эффективная нейтрализация которой, требует оперативного применения уголовно-правовых мер» [24, с. 54]. Оперативность обнаружения соответствующий правонарушений осложнена следующими факторами. Указанные правонарушения в основном содержат в себе признаки уголовных правонарушений, предусмотренных статьями 138 и 138.1 Уголовного кодекса. Такие правонарушения, по смыслу уголовно-процессуального закона, находятся в подведомственности Следственного комитета Российской Федерации [35]. При этом альтернативная подследственность в данном случае отсутствует, исключая возможность привлечения ресурса следственных подразделений правоохранительных органов для обеспечения информационной безопасности. В свою очередь это снижает эффективность противодействия в целом. В связи с этим, для повышения оперативности расследования выявленных эпизодов использования на предприятиях специальных технических средств, предназначенных для негласного получения информации мы предлагаем внести статьи 138 и 138.1 Уголовного кодекса в часть пятую статьи 151 Уголовно-процессуального кодекса, обеспечив возможность проводить расследование по указанным преступлениям органам, которые выявили это преступление.

Г.И. Шархворостов обращает внимание на следующую проблему, которая препятствует нормальному обеспечению информационной безопасности. «В настоящее время на недостаточном уровне определены основные интересы Российской Федерации и ее субъектов в информационной сфере по предметам совместного ведения, а также интересы субъектов Федерации по предметам их исключительного ведения, наиболее опасные угрозы этим интересам, направления и механизмы участия органов федеральной системы обеспечения информационной безопасности, органов государственной власти субъектов Российской Федерации, государственных, общественных и иных организаций и граждан, проживающих на территории субъекта Российской Федерации, в реализации мероприятий по противодействию этим угрозам, а также порядок координации данной деятельности. Основная сложность определения и разграничения интересов страны и регионов обусловлена неформальным характером задачи выделения среди множества жизненно важных целей развития регионов таких, достижение которых в существенной степени зависит от информационной сферы и защита которых составляет предмет региональной информационной безопасности» [46, с. 30]. Для решения заявленной проблемы важно руководствоваться интересами, которые основным законом определяются в качестве предмета совместного ведения. После чего необходимо выявить направления, которые прямо или косвенно затрагивают вопроса обеспечения информационной безопасности. Касательно же региональной политики в данной сфере, требуется руководствоваться теми полномочиями, которые признаются исключительными полномочиями субъекта. К их числу мы можем отнести: распространение информации на территории региона, взаимодействие с информационными ресурсами, которые осуществляют свою деятельность на территории субъекта, формирование и развитие информационной структуры внутри региона.

Другой не менее важной проблемой является рост числа правонарушений, посягающих на безопасность персональных данных граждан

[9, с. 272]. За последние несколько лет произошел ряд крупных утечек персональных данных граждан. Так, в 2022 году данные сервисов СДЭК и ДНС попали в сеть и стали общедоступными [4]. Стоит добавить, что на практике имеют место быть случаи, когда сотрудники государственных учреждений передают персональные данные третьим лицам. Так, практика знает случаи, когда после регистрации коммерческого юридического лица или статуса индивидуального предпринимателя гражданину практически сразу начинают поступать звонки от банков с предложениями открыть счет или приобрести иные услуги. Это указывает на то, что отдельные сотрудники налоговых органов недобросовестно исполняют свои обязанности. На ненадлежащую охрану персональных данных указывает и то обстоятельство, что любой желающий при помощи аккаунта в телеграмме и небольшой оплаты может получить общую информацию практически о каждом гражданине. Как правило, в такую информационную справку входят: фамилия, имя, отчество, номер телефона, наличие банковских карт. Чуть реже можно встретить информацию о номерах автомобилей, адресах проживания, номер и серия паспорта и так далее. Хотя отечественное законодательство содержит нормы, которые закрепляют ответственность за нарушения в сфере охраны персональных данных, как правило, к ответственности виновные привлекаются только в случае крупных и резонансных утечек данных. Объяснить данное обстоятельство мы можем тем, что в Российской Федерации уровень правовой и информационной культуры находится на относительно низком уровне. В случае обнаружения утечки своих или чьих-либо данных, гражданин с минимальной вероятностью обращаются в правоохранительные органы или к администратору ресурса с требованием удалить информацию с персональными данными. Для улучшения ситуации в данной сфере требуется проведение мероприятий, которые направлены на формирование у населения понимания важности сохранности персональных данных, угрозе их распространения, а также алгоритме действий при обнаружении таких утечек.

Рассматривая проблемные аспекты обеспечения информационной безопасности, необходимо уделить внимание вопросам ответственности за совершение правонарушений, посягающих на объекты охраны информационной безопасности.

Уголовный кодекс содержит ряд составов преступлений, которые посягают на информационную безопасность. Одним из таких преступлений является разглашение тайны усыновления (удочерения). Среди ученых ведутся споры относительно целесообразности уголовной ответственности за данное деяние. Свою позицию представители данной точки зрения мотивируют тем, что «данная норма является своего рода пережитком прошлого, не соответствует мировой практике и уголовная ответственность за разглашение тайны усыновления должна подлежать отмене, факт усыновления рано или поздно станет известным усыновленному, поэтому в принципе не может не причинить ему психологической травмы» [17, с. 819]. Мы не можем согласиться с позицией автора, поскольку, на наш взгляд, разглашение информации об усыновлении может повлиять на психологическое развитие несовершеннолетнего или вовсе нанести травму его психике. В связи с этим криминализация данного деяния абсолютно оправдана.

Анализируя положения статьи 155 Уголовного кодекса, можно отметить, что она состоит из одной части, то есть, в ней отсутствуют квалифицирующие составы. Субъектом преступления выступает лицо, на которое возложена обязанность хранить тайну усыновления (удочерения), а также иные лица, если тайна разглашается по мотивам корысти или иных низменных побуждений. Законодатель одинаково оценивает степень общественной опасности названных субъектов, хотя очевидно, что лицо, нарушающее служебную или профессиональную тайну, совершает более общественно-опасное деяние. Поэтому мы рекомендуем изменить статью 155 Уголовного кодекса, в частности разделить ее на общий состав и квалифицированный. Часть первая будет содержать общий состав

преступления и закреплять уголовную ответственность за разглашение тайны усыновления (удочерения) для лиц, которые узнали информацию не в силу профессиональной или служебной деятельности. При этом мы рекомендуем исключить специальные признаки субъективной стороны – корыстный мотив или иные низменные побуждения. Во второй части мы рекомендуем включить квалифицирующий состав преступления. Квалифицирующим признаком в данном случае будет профессиональная или служебная обязанность хранить тайну усыновления (удочерения). Это позволит дифференцировать уголовную ответственность в зависимости от степени общественной опасности деяния.

Аналогичные споры возникают относительно содержания в тексте уголовного закона статьи 140, в которой закрепляется ответственность за неправомерный отказ в получении информации. Выступая за исключение указанной статьи, М.Г. Адыханов аргументирует свою позицию тем, что «с момента принятия УК РФ общее количество зарегистрированных преступлений по статье 140 УК РФ не превысило и десяти эпизодов, в определенном смысле, это позволяет утверждать, что в современных условиях уголовно-правовая норма, предусмотренная статьей 140 УК РФ, может быть причислена к категории так называемого символического уголовного законодательства и не имеет практической ценности» [1, с. 140]. Само по себе отсутствие правоприменительной практики по данной статье не указывает на необходимость ее упразднения, скорее речь идет о проблемах квалификации и применения при такой форме изложения. Так, стоит принимать во внимание, что состав данного преступления является материальным, то есть, преступление считается оконченным с момента, когда деяния должностного лица приводят к нарушению прав и законных интересов гражданина. При этом важно понимать, что сам по себе неправомерный отказ в информации уже является нарушением прав и законных интересов. То есть, по смыслу самой нормы, преступление окончено с момента его совершения. Ситуация осложняется тем, что Кодекс об административных правонарушениях содержит идентичный состав. Отличие заключается в том, что

административное правонарушение не требует наступления каких-либо последствий в виде нарушений прав и законных интересов [14]. Таким образом, у нас имеется два идентичных состава, которые создают конкуренцию норм административного и уголовного права. В этих условиях правоприменитель, как правило, принимает решение в пользу административного правонарушения. Для решения обозначенной проблемы мы видим возможным расширить диспозицию статьи 140 Уголовного кодекса, путем перечисления конкретизирующих признаков преступного результата преступного деяния.

Отдельно авторами обращается внимание на следующие аспект, препятствующий привлечению к ответственности лиц, совершивших информационное правонарушение. «Неопределенность местоположения участников взаимодействия в интернете, то есть, физически лица могут находиться в неопределенном месте, государстве, может привести к коллизиям норм. Другая сложность может быть связана с возможностью определения сторон, то есть, лицо, совершающее административное правонарушение, может быть анонимным и определить его невозможно» [3, с. 182]. Определенно, заявленная проблема характерна для отечественного законодательства. Например, имеются трудности в процессе привлечения к ответственности лица, распространяющего высказывания дискриминирующие по национальному признаку в социальных сетях, если сам нарушитель имеет гражданство другой страны и проживает на территории другого государства. Даже в том случае, если получится идентифицировать личность правонарушителя, то фактически привлечь его к ответственности практически не представляется возможным. Единственное реальное лишение, которому можно подвергнуть нарушителя, заблокировать его профиль на сайте, где такая вредоносная информация была размещена, однако, это не помешает ему зарегистрировать новый профиль и продолжать совершать информационные правонарушения.

Отдельно среди исследователей критике подвергается эффективность в сфере обеспечения информационной безопасности норма, которая предусматривает ответственность за злоупотребление свободой массовой информации (13.15 КоАП). Анализ указанной нормы позволяет нам сделать вывод, что злоупотребление свободой массовой информации может выражаться в совершении различных деяний. То есть, законодатель весьма подробно проработал диспозицию данной статьи. Указанную норму можно рассматривать в качестве инструмента, который законодатель использовал, для ликвидации пробелов в нормативно правовой базе в сфере ответственности за информационные правонарушения. По сути, законодатель может дополнять ее другими деяниями, которые будут рассматриваться в качестве злоупотребления свободой массовой информации. Более того, актуальность данной нормы, на наш взгляд, вызвана многочисленными угрозами для сферы информационной безопасности в нынешней политической ситуации. Очевидным является тот факт, что столь широкое скопление различных составов правонарушений в рамках одной статьи создает определенные трудности при разграничении составов административных правонарушений между собой. Однако нельзя отрицать, что при помощи указанной нормы возможно привлечь к ответственности юридическое лицо за правонарушения, которые в силу специфики уголовного законодательства не могут быть им инкриминированы. Поэтому мы не разделяем позицию автора, что наличие указанной нормы не имеет практической ценности.

В завершении данной главы считаем необходимым сделать следующие выводы.

Во-первых, для повышения оперативности расследования выявленных эпизодов использования на предприятиях специальных технических средств, предназначенных для негласного получения информации мы предлагаем внести статьи 138 и 138.1 Уголовного кодекса в часть пятую статьи 151 Уголовно-процессуального кодекса, обеспечив возможность проводить

расследование по указанным преступлениям органам, которые выявили это преступление.

Во-вторых, для решения вопроса о совместной и исключительной компетенции органов власти субъекта в сфере информационной безопасности важно руководствоваться интересами, которые основным законом определяются в качестве предмета совместного ведения. После чего необходимо выявить направления, которые прямо или косвенно затрагивают вопроса обеспечения информационной безопасности. Касательно же региональной политики в данной сфере, требуется руководствоваться теми полномочиями, которые признаются исключительными полномочиями субъекта. К их числу мы можем отнести: распространение информации на территории региона, взаимодействие с информационными ресурсами, которые осуществляют свою деятельность на территории субъекта, формирование и развитие информационной структуры внутри региона.

В-третьих, для улучшения ситуации в сфере охраны персональных данных, на наш взгляд, требуется проведение мероприятий, которые направлены на формирование у населения понимания важности сохранности персональных данных, угрозе их распространения, а также алгоритме действий при обнаружении таких утечек.

В-четвертых, мы рекомендуем изменить статью 155 Уголовного кодекса, в частности разделить ее на общий состав и квалифицированный. Часть первая будет содержать общий состав преступления и закреплять уголовную ответственность за разглашение тайны усыновления (удочерения) для лиц, которые узнали информацию не в силу профессиональной или служебной деятельности. При этом мы рекомендуем исключить специальные признаки субъективной стороны – корыстный мотив или иные низменные побуждения. Во второй части мы рекомендуем включить квалифицирующий состав преступления. Квалифицирующим признаком в данном случае будет профессиональная или служебная обязанность хранить тайну усыновления

(удочерения). Это позволит дифференцировать уголовную ответственность в зависимости от степени общественной опасности деяния.

В-пятых, состав преступления, предусмотренного статьей 140 Уголовного кодекса, является материальным, то есть, преступление считается оконченным с момента, когда деяния должностного лица приводят к нарушению прав и законных интересов гражданина. При этом важно понимать, что сам по себе неправомерный отказ в информации уже является нарушением прав и законных интересов. То есть, по смыслу самой нормы, преступление окончено с момента его совершения. Ситуация осложняется тем, что Кодекс об административных правонарушениях содержит идентичный состав. Отличие заключается в том, что административное правонарушение не требует наступления каких-либо последствий в виде нарушений прав и законных интересов. Таким образом, у нас имеется два идентичных состава, которые создают конкуренцию норм административного и уголовного права. В этих условиях правоприменитель, как правило, принимает решение в пользу административного правонарушения. Для решения обозначенной проблемы мы видим возможным расширить диспозицию статьи 140 Уголовного кодекса, путем перечисления конкретизирующих признаков преступного результата преступного деяния.

Заключение

Информационная безопасность рассматривается как «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». Легальное определение, на наш взгляд, содержит в себе все основополагающие признаки, поэтому не требует каких-либо существенных корректировок. Нами было отмечено, что информационная безопасность может рассматриваться в двух ипостасях. С одной стороны, информационная безопасность направлена на обеспечение сохранности информации от противоправного завладения, использования, распространения, если законом предусмотрена ее охрана. Примером таких сведений является государственная тайна, тайна усыновления, тайна частной жизни и так далее. С другой стороны, информационная безопасность подразумевает защиту населения от информации, которая может причинить вред человеку, обществу и государству. Говоря о вредоносной информации, имеются в виду сведения, которые потенциально могут нести опасность субъектам защиты информационной безопасности.

В ходе анализа элементов правового регулирования информационной безопасности нами было обращено внимание на следующие обстоятельства.

Во-первых, при буквальном толковании абзаца 4-го статьи 7-ой Закона Российской Федерации «О государственной тайне», можно прийти к выводу, что речь идет только о привилегиях, компенсациях, социальных гарантиях, которые предоставляются органами государственной власти или органами власти субъектов. Таким образом, без внимания остаются льготы, которые предоставляются гражданам за счет средств из бюджета муниципального образования, поскольку муниципальная власть не входит в понятие

государственной власти. Для устранения данной неточности в тексте закона, мы предлагаем дополнить абзац 4-ый статьи 7-ой Закона Российской Федерации «О государственной тайне» так, чтобы по смыслу ее новой редакции было очевидно, что запрещается относить к категории государственная тайна льготы, предоставляемые государством и муниципальными образованиями.

Во-вторых, в ходе исследования нами было обращено внимание, что упомянутые в Конституции понятия «личная тайна» и «семейная тайна» должны не просто провозглашаться в положениях основного закона, но и в дальнейшем конкретизироваться в положениях других нормативно-правовых актов. Для устранения указанной проблемы мы видим возможным раскрыть основные критерии отнесения информации к категориям личная и семейная тайна. В этом случае станет возможным не просто ссылаться на наличие такого понятия в законодательстве, а мотивировать то или иное решение о допуске или отказе в допуске к информации, ссылаясь на конкретные критерии. Это позволит решить ряд проблем, в том числе и рассмотренную нами выше, связанную с неправильным толкованием понятий личная тайна и семейная и последующий неправомерный отказ в доступе к информации или, напротив, неправомерный доступ к получению информации.

В-третьих, отдельно нами было обращено внимание на то, что Доктрина подразумевает взаимодействие между госорганами, объединениями и гражданами. При этом без внимания остаются органы местного самоуправления, которые законодателем включены в список организационных основ. Как уже было отмечено ранее, органы местного самоуправления не могут быть отнесены к государственным органам, поэтому, мы считаем, что следует дополнить рассматриваемый нами принцип и представить его следующим образом: «конструктивное взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности».

В-четвертых, мы положительно оцениваем применение морально-этических мер в сфере обеспечения информационной безопасности, поскольку в актуальных условиях особенно важно повысить уровень правовой культуры граждан и закрепить в их сознании установку о губительном влиянии распространения недостоверной информации, а также совершения других правонарушений, которые могут причинить вред и так находящейся под угрозой информационной сфере. Подобные нарушения могут вызвать панику и иные неблагоприятные для общества последствия.

Для обеспечения информационной безопасности несовершеннолетних в сети «Интернет» мы видим перспективными следующие способы ее решения. Во-первых, требуется внедрение в школьную программу профильных уроков информационной грамотности. Это может быть отдельный курс, либо часть дисциплины «информатика». В рамках таких курсов необходимо объяснить несовершеннолетним, какие наиболее частые угрозы встречаются в сети «Интернет» и какого алгоритма действий необходимо придерживаться в случае их обнаружения. Вполне возможно провести отдельные занятия в рамках родительских собраний, поскольку на них в большей степени возложена обязанность по контролю за деятельностью несовершеннолетних. Отсутствие достаточной вовлеченности с их стороны благоприятно способствует увеличению влияния вредоносной информации. Большинство современных девайсов имеют механизмы родительского контроля, но, как правило, они просто не используются или со временем легко обходятся.

Мы предлагаем следующие рекомендации по совершенствованию правового регулирования противодействия распространения экстремистских материалов в сети «Интернет». Во-первых, необходимо более подробно разъяснять объективную сторону преступлений, предусмотренных статьями 280, 280.1, 282 Уголовного кодекса, в том числе разъяснить практику применения данных норм в отношении действий в социальных сетях. Во-вторых, требуется смягчение уголовной ответственности за такие действия, поскольку их общественная опасность несоразмерна назначаемым

наказаниям. В-третьих, в первую очередь необходимо привлекать авторов распространяемой информации, которая признана содержащей элементы экстремистских высказываний, а уже только после этого лиц, которые ее распространяют.

В ходе анализа проблемных аспектов обеспечения информационной безопасности, нами были сделаны следующие выводы.

Во-первых, для улучшения ситуации в сфере охраны персональных данных, на наш взгляд, требуется проведение мероприятий, которые направлены на формирование у населения понимания важности сохранности персональных данных, угрозе их распространения, а также алгоритме действий при обнаружении таких утечек.

Во-вторых, мы рекомендуем изменить статью 155 Уголовного кодекса, в частности разделить ее на общий состав и квалифицированный. Часть первая будет содержать общий состав преступления и закреплять уголовную ответственность за разглашение тайны усыновления (удочерения) для лиц, которые узнали информацию не в силу профессиональной или служебной деятельности. При этом мы рекомендуем исключить специальные признаки субъективной стороны – корыстный мотив или иные низменные побуждения. Во второй части мы рекомендуем включить квалифицирующий состав преступления. Квалифицирующим признаком в данном случае будет профессиональная или служебная обязанность хранить тайну усыновления (удочерения). Это позволит дифференцировать уголовную ответственность в зависимости от степени общественной опасности деяния.

В-третьих, состав преступления, предусмотренного статьей 140 Уголовного кодекса, является материальным, то есть, преступление считается оконченным с момента, когда деяния должностного лица приводят к нарушению прав и законных интересов гражданина. При этом важно понимать, что сам по себе неправомерный отказ в информации уже является нарушением прав и законных интересов. То есть, по смыслу самой нормы, преступление окончено с момента его совершения. Ситуация осложняется

тем, что Кодекс об административных правонарушениях содержит идентичный состав. Отличие заключается в том, что административное правонарушение не требует наступления каких-либо последствий в виде нарушений прав и законных интересов. Таким образом, у нас имеется два идентичных состава, которые создают конкуренцию норм административного и уголовного права. В этих условиях правоприменитель, как правило, принимает решение в пользу административного правонарушения. Для решения обозначенной проблемы мы видим возможным расширить диспозицию статьи 140 Уголовного кодекса, путем перечисления конкретизирующих признаков преступного результата преступного деяния.

Список используемой литературы и используемых источников

1. Адылханов М.Г. Уголовная ответственность за отказ в предоставлении гражданину информации: проблемные вопросы квалификации и законодательного определения // Гуманитарные, социально-экономические и общественные науки. 2019. №11. С. 139-144.

2. Баринов С.В. О правовом определении понятия «Информационная безопасность личности» // Актуальные проблемы российского права. 2016. №4 (65). С. 97-105.

3. Безручко Е.В., Рысай Б.Г. Некоторые проблемы административной ответственности в сфере связи и информации // ЮП. 2020. №1(92). С. 180-185.

4. В компании DNS была обнаружена утечка персональных данных клиентов и сотрудников // [Электронный ресурс]. - https://www.dns-shop.ru/news/a67100f1-4205-11ed-902a-00155d8ed20c/ (дата обращения 01.05.2023)

5. Власенко М.С. Обеспечение информационной безопасности несовершеннолетних в сети Интернет: современное состояние и совершенствование правового регулирования // Вестник ВУиТ. 2019. №3. С. 98-105.

6. Гражданский кодекс Российской Федерации (часть третья) от 26.11.2001 №146-ФЗ (ред. от 01.07.2021) // СЗ РФ. 2001. №49. Ст. 4552.

7. Детей до 14 лет предложили не пускать в соцсети // [Электронный ресурс]. - https://www.pnp.ru/politics/detey-do-14-let-predlozhili-ne-puskat-v-socseti.html (дата обращения 01.05.2023)

8. Дзанагова М.К., Бетеева М.М. Информационная безопасность детей: понятие и принципы // Право и государство: теория и практика. 2020. №3(183). С. 273-274.

9. Жуйков А.А. Современные проблемы информационной безопасности // Вестник КРУ МВД России. 2015. №4 (30). С. 270-273.

10. Закон РФ «О государственной тайне» от 21.07.1993 №5485-1 (ред. от 04.08.2022) // РГ. 1993. №182.

11. Закон РФ «О средствах массовой информации» от 27.12.1991 №2124-1 (ред. от 14.07.2022) // РГ. 1992. №32.

12. Ибрагимова А.Н. Понятие персональных данных; информационная безопасность права на неприкосновенность частной жизни согласно анализу статьи 8 Европейской конвенции по правам человека // Северо-Кавказский юридический вестник. 2021. №4. С. 92-103.

13. Истории россиян, осужденных за лайки // [Электронный ресурс]. - https://lenta.ru/articles/2018/07/24/likeshare/ (дата обращения 01.05.2023)

14. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 №195-ФЗ (ред. от 24.09.2022) // СЗ РФ. 2002. №1. Ст. 1.

15. Колобаева Н.Е., Несмеянова С.Э. Информационная безопасность несовершеннолетних и право на доступ в интернет // Электронное приложение к Российскому юридическому журналу. 2020. №6. С. 14-21.

16. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ, от 14.07.2020 № 1-ФКЗ) // РГ. 1993. №237.

17. Корнакова С.В., Чигрина Е.В. Разглашение тайны усыновления: проблемы реализации комплексного правового механизма в Российской Федерации // Всероссийский криминологический журнал. 2018. №6. С. 817-825.

18. Кубякин Е.О., Сафронов А.Н. Информационный экстремизм в среде молодежи как деструктивный феномен современного российского общества // Вестник КРУ МВД России. 2013. №4 (22). С. 100-104.

19. Мазуров В.А., Невинский В.В. Понятие и принципы информационной безопасности // Известия АлтГУ. 2003. №2. С. 57-63.

20. Мамедова К.А. Основные принципы обеспечения информационной безопасности страны // Информационная безопасность регионов. 2016. №1(22). С. 16-20.

21. Манжуева О.М., Костылева О.П. Краткий анализ основных мер обеспечения информационной безопасности // Евразийский Союз Ученых. 2018. №6(51). С. 45-48.

22. Михайлова Л.С. Конституционно-правовые основы обеспечения информационной безопасности в России // Информационная безопасность регионов. 2014. №2(15). С. 17-22.

23. Мошенничество в сети: судебная практика и ключевые аспекты // [Электронный ресурс]. - https://rtmtech.ru (дата обращения 14.12.2022)

24. Озимко К.Д. Современные проблемы обеспечения информационной безопасности в Российской Федерации // Отечественная юриспруденция. 2016. №11(13). С. 53-55.

25. Олейникова П.А. Уголовная ответственность за лайки и репосты – проблемы квалификации и наказание за содеянное // E-Scio. 2020. №7 (46). С. 90-100.

26. Определение Конституционного Суда РФ от 09.06.2005 №248-О «Об отказе в принятии к рассмотрению жалобы граждан Захаркина Валерия Алексеевича и Захаркиной Ирины Николаевны на нарушение их конституционных прав пунктом «б» части третьей статьи 125 и частью третьей статьи 127 Уголовно-исполнительного кодекса Российской Федерации» // Консультант плюс: справочно-правовая система.

27. Павкина Л.Г., Крашенинникова А.В., Прокин А.А. Обеспечение информационной безопасности: содержание и структура понятия // E-Scio. 2021. №3 (54). С. 260-266.

28. Привалов С.А. Запрет цензуры как гарантия свободы массовой информации в России и Германии // Вестник ПАГС. 2021. №3. С. 13-20.

29. Савкина Т.Б., Царенко Л.С., Борисенко К.С. Этапы и методы вербовки в террористические организации // Научные исследования и инновации. 2021. №9. С. 388-396.

30. Саликов М.С., Несмеянова С.Э. К постановке проблемы об особенностях реализации и защиты прав и свобод человека в сети Интернет // Российское право: образование, практика, наука. 2019. №1(109). С. 5-13.

31. Слесарев Ю.В., Лосяков А.В. Проблемы защиты конфиденциальной информации в сети интернет: правовой аспект // БГЖ. 2018. №1(22). С. 383-385.

32. Семейный кодекс Российской Федерации от 29.12.1995 №223-ФЗ (ред. от 04.08.2022) // СЗ РФ. 1996. №1. Ст. 16.

33. Терещенко Л.К. Тенденции установления административной ответственности в информационной сфере // Журнал российского права. 2017. №10(250). С. 61-71.

34. Тершуков Д.А. Анализ современных угроз информационной безопасности // NBI-technologies. 2018. №3. С. 6-12.

35. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 №174-ФЗ (ред. от 24.09.2022) // СЗ РФ. 2001. №52. Ст. 4921.

36. Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. от 14.07.2022) // СЗ РФ. 1996. №25. Ст. 2954.

37. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Консультант плюс: справочно-правовая система.

38. Указ Президента РФ от 17.03.2008. № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // СЗ РФ. 2008. №12. Ст. 1110.

39. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и

информационнотелекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационнотелекоммуникационной сети «Интернет») // СЗ РФ. 2015. № 21. Ст. 3092.

40. Указ Президента РФ от 02.07.2021 №400 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2021. №27. Ст. 5351.

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

42. Федеральный закон «Об архивном деле в Российской Федерации» от 22.10.2004 №125-ФЗ (ред. от 11.06.2021) // СЗ РФ. 2004. №43. Ст. 4169.

43. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 №187-ФЗ // СЗ РФ. 2016. №50. Ст. 7074.

44. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2006. №31. Ст. 3448.

45. Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации» от 21.11.2011 №323-ФЗ (ред. от 11.06.2022, с изм. от 13.07.2022) // СЗ РФ. 2011. №48. Ст. 6724.

46. Шахворостов Г. И., Кустов А. И., Самсонов В. С., Жданов М. А. Актуальные направления совершенствования административного управления системой обеспечения информационной безопасности субъекта Российской Федерации: проблемы и предложения // РСЭУ. 2022. №1 (56). С. 28-35.

47. Швыряев П.С. Киберпреступность в России: новый вызов для общества и государства // Государственное управление. Электронный вестник. 2021. №89. С. 184-196.

48. Шогенов Т.М. О некоторых вопросах распространения экстремистских материалов с использованием сети Интернет // Общество: политика, экономика, право. 2016. №5. С. 160-162.

49. Шубина О.А. Особенности системы правового обеспечения информационной безопасности // Система ценностей современного общества. 2010. №13. С. 113-116.

50. Global Digital 2022 ежегодный отчет об интернете и социальных сетях // [Электронный ресурс]. - https://www.sostav.ru (дата обращения 01.05.2023)