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 Проблемы правового регулирования информационной безопасности

Обучающийся А.С. Ячменцева _____
(Инициалы Фамилия) (личная подпись)

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

Тольятти 2022

Аннотация

Актуальность темы выпускной работы заключается в том, что для правового регулирования информационной безопасности в Российской Федерации характерен ряд проблемных аспектов. К их числу мы можем отнести, например, отсутствие законодательного закрепления понятий личная и семейная тайна. Указанное обстоятельство повышает значение субъективного фактора в процессе их толкования уполномоченными лицами, что существенно влияет на единообразие правоприменительной практики, а также может стать причиной неправомерного отказа в доступе к информации.

Объект работы – общественные отношения, возникающие в процессе осуществления правового регулирования информационной безопасности.

Предмет работы – правовые нормы, материалы научных работ и судебной практики, при помощи которых возможно детально изучить вопросы правового регулирования информационной безопасности, а также выявить актуальные для него проблемные аспекты.

Цель работы – проведение комплексного исследования вопросов правового регулирования информационной безопасности, а также выявление актуальных для него проблемных аспектов и подготовка рекомендаций для их решения.

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

Объем работы составляет 73 страницы.

Оглавление

Введение

В современных условиях жизни и развития общества информация является ценным ресурсом, а также, в некотором роде, инструментом регулирования общественного поведения. Определенная информация требует особой защиты, поскольку представляет собой сугубо личные или государственно важные сведения, а другая информация может нести угрозу для общества. Этим обусловлено государственное вмешательство в процесс размещения, распространения, получения и защиты информации, а также внедрение в отечественную нормативно-правовую базу понятия «информационная безопасность».

Актуальность темы выпускной работы заключается в том, что для правого регулирования информационной безопасности в Российской Федерации характерен ряд проблемных аспектов. К их числу мы можем отнести, например, отсутствие законодательного закрепления понятий личная и семейная тайна. Указанное обстоятельство повышает значение субъективного фактора в процессе их толкования уполномоченными лицами, что существенно влияет на единообразие правоприменительной практики, а также может стать причиной неправомерного отказа в доступе к информации.

Рассмотрение правовой политики в сфере информационной безопасности непосредственно связано с регулированием правоотношений в сети «Интернет». На сегодняшний день интернет плотно вошел в жизнь практически каждого жителя нашей страны. С его помощью люди поддерживают связь, проводят досуг, работают и получают информацию. По данным исследования, которое ежегодно проводит Global Digital, в среднем в интернете человек проводит около семи часов. Учитывая, что восемь часов необходимо для сна, выходит, что половину своего свободного времени человек проводит в интернете. Подобный масштаб свидетельствует о том, что вопросам обеспечения информационной безопасности в сети «Интернет» необходимо уделять особое внимание.

Объект работы – общественные отношения, возникающие в процессе осуществления правового регулирования информационной безопасности.

Предмет работы – правовые нормы, материалы научных работ и судебной практики, при помощи которых возможно детально изучить вопросы правового регулирования информационной безопасности, а также выявить актуальные для него проблемные аспекты.

Цель работы – проведение комплексного исследования вопросов правового регулирования информационной безопасности, а также выявление актуальных для него проблемных аспектов и подготовка рекомендаций для их решения.

Обозначив цель, мы можем выделить следующие задачи, необходимые для ее достижения:

- проанализировать понятие, признаки и принципы информационной безопасности;
- рассмотреть виды правонарушений в сфере информационной безопасности;
- определить конституционно-правовые основы регулирования информационной безопасности;
- рассмотреть организационные основы регулирования информационной безопасности;
- ознакомиться с особенностями правового регулирования информационной безопасности в сети «Интернет»;
- выявить проблемы правового регулирования информационной безопасности в Российской Федерации и предложить рекомендации для их решения.

В основу исследования были положены работы следующих ученых: М.Г. Адылханова, А.В. Александровой, М.З. Али, Я.С. Артамоновой, С.В. Баринова, И.П. Батаевой, Е.В. Безручко, А.В. Бецкова, А.А. Васютина, Т.А. Вепренцевой, М.С. Власенко, А.А. Гребенькова, М.К. Дзанаговой, Т.И. Ежевской, М.А. Ефремовой, С.Н. Клименко, Н.Е. Колобаевой, Ю.Е.

Кулавской, В.А. Мазурова, К.А. Мамедовой, О.М. Манжуевой, Л.С. Михайловой, К.Д. Озимко, А.В. Савоськина, М.С. Саликова, Ю.В. Слесарева, Г.В. Синцова, Л.К. Терещенко, Ш.Г. Утарбекова, В.М. Филиппова, Г.И. Шахворостов, А.А. Ширкина, Т.М. Шогенова, О.А. Шубиной, М.З. Юсуповой.

В ходе проведенного исследования были исследованы следующие нормативно-правовые акты: Конституция РФ, Гражданский кодекс РФ (часть первая), Гражданский кодекс РФ (часть третья), Закон РФ «О государственной тайне», Закон РФ «О средствах массовой информации», Кодекс административного судопроизводства РФ, Кодекс Российской Федерации об административных правонарушениях, Семейный кодекс РФ, Трудовой кодекс РФ, Уголовный кодекс РФ, Уголовно-процессуальный кодекс РФ, Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «Об оперативно-розыскной деятельности», Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон «О государственной гражданской службе Российской Федерации», Федеральный закон «О коммерческой тайне», Федеральный закон «О противодействии экстремистской деятельности», 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 информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет»), Указ Президента РФ «О Стратегии национальной 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.

Объем работы составляет 73 страницы.

Глава 1 Информационная безопасность как элемент системы национальной безопасности Российской Федерации

1.1 Понятие, признаки и принципы информационной безопасности

В современных условиях жизни и развития общества информация является ценным ресурсом, а также, в некотором роде, инструментом регулирования общественного поведения. Определенная информация требует особой защиты, поскольку представляет собой сугубо личные или государственно важные сведения, а другая информация может нести угрозу для общества. Этим обусловлено государственное вмешательство в процесс размещения, распространения, получения и защиты информации, а также внедрение в отечественную нормативно-правовую базу понятия «информационная безопасность». Данное определение занимает центральное место в Доктрине информационной безопасности Российской Федерации. В ней 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» [41].

Рассматривая определение понятия «информационная безопасность» можно отметить, что оно схоже со своим родовым понятием «национальная безопасность». Дело в том, что национальная безопасность является объемной системой, которая ориентируется на защиту широкого перечня общественных отношений. Информационная безопасность входит в структуру национальной безопасности, ввиду этого мы можем наблюдать в Стратегии национальной безопасности практически идентичное определение последней: «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» [44]. Весьма очевидным является тот факт, что именно определение национальной безопасности легло в основу определения информационной безопасности. При этом не совсем понятно, почему законодатель не включил в определение отдельные признаки информационной безопасности, а руководствовался лишь спецификой регулируемых отношений. Для наиболее полного понимания сущности категории информационная безопасность, считаем необходимым, рассмотреть материалы периодической печати, содержащие исследования по данному вопросу.

А.В. Бецков употребляет категорию «информационная безопасность» как «как состояние защищенности основных сфер жизнедеятельности по отношению к опасным информационным воздействиям» [8, с. 42]. На наш взгляд, представленное определение не отражает всей полноты признаков рассматриваемой категории. Основной аспект здесь уделяется защите общественных отношений, в то время как законодатель говорит о защите личности, общества и государства. Такой подход объясняется тем, что Конституция провозглашает принцип гуманизма. Кроме того, защита должна быть направлена не на абстрактные общественные отношения, а на интересы конкретных субъектов.

О.А. Шубина предлагает следующее определение. «Информационная безопасность – это получение максимальной информации о намерениях и потенциальных действиях своих оппонентов и минимальная утечка информации о своих планах» [58, с. 114]. Оценивая данное определение, стоит отметить, что оно весьма узконаправленное. То есть, оно рассматривает информационной безопасности в контексте бизнеса или информационного противостояния.

Я.С. Артомонова рассматривает информационную безопасность как «защищенность 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» [4, с. 320]. В этом варианте определения автор подробно раскрывает социальные группы, для которых обеспечивается информационная безопасность. Определение раскрывается через категорию «потребность», что имеет место быть, поскольку в современном мире, где число источников информационного поля чрезмерно велико, объективно растет потребность в получении качественной информации. Здесь же стоит обратить внимание, что автор нивелирует потребность государства в качественной информации. Поэтому автору следовало бы акцентировать внимание не только на соответствующую потребность не только отдельных граждан, их объединений, но и непосредственно государства в лице его органов и должностных лиц.

В свою очередь при определении информационной безопасности В.А. Мазуров на первый план ставит именно защиту информации, которая является основным элементом информационной безопасности. Автор предлагает рассматривать информационную безопасность следующим образом. «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» [26, с. 59]. В этом определении особое внимание уделяется мерам обеспечения информационной безопасности, причем акцентируя внимание именно на технических средствах. Такой подход вполне понятен, поскольку именно при помощи технических средств реализуется практическая составляющая обеспечения информационной безопасности. При этом необходимо понимать, что наше исследование осуществляется с точки зрения юриспруденции, поэтому технический аспект нас интересует в меньшей степени.

В целом можно сделать вывод, что информационная безопасность может быть рассмотрена с двух ракурсов. С одной стороны информационная безопасность направлена на защиту охраняемой законом информации от противоправного завладения, использования, распространения. Такими сведениями является информация отнесенная законом к категории государственная тайна, коммерческая тайна, тайна частной жизни и так далее. С другой стороны информационная безопасность направлена на достижение состояния защищенности от вредоносной информации. Вредоносная информация характеризуется тем, что ее распространение потенциально несет вред или опасность общественным отношениям. Примером такой информации является информация, которая вводит население в заблуждение относительно новой короновирусной инфекции.

В результате проведенного анализа мы можем выделить следующие признаки категории «информационная безопасность»:

- представляет собой состояние защищенности;
- направлена на защиту интересов личности, общества и государства;
- обеспечивает защиту от незаконного получения, распространения и передачи информации, которая охраняется законом;
- обеспечивает защиту от вредной информации, потенциально оказывающей негативное воздействие на общественные отношения;
- направлена на реализацию конституционных прав и свобод человека и гражданина;
- направлена на достойные качество и уровень жизни граждан;
- направлена на сохранение и защиту государственного и народного суверенитета;
- направлена на сохранение территориальной целостности;
- направлена на обеспечение устойчивого социально-экономического развития Российской Федерации;
- направлена на оборону и безопасность государства.

Таким образом, мы можем сделать вывод, что определение информационной безопасности, предусмотренное соответствующей доктриной, в целом раскрывает основные характеристики рассматриваемой категории и не требует внесения существенных изменений.

Система информационной безопасности, равно как и любая другая система выстраивается вокруг базиса, а именно принципов, которые лежат в основе ее формирования [59, с. 80]. Доктрина содержит указание только на принципы деятельности госорганов, направленной на обеспечение информационной безопасности. Однако круг субъектов обеспечения информационной безопасности шире. Обращаясь к научной литературе, мы встретили следующие принципы, выделяемые в рамках исследования вопросов обеспечения информационной безопасности.

В первую очередь необходимо обозначить, что информационная безопасность реализуется в рамках общеправовых принципов. К их числу мы можем отнести: законность, равенство всех перед законом и судом, справедливость, гуманизм, единство прав и обязанностей и так далее. Мы не будем подробно акцентировать на них внимание, а сразу перейдем к специальным принципам, характеризующим специфику информационной безопасности.

Отдельные принципы обеспечения информационной безопасности мы можем найти в статье третьей Федерального закона «Об информации, информационных технологиях и о защите информации». К их числу законодатель относит:

- «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» [48].

В целом мы можем отметить, что практически каждый из перечисленных принципов дублирует или частично раскрывает конституционные положения относительно прав и свобод граждан в информационной сфере. Например, принцип свободы поиска, получения, передачи, производства и распространения информации любым законным способом был взят непосредственно из части четвертой статьи 29 Конституции Российской Федерации. Отдельно можно выделить принцип равноправия языков при создании информационных систем и их эксплуатации. Его нормативное закрепление можно объяснить тем, что народ Российской Федерации является многонациональным. Это в свою очередь создает необходимость при разработке информационных систем адаптировать интерфейс не только под русский язык, но и под язык, используемый на территории отдельных субъектов Российской Федерации.

Обращаясь по поводу принципов обеспечения информационной безопасности к научной литературе, можно встретить следующие точки зрения ученых-юристов. С.В. Баринов выделяет принцип 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» [5, с. 97]. Говоря более простым языком, с точки зрения юриспруденции, своевременность означает, что меры обеспечения информационной безопасности применяются своевременно. Ярким примером является закрепление административной ответственности за дискредитацию вооруженных сил Российской Федерации. Указанная мера была внесена в Кодекс об административных правонарушениях спустя месяц после начала специальной военной операции. Сначала был проведен мониторинг реакции населения, оценены риски от возможного влияния подобной информации на общественные отношения и принято решение предложить данную инициативу.

Многие исследователи выделяют принцип обоснованности информационной безопасности [45, с. 34]. Суть данного принципа заключается в том, чтобы меры, осуществляемые в рамках информационной безопасности, были соразмерны потенциальным угрозам. Оценка основана на сопоставление вероятных последствий запрета той или иной информации и потенциальной угрозы интересам личности, общества и государства. Кроме того, при разработке мер обеспечения информационной безопасности должны учитываться вероятные последствия применения таких мер, руководствуясь интересами личности, общества и государства. Нарушение принципа обоснованности нарушает права граждан на свободный доступ к информации, а также препятствует развитию отдельных сфер жизни общества.

Практическая составляющая выглядит следующим образом. Например, в сети начала появляться недостоверная информация о масштабах распространения короновирусной инфекции. Это приводит к волнениям среди населения. Наиболее верным в данном случае стало применение мер ответственности к распространителям такой информации, а также размещение на официальных ресурсах ежедневных сводок о распространении инфекции. Применение более категоричных мер (блокировка сайтов, где была размещена информация) было бы нецелесообразно, Применение более лояльных мер не возымело бы практического эффекта.

Отдельно исследователи выделяют принцип прогноза информационной безопасности [15, с. 273]. Указанный принцип заключается в том, что уполномоченные на обеспечение информационной безопасности органы проводят постоянный мониторинг, выявляют потенциальные угрозы и при помощи анализа возможного развития событий разрабатывают программу реализации мер на каждый из вероятных сценариев. Поэтому уже на стадии формирования угрозы уже имеется примерный план реализации мер обеспечения информационной безопасности. Таким образом, при возникновении угрозы удается свести возможный ущерб к минимуму. В основе аналитики и разработки прогноза лежит отечественный и зарубежный опыт обеспечения информационной безопасности, а также научные исследования по данному вопросу и технические разработки.

В качестве отдельного основополагающего начала можно выделить принцип распределения обязанностей в сфере обеспечения национальной 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» [27, с. 18].

Ю.Е. Кулаская предлагает в качестве самостоятельного принципа обеспечения информационной безопасности принцип глубокой защиты [25, с. 253]. Его характеристика несколько схожа с содержанием принципа прогноза. Основное отличие заключается в том, что принцип прогноза направлен на предотвращение потенциальных угроз, в то время, как рассматриваемый нами принцип допускает, что угроза уже имеет место быть. Глубокая защита подразумевает, что непосредственно сама информационная сфера в целом или ее отдельная часть подверглись противоправному воздействию, и необходимо применять специальные меры, поскольку остальные не возымели должного эффекта.

Обобщая все вышеизложенное касательно принципов информационной безопасности, мы можем отметить следующее. Принципы информационной безопасности – совокупность основополагающих начал, положений, идей, на которых строится система обеспечения информационной безопасности. Систему принципов можно разделить на общеправовые принципы и специальные, характерные исключительно информационной сфере. Можно отметить, что система принципов характеризуется не только направленностью защиты от внутренних и внешних угроз, но и особым вниманием на мониторинг и выявление потенциальных угроз, а также на формирование системы глубокой защиты, которая призвана минимизировать ущерб и устранить угрозу при самом негативном развитии событий.

Обобщая все вышеизложенное в данном параграфе, мы можем сделать ряд выводов, касательно темы настоящего исследования.

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». Мы можем сделать вывод, что определение информационной безопасности, предусмотренное соответствующей доктриной, в целом раскрывает основные характеристики рассматриваемой категории и не требует внесения существенных изменений. Отдельно нами было обращено внимание, что информационная безопасность может быть рассмотрена с двух ракурсов. С одной стороны информационная безопасность направлена на защиту охраняемой законом информации от противоправного завладения, использования, распространения. Такими сведениями является информация отнесенная законом к категории государственная тайна, коммерческая тайна, тайна частной жизни и так далее. С другой стороны информационная безопасность направлена на достижение состояния защищенности от вредоносной информации. Вредоносная информация характеризуется тем, что ее распространение потенциально несет вред или опасность общественным отношениям. Примером такой информации является информация, которая вводит население в заблуждение относительно новой короновирусной инфекции.

1.2 Правонарушения в сфере информационной безопасности

Для сферы обеспечения информационной безопасности характерно совершение различных правонарушений, за которые лицо может быть привлечено к уголовной, административной, дисциплинарной и гражданско-правовой ответственности. Определяя понятие правонарушения в сфере информационной безопасности, необходимо руководствоваться следующими признаками. Во-первых, это деяние, то есть, действие (распространение информации, которая является государственной тайной) или бездействие (отказ предоставить информацию, затрагивающую права и законные интересы гражданина. Во-вторых, имеет противоправный характер, то есть, совершение деяния противоречит положениям, предусмотренным одной или несколькими

правовыми нормами. В-третьих, как уже было отмечено ранее, указанное деяние запрещено под угрозой уголовного, административного наказания, а также применения дисциплинарных и гражданско-правовых санкций. В-четвертых, указанное деяние причиняет вред сфере информационной безопасности. В-пятых, такое деяние может быть совершено любым субъектом, то есть, физическим или юридическим лицом. При этом необходимо отметить, что физическое лицо должно достигнуть возраста соответствующего вида юридической ответственности и обладать полной дееспособностью. На квалификацию может влиять должностное и служебное положение лица [14, с. 115]. Таким образом, мы делаем вывод, что правонарушение в сфере обеспечения информационной безопасности – противоправное деяние, совершенное физическим или юридическим лицом, запрещенное под угрозой уголовной, административной, дисциплинарной и гражданско-правовой ответственности, направленное на причинение вреда человеку, юридическому лицу, объединениям граждан, государству, а также несущее угрозу сфере информационной безопасности.

Основываясь на том, к какому виду ответственности может быть привлечен нарушитель, в сфере обеспечения информационной безопасности мы можем выделить: преступления, административные правонарушения, дисциплинарные проступки, гражданско-правовые правонарушения.

В Уголовном кодексе Российской Федерации можно встретить следующие составы преступлений, направленных на охрану отношений в сфере обеспечения информационной безопасности:

- «нарушение неприкосновенности частной жизни;
- нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений;
- незаконный оборот специальных технических средств, предназначенных для негласного получения информации;
- отказ в предоставлении гражданину информации;
- разглашение тайны усыновления (удочерения);

– мошенничество в сфере компьютерной информации;
– незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну;
– злостное уклонение от раскрытия или предоставления информации, определенной законодательством Российской Федерации о ценных бумагах;
– неправомерное использование инсайдерской информации;
– сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей;
– неправомерный доступ к компьютерной информации;
– создание, использование и распространение вредоносных компьютерных программ;
– разглашение государственной тайны;
– незаконное получение сведений, составляющих государственную тайну;
– нарушение требований по защите государственной тайны;
– утрата документов, содержащих государственную тайну;
– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» [39].

Для квалификации отдельных видов преступлений в сфере обеспечения информационной безопасности характерен ряд проблемных аспектов. Рассмотрим некоторые из них, с целью разработки рекомендаций по совершенствованию системы противодействия правонарушениям в сфере информационной безопасности. Например, критике подвергается наличие в Уголовном кодексе состава преступления, который предусматривает ответственность за разглашение тайны усыновления (удочерения). Противники данной нормы указывают, что «такое положение 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» [20, с. 90]. На наш взгляд, подобное мнение не берет в расчет важность нормального психического развития ребенка. Сообщение подобной информации может нанести психологическую травму, а также прямо или косвенно создать определенные проблемы (например, травля среди сверстников). Следует также обратить внимание, что диспозиция статьи 155 Уголовного кодекса имеет своеобразный характер. Перечисляя субъекты преступления, законодатель, во-первых, ставит в один ряд обычных граждан и лица, которые обладают знаниями об усыновлении (удочерении) ввиду своих профессиональных или служебных обязанностей. Такой подход нельзя назвать корректным, поскольку во втором случае речь идет о более общественно-опасном деянии. Соответственно, наказание за его должно быть более суровым. Во-вторых, не совсем понятно с какой целью законодатель в качестве обязательного признака субъективной стороны для обычных граждан указывает корыстный или низменный мотив. При этом вопрос о понимании низменных мотивов является открытым, поскольку указанная формулировка имеет абстрактный характер и может толковаться «от ситуации к ситуации». Таким образом, мы предлагаем изменить редакцию статьи 155 Уголовного кодекса и изложить ее следующим образом:

«Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, независимо от мотива таких действий наказывается (предусмотренные уголовным законом возможные виды наказания по данному преступлению).

То же деяние, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну наказывается (предусмотренные уголовным законом возможные виды наказания по данному преступлению)».

Это позволит устранить выявленные нами спорные законодательные решения и поспособствует справедливости уголовного законодательства.

Другой проблемный аспект характерен для статьи 140 Уголовного кодекса. Исследователи подвергают критике и ставят под сомнение наличие уголовной ответственности за неправомерный отказ в получении информации. «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]. Невысокое число зарегистрированных преступлений по указанной статье, может свидетельствовать о двух альтернативных обстоятельствах. Во-первых, наличие нормы носит символический характер, поскольку никто не совершает указанное преступление ввиду различных обстоятельств. Однако такой вариант кажется маловероятным. Куда более реальным кажется тот факт, что подобная статистика указывает на серьезные проблемы при квалификации деяния по статье 140 Уголовного кодекса. Стоит отметить, что в Кодексе об административных правонарушениях в статье 5.39 предусмотрен аналогичный состав [22]. Отличие заключается в том, что административная ответственность предусматривается за формальный состав, а уголовная ответственность за материальный состав. Уголовный закон предусматривает последствия в виде вреда правам и законным интересам граждан. Мы весьма скептически относимся к подобной формулировке и считаем ее неудачной, поскольку совершение любого правонарушения причиняет вред правам и законным интересам граждан. Для решения указанной проблемы мы рекомендуем два альтернативных способа. Во-первых, можно изменить формулировку «вред правам и законным интересам граждан» и указать конкретные последствия, которые должны последовать после неправомерного отказа для квалификации по указанной статье Уголовного кодекса РФ. Во-вторых, можно исключить статью 5.39 из Кодекса РФ об административных правонарушениях и оставить только статью 140 Уголовного кодекса,

исключив из ее редакции слова «вред правам и законным интересам граждан». Поскольку сам по себе неправомерный отказ несет вред правам и законным интересам, а наличие двух идентичных по своей сути статей в разных нормативно-правовых актах создает трудности при осуществлении правоприменителем деятельности, направленной на квалификацию деяния.

Отдельными авторами обращается внимание на то обстоятельство, «что в диспозиции статьи 138 Уголовного кодекса, которая предусматривает ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, отсутствует указание на незаконность таких действий» [17, с. 56]. Так, согласно Федеральному закону «Об оперативно-розыскной деятельности», «оперативно-розыскные мероприятия, связанные с контролем почтовых отправлений, телеграфных и иных сообщений, прослушиванием телефонных переговоров с подключением к станционной аппаратуре предприятий, учреждений и организаций независимо от форм собственности, физических и юридических лиц, предоставляющих услуги и средства связи, со снятием информации с технических каналов связи, проводятся с использованием оперативно-технических сил и средств органов федеральной службы безопасности, органов внутренних дел и органов по контролю за оборотом наркотических средств и психотропных веществ в порядке, определяемом межведомственными нормативными актами или соглашениями между органами, осуществляющими оперативно-розыскную деятельность. При этом запрещается проведение оперативно-розыскных мероприятий и использование специальных и иных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, не уполномоченными на то вышеназванным Федеральным законом физическими и юридическими лицами» [49]. Само по себе наличие состава в тексте Уголовного кодекса означает его противоправность, то есть, отсутствие правовых оснований для совершения такого деяния. В этой связи мы не разделяем позицию авторов, которые

предлагают указать в тексте 138 Уголовного кодекса на незаконность совершаемых действий.

В ранее представленном нами перечне преступлений против информационной безопасности не была включена клевета. При этом отдельные ученые считают, что она должна относиться к числу таковых [56, с. 108]. Сама по себе клевета подразумевает искажение данных и их распространение третьим лицам. То есть, мы можем наблюдать в составе данного правонарушения воздействие на информационную сферу. По сути, указанное преступление сравнимо с той же самой дискредитацией вооруженных сил Российской Федерации, которая предусматривает административную ответственность. То есть, это заведомо ложные сведения, которые дискредитируют личность и создают у других членов общества ошибочное представление о ней, ее деяниях и прочих связанных с ней обстоятельствах. Таким образом, мы можем поддержать представленную позицию и отнести клевету к числу преступлений против информационной безопасности. При этом необходимо понимать, что в первую очередь клевета является преступлением против личности, а уже потом может быть отнесено к рассматриваемой категории преступлений.

Административная ответственность в сфере информационной безопасности предусмотрена главой 13 Кодекса Российской Федерации об административных правонарушениях. Стоит сразу сделать оговорку и отметить, что отдельные составы, входящие в систему мер обеспечения информационной безопасности, предусмотрены статьями, не входящими в указанную главу. Например, неправомерный отказ в предоставлении информации, публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации и ее граждан, поддержания международного мира и безопасности или исполнения государственными органами Российской Федерации своих полномочий в указанных целях и другие составы административных правонарушений. Глава 13 Кодекса РФ об

административных правонарушениях содержит следующие правонарушения против информационной безопасности:

- «нарушение правил использования на территории Российской Федерации спутниковых сетей связи, находящихся под юрисдикцией иностранных государств;
- нарушение установленного федеральным законом запрета публичного отождествления целей, решений и действий руководства СССР, командования и военнослужащих СССР с целями, решениями и действиями руководства нацистской Германии, командования и военнослужащих нацистской Германии и европейских стран оси в ходе Второй мировой войны, а также отрицания решающей роли советского народа в разгроме нацистской Германии и гуманитарной миссии СССР при освобождении стран Европы;
- неисполнение обязанностей, предусмотренных законодательством о деятельности иностранных лиц в информационно-телекоммуникационной сети Интернет на территории Российской Федерации;
- нарушение законодательства Российской Федерации в области персональных данных;
- распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера;
- нарушение правил защиты информации;
- нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;
- незаконная деятельность в области защиты информации;
- разглашение информации с ограниченным доступом;
- незаконное получение информации с ограниченным доступом;
- злоупотребление свободой массовой информации;

– воспрепятствование распространению продукции средства массовой информации;
– воспрепятствование уверенному приему радио- и телепрограмм и работе сайтов в сети Интернет;
– непредоставление первичных статистических данных;
– нарушение порядка размещения информации в государственной информационной системе жилищно-коммунального хозяйства;
– нарушение порядка размещения информации в единой информационной системе жилищного строительства;
– нарушение порядка представления сведений в федеральный реестр инвалидов и размещения указанных сведений в данном реестре;
– нарушение правил хранения, комплектования, учета или использования архивных документов;
– нарушение порядка изготовления или распространения продукции средства массовой информации;
– нарушение порядка представления обязательного экземпляра документов, письменных уведомлений, уставов и договоров;
– нарушение требований законодательства о хранении документов и информации, содержащейся в информационных системах;
– нарушение сроков и (или) порядка доставки (вручения) адресату судебных извещений;
– нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети Интернет;
– нарушение требования о размещении на территории Российской Федерации технических средств информационных систем;
– нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления;
– неисполнение обязанностей организатором распространения информации в сети Интернет;

– неисполнение обязанностей владельцем новостного агрегатора;
– нарушение установленных правил создания (замены) и выдачи ключа простой электронной подписи и правил использования федеральной государственной информационной системы;
– неисполнение оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети Интернет, обязанности по ограничению или возобновлению доступа к информации, доступ к которой должен быть ограничен или возобновлен на основании сведений, полученных от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере связи, информационных технологий и массовых коммуникаций;
– распространение владельцем аудиовизуального сервиса незарегистрированных средств массовой информации;
– нарушение владельцем аудиовизуального сервиса установленного порядка распространения среди детей информации, причиняющей вред их здоровью и (или) развитию;
– распространение владельцем аудиовизуального сервиса информации, содержащей публичные призывы к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремистской деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности;
– неисполнение обязанностей оператором поисковой системы;
– нарушение порядка ограничения доступа к информации, информационным ресурсам, доступ к которым подлежит ограничению в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о

защите информации, и (или) порядка удаления указанной информации»[22].

«Дела об административных правонарушениях в области связи и информации рассматривают:

– судьи; органы внутренних дел;
– органы, осуществляющие государственный надзор за связью и информатизацией;
– органы, осуществляющие контроль за обеспечением защиты государственной тайны;
– органы, осуществляю осуществляющие государственный контроль в области обращения и защиты информации;
– органы государственного статистического учета» [21].

В целом можно отметить, что административное законодательство предусматривает весьма широкий перечь административных правонарушений в сфере информационной безопасности, который учитывает все области жизни общества и соответствует высокой динамике общественных отношений, обусловленной стремительным развитием и ростом числа информационных правонарушений.

Наряду с преступлениями, при квалификации административных правонарушений против информационной безопасности можно встретить отдельные проблемные аспекты. Одной из явных проблем привлечения лица к административной ответственности в сфере информационной безопасности является «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» [7, с. 182]. Анонимность в интернете является важным вопросом в процессе регулирования правовой политики в сфере информационной безопасности. Данная категория имеет дискуссионный характер и весьма

сложна в урегулировании. В первую очередь стоит обратить внимание, что она является основополагающим условием повышения латентности рассматриваемой группы административных правонарушений. Например, распространение заведомо ложной, а также дискредитирующий информации может осуществляться посредством анонимных аккаунтов или с использованием специальных технических средств, которые делают невозможным обезличивание автора. При этом общество благосклонно относится к анонимности в сети Интернет, так как, с ее помощью можно создать дополнительные гарантии безопасности при подаче разного рода жалоб. На наш взгляд, абсолютная анонимность недопустима. Любое высказывание или утверждение должно иметь авторство, иначе высока вероятность использования анонимности в качестве инструмента для совершения правонарушения. В связи с этим мы выступаем за отмену абсолютной анонимности в сети Интернет, поскольку это будет способствовать обеспечению соблюдению правовых норм, а также уменьшит число правонарушений в сети.

Л.К. Терещенко обращает внимание, что определенные сомнения относительно целесообразности и эффективности возникают при анализе злоупотребления свободой массовой информации [37, с. 65]. Статья 13.15 Кодекса об административных правонарушениях содержит в себе различные составы административных правонарушений. В ней сконцентрировано более десяти различных конструкций, направленных на обеспечение информационной безопасности. Сама по себе формулировка «злоупотребление свободой массовой информации» кажется нам не совсем корректной, поскольку имеется две полярности «свобода массовой информации» и совершение запрещенного законом деяния. Если лицо нарушает правовую норму, то указанное деяние, на наш взгляд, не может быть отнесено к реализации права на свободу массовой информации. Можно отметить, что законодатель использует указанную норму в качестве способа упразднения пробелов в административном законодательстве и при

необходимости с ее помощью закрепляет новые составы правонарушений в сфере обеспечения информационной безопасности, если возникает такая необходимость. На наш взгляд, необходимо исключить указанную норму из Кодекса об административных правонарушенях и закрепить, предусмотренные ей конструкции в качестве отдельных, самостоятельных составов административных правонарушений. Нет никакой сложности в том, чтобы закрепить новое правонарушение в качестве самостоятельной статьи, а не заполнять постоянно одну статью новыми противоправными деяниями, которые, по мнению законодателя, являются проявлениями злоупотребления свободой массовой информации.

Гражданско-правовая ответственность в сфере информационной безопасности реализуется посредством подачи иска за причинение морального вреда, упущенной выгоды, причинения вреда деловой репутации. Согласно статье 151 Гражданского кодекса моральный вред представляет собой физические или нравственные страдания [12]. Моральный вред может быть вызван различными правонарушениями в сфере информационной безопасности. Например, распространение информации о частной жизни может стать основанием для взыскания компенсации за моральный вред. По сути, привлечение к материальной ответственности за совершение правонарушения в сфере информационной безопасности является видом внедоговорной ответственности. Внедоговорную ответственность можно расценивать как, причинение вреда личности субъекта правоотношений или его имуществу, несвязанного с исполнением договорных обязательств.

Дисциплинарная ответственность за совершение правонарушений в сфере информационной безопасности, как правило, связано с нарушением служебных и профессиональных обязанностей. Действующий Трудовой кодекс предусматривает следующие меры дисциплинарной ответственности:

– «замечание;
– выговор;
– увольнение» [38].

Например, пункт «в» статьи 81 ТК РФ предусматривает право работодателя уволить работника в том случае, если им была разглашена государственная, коммерческая или иная тайна, которая стала известна ему в силу исполнения служебной или профессиональной обязанности. Отдельно можно сослаться на положения Федерального закона от 29.07.2004 №98-ФЗ «О коммерческой тайне», в котором указано, что «работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации» [52].

Для государственных служащих предусмотрена более широкая система дисциплинарных наказаний. К их числу законодатель относит: замечание, выговор, предупреждение о неполном должностном соответствии, увольнение [51]. Стоит обратить внимание, что, как правило, инициации служебной проверки может стать основанием не только для дисциплинарной ответственности, но и для других вышеперечисленных видов ответственности. Так, в случае, когда в ходе проведения проверки в действиях лица была обнаружена необходимая совокупность признаков состава правонарушений, материалы служебной проверки направляются в правоохранительные органы для привлечения лица к административной или уголовно ответственности.

В завершении темы данной главы, мы считаем необходимым обратить внимание на следующие обстоятельства.

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». Мы можем сделать вывод, что определение информационной безопасности, предусмотренное соответствующей доктриной, в целом раскрывает основные характеристики рассматриваемой категории и не требует внесения существенных изменений. Отдельно нами было обращено внимание, что информационная безопасность может быть рассмотрена с двух ракурсов. С одной стороны информационная безопасность направлена на защиту охраняемой законом информации от противоправного завладения, использования, распространения. Такими сведениями является информация отнесенная законом к категории государственная тайна, коммерческая тайна, тайна частной жизни и так далее. С другой стороны информационная безопасность направлена на достижение состояния защищенности от вредоносной информации. Вредоносная информация характеризуется тем, что ее распространение потенциально несет вред или опасность общественным отношениям. Примером такой информации является информация, которая вводит население в заблуждение относительно новой короновирусной инфекции. Принципы информационной безопасности – совокупность основополагающих начал, положений, идей, на которых строится система обеспечения информационной безопасности. Систему принципов можно разделить на общеправовые принципы и специальные, характерные исключительно информационной сфере.

В ходе проведенного исследования нами были предложены следующие изменения в законодательстве.

Уголовный состав неправомерного отказа в предоставлении информации отличается от аналогичного административного состава, тем, что в Уголовном кодексе есть указание на последствия в виде вреда правам и законным интересам граждан. Мы весьма скептически относимся к подобной формулировке и считаем ее неудачной, поскольку совершение любого правонарушения причиняет вред правам и законным интересам граждан. Для решения указанной проблемы мы рекомендуем два альтернативных способа. Во-первых, можно изменить формулировку «вред правам и законным

интересам граждан» и указать конкретные последствия, которые должны последовать после неправомерного отказа для квалификации по указанной статье Уголовного кодекса. Во-вторых, можно исключить статью 5.39 из кодекса об административных правонарушениях и оставить только статью 140 Уголовного кодекса, исключив из ее редакции слова «вред правам и законным интересам граждан». Поскольку сам по себе неправомерный отказ несет вред правам и законным интересам, а наличие двух идентичных по своей сути статей в разных нормативно-правовых актах создает трудности при осуществлении правоприменителем деятельности, направленной на квалификацию деяния.

На наш взгляд, необходимо исключить статью 13.15 из Кодекса об административных правонарушениях и закрепить, предусмотренные ей конструкции в качестве отдельных, самостоятельных составов административных правонарушений. Нет никакой сложности в том, чтобы закрепить новое правонарушение в качестве самостоятельной статьи, а не заполнять постоянно одну статью новыми противоправными деяниями, которые, по мнению законодателя, являются проявлениями злоупотребления свободой массовой информации.

Защита информации (данных, сведений, охраняемой законом тайны) необходимо осуществлять и с точки зрения уголовного законодательства, что потребует разностороннего совершенствования уголовного законодательства, включения в его состав новых норм и институтов, отвечающих потребностям стремительно развивающейся информационной сферы современного российского общества.

Мы предлагаем изменить редакцию статьи 155 Уголовного кодекса следующим образом.

«Разглашение тайны усыновления (удочерения) вопреки воле усыновителя, независимо от мотива таких действий наказывается (предусмотренные уголовным законом возможные виды наказания по данному преступлению).

То же деяние, совершенное лицом, обязанным хранить факт усыновления (удочерения) как служебную или профессиональную тайну наказывается (предусмотренные уголовным законом возможные виды наказания по данному преступлению)».

Указанные изменения, на наш взгляд, позволят повысить эффективность мер обеспечения информационной безопасности.

Глава 2 Элементы правового регулирования информационной безопасности

2.1 Конституционно-правовые основы регулирования информационной безопасности

В основе любой правовой политики лежат нормы конституционного права. С их помощью законодатель закладывает фундамент для того или иного правового института или отрасли. В дальнейшем такие фундаментальные нормы, как правило, находят свое развитие и конкретизируются в федеральных законах, а также иных нормативно-правовых актов. Изучение конституционно-правовых основ позволяет установить, какие именно направления развития являются приоритетными, а также выявить пробелы, допущенные еще на стадии формирования системы правового регулирования информационной сферы. Конституция содержит в себе ряд положений, которые мы можем рассматривать в качестве конституционно-правовых основ формирования системы информационной безопасности.

Хотя каждое положение главы второй Конституции Российской Федерации имеет одинаковую юридическую силу, на наш взгляд, фундаментальным для всей системы информационной безопасности является положение части четвертой статьи 29 Конституции, содержание которой выглядит следующим образом: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» [24]. По своей структуре указанная норма похожа на норму о праве собственности, где законодатель ограничивается перечислением доступных собственнику прав. В этом случае при помощи перечисления законодатель раскрывает принцип свободы информации.

Как уже было отмечено ранее, свобода информации не абсолютна, она ограничена рядом правовых институтов, одним из которых является институт государственной тайны. «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» [18]. Необходимость ограничения прав в информационной сфере путем внедрения института государственной тайны обусловлено тем, что отдельная информация имеет стратегическую важность и ее широкое распространение можно нанести вред охраняемым государством интересам. Например, распространение информации о размещении военных и стратегически-важных объектов может отрицательно сказаться на обороноспособности государства. Можно выделить четыре основных видов информации, которые относятся к категории «государственная тайна»:

– сведения в военной области;

– сведения в области экономики, науки и техники;

– сведения в области внешней политики и экономики;

– сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму.

Выделяя категории сведений, которые могут быть признаны государственной тайной, законодатель отдельно перечисляет отдельные сведения, которые не могут признаваться государственной тайной не при каких обстоятельствах. К их числу законодатель относит сведения:

- «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)» [18].

Оценивая каждый из представленных элементов списка, мы можем сделать вывод, что сведения не могут стать государственной тайной, если они затрагивают наиболее значимые, с точки зрения законодателя, права и свободы. Например, человек, его права и свободы признаются в нашей стране высшей ценностью, поэтому запрещено скрывать информацию о фактах их нарушения. Аналогично дела обстоят и с информацией об обстоятельствах, потенциально угрожающих жизни и здоровью граждан. Запрет на сокрытие информации состоянии здоровья высших должностных лиц обусловлен тем, что Российская Федерация является демократическим государством. Соответственно, каждый гражданин имеет право на участие в управлении делами государство. Из этого следует, что он имеет право знать о том, что высшее должностное лицо в силу состояния здоровья не может выполнять свои должностные обязанности.

Следующий элемент конституционно-правового статуса в сфере обеспечения информационной безопасности закреплен в статье 23 основного закона. В указанной статье закреплено право каждого на личную и семейную тайну. Здесь стоит обратить внимание, что, в законодательстве отсутствует легальное определение понятий «личная тайна» и «семейная тайна», а также их оценочные критерии. На сегодняшний день упоминание указанных понятий можно найти в части третьей статье 25 Федерального закона «Об архивном деле в Российской Федерации». Так, в указанной статье установлено, 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» [46]. На практике указанная норма создает определенные сложности в получении информации относительно жизни тех или иных лиц. В основном эта проблема затрагивает исследовательскую деятельность. В отсутствии конкретики относительно понятий «личная тайна» и «семейная тайна» сотрудники архива могут толковать их смысл по своему личному усмотрению. По этому в отдельных случаях при идентичных запросах гражданам отказывают в доступе к информации, а в других допускают к архивной документации.

Стоит отметить, что в 2005 году Конституционный Суд в своем определении давал разъяснение по поводу 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» [31]. Отметим, что в определении весьма размыто раскрыты критерии отнесения информации к понятию частная жизнь. Однако мы можем с уверенностью утверждать, что сведения о противоправных действиях гражданина не входит в категорию частная жизнь.

Можно предположить, что законодатель исходит из того, что личная и семейная тайна это собирательные категории, которые объединяют закрепленные в других нормативно-правовых актах виды засекреченной информации личного и семейного характера. В подтверждение данного предположения можно указать, что к категории личная тайна могут быть отнесены, например, врачебная тайна [50] или тайна совершения завещания [13]. В свою очередь к семейной тайне мы можем отнести, например, тайну усыновления [35]. Применения подхода к пониманию личной и семейной тайны означает, что уполномоченное лицо должно ссылаться не на само понятие, упомянутое в законе, а на конкретное положение нормативно-

правового акта, ограничивающее доступ к той или иной информации. С целью обеспечения единства правоприменительной практики мы видим возможным следующее решение возникшей проблемы. На наш взгляд, закрепить понятие личной и семейной тайны или их признаки, при помощи которых стало бы возможно, более точно утверждать относится та или иная информация к личной или семейной тайне или нет. Кроме того, Пленуму Верховного Суда необходимо разъяснить положения части третьей статьи 25 Федерального закона «Об архивном деле в Российской Федерации» с целью ограничить неправомерный отказ в получении информации со ссылкой на указанную норму.

«Отдельно в основном законе закреплена обязанность органов государственной власти и местного самоуправления обеспечить возможность ознакомиться с документами и материалами, затрагивающими его права и свободы. Соответственно, можно сделать вывод, что каждый имеет право на допуск к информации, содержащейся в документах, относительно его прав и свобод, если это не противоречит федеральному законодательству» [2, с. 65].

Отдельно можно отметить, что в статье 28 основного закона указано, что каждому гарантируется право свободно исповедовать свою религию и иные убеждения. Мы можем отнести данное положение к группе прав в сфере информации, поскольку его реализация позволяет распространять информацию о своем вероисповедании, а также своих убеждениях. Отдельно стоит обратить внимание, что, как правило, законодатель в основном законе указывает на возможные ограничения того или иного права. «Однако в данном случае указание на ограничение отсутствует. При этом можно с уверенностью утверждать, что далеко не все религии и убеждения могут свободно исповедоваться в Российской Федерации. Например, если религиозные постулаты или убеждения направлены на возбуждение вражды или ненависти, то такие убеждения не могут свободно распространяться, поскольку такое деяние является преступлением, предусмотренным статьей 282 Уголовного кодекса» [36, с. 17]. Указанное обстоятельство позволяет нам рекомендовать

внесение изменений в статью 28 Конституции Российской Федерации. Рекомендованная редакция выглядит следующим образом.

«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».

Частью пятой статьи 29 Конституции Российской Федерации установлена гарантия свободы массовой информации. Законодатель делает отдельную оговорку и указывает, что цензура средств массовой информации в любом ее виде запрещена. Вопрос цензуры является актуальным в современных реалиях, поскольку с каждым годом мы видим увеличение государственного влияния на средства массовой. Здесь стоит обозначить, что именно в отечественном законодательстве принято понимать в качестве цензуры. «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» [19]. Представленное определение не учитывает того обстоятельства, что воздействие на средства массовой информации может оказываться посредством третьих лиц. То есть, представитель органа власти может попытаться повлиять на публикацию того или иного материала путем опосредованных угроз. Например, должностное лицо может обратиться к главному редактору издания с угрозами применить свои полномочия во вред, если последним будет опубликован «неугодный» материал. Поэтому мы предлагаем внести изменения в действующее определение цензуры, в новой редакции оно будет выглядеть следующим образом: «Цензура массовой

информации, то есть требование от редакции средства массовой информации непосредственно со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений или по их инициативе через третьих лиц 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».

Отдельные авторы, рассматривая вопросы цензуры в современной России, говорят о наличии негласной цензуры. Так, автор исследователи обращают внимание на случаи, «когда отдельные СМИ, поддерживающие оппозиционные движения, были заблокированы по весьма сомнительным основаниям. Как правило, такими основаниями являлись призывы к противоправному участию в массовых мероприятиях» [9, с. 7]. Однако в этом случае, с точки зрения законодательства, такие действия нельзя рассматривать как цензуру. Мы бы охарактеризовали это как давление в рамках действующего законодательства. Поэтому мы не разделяем позицию ученых, которые заявляют о наличии цензуры в современной Российской Федерации. Можно проследить определенные признаки воздействия на средства массовой информации, однако, такие действия осуществляются исключительно в рамках действующего законодательства.

«К числу конституционных гарантий обеспечения информационной безопасности право обращаться лично или коллективно в органы государственной власти и органы местного самоуправления, право на получение достоверной информации о состоянии окружающей среды, а также право не свидетельствовать против самого себя, супруга и близких родственников» [29, с. 18]. В обоснование указанной позиции можно встретить следующие точки зрения. Так, «право на обращение граждан нельзя назвать информационным правом в чистом виде. Оно служит инструментом в рамках реализации иных конституционных прав. Например, посредством обращения гражданин может получить сведения, которые затрагивают его

права и обязанности, или иную информацию из архивной документации (планы города, перечень проделанных работ в рамках благоустройства города и так далее). И поскольку при помощи права на обращения реализуются иные конституционные права и свободы в информационной сфере, косвенно мы можем отнести его к числу конституционных гарантий обеспечения информационной безопасности» [32, с. 90].

В сфере обеспечения информационной безопасности можно выделить право на достоверную информацию об окружающей среде. Наличие указанного право обусловлено тем, что состояние окружающей среды прямо влияет на состояние здоровья гражданина, поэтому он имеет право обладать достоверной информации относительно ее состояния. Как уже было отмечено нами ранее, информация об окружающей среде не может быть отнесена к категории «государственная тайна». Указанное положение, по сути, является гарантией права на получение достоверной информации об окружающей среде.

Право каждого не свидетельствовать против самого себя, своего супруга или своих близких родственников непосредственно связано с категориями «семейная тайна» и «тайна частной жизни». Как ранее уже было нами отмечено, информация о совершении противоправных действий не может являться семейной или какой-либо другой тайной. При этом действие может быть признано противоправным только по решению уполномоченного лица при наличии достаточных для этого оснований, до этого информация о любых действиях лица справедливо признается тайной и может не разглашаться без каких-либо последствий.

В рамках данного параграфа нами были сделаны следующие выводы.

Конституция содержит в себе ряд положений, которые мы можем рассматривать в качестве конституционно-правовых основ формирования системы информационной безопасности.

С целью обеспечения единства правоприменительной практики мы предлагаем конкретизировать понятия «личная тайна» и «семейная тайна»

посредством принятия соответствующего федерального закона, в котором будут конкретизированы указанные понятия, перечислены их сущностные признаки, а также определены правила их правоприменения.

Мы рекомендуем внести изменения в статью 28 Конституции Российской Федерации. Рекомендованная редакция выглядит следующим образом.

«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».

Мы предлагаем внести изменения в действующее определение цензуры, в новой редакции оно будет выглядеть следующим образом: «Цензура массовой информации, то есть требование от редакции средства массовой информации непосредственно со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений или по их инициативе через третьих лиц 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».

2.2 Организационные основы регулирования информационной безопасности

Конституционно-правовые основы задают общие направления формирования системы обеспечения информационной безопасности. В свою очередь деятельность данной системы выстраивается, в том числе, вокруг организационных основ, которые, по сути, выступают продолжением норм конституционного права, развивая их положения и углубляясь в

информационную специфику. 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. Указанное положение позволяет нам сделать вывод, что при реализации правовой политики, направленной на обеспечение информационной безопасности, задействованы не только органы власти и местного самоуправления, но и сами граждане, а также их объединения. На наш взгляд это является положительным условием реализации политики в области информационной безопасности. Хотя стоит принимать во внимание, что в нынешних условиях, когда в обществе творится информационный хаос, задействовать общественный потенциал становится весьма проблематично. Поэтому непосредственно в нынешних условиях упор при обеспечении информационной безопасности должен делаться на работу органов государственной власти.

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» [41].

Каждый из названных выше субъектов имеет в своей компетенции отдельные полномочия в сфере информационной безопасности. Например, верхняя и нижняя палаты Федерального Собрания занимаются разработкой и принятием законопроектов, направленных на обеспечение информационной безопасности в Российской Федерации. Органы исполнительной власти разрабатывают и принимают концепции обеспечения информационной безопасности на территории субъекта. Следует обратить внимание, что полномочия Президента Российской Федерации также подразумевают участие в процессе обеспечения информационной безопасности. Так, в статье шестой Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» указано, что «Президент Российской Федерации определяет основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры» [47]. Более того, Президентом утверждается Доктрина информационной безопасности Российской Федерации, поэтому нам кажется не совсем корректным его отсутствие в перечне. В связи с этим, не совсем понятно по какой причине Президент отсутствует в рассмотренном нами списке. Возможно, стоит рассмотреть возможность его включения в предусмотренный Доктриной список, поскольку он обладает широким спектром полномочий в сфере обеспечения информационной безопасности.

Нам кажется возможным в нынешних реалиях рассмотреть возможность создания специализированного органа, деятельность которого будет полностью направлена на обеспечение информационной безопасности. В частности к его полномочиям могут быть отнесены:

– контроль за распространением ложной информации, которая подрывает интересы Российской Федерации, нарушает права и

свободы человека, а также наносит вред духовным и нравственным ориентирам общества (культура, история и так далее);

- противодействие органам иностранных государств, чья деятельность направлена на реализацию информационно-психологического воздействия на население Российской Федерации;
- мониторинг за наиболее актуальными темами и обращение в соответствующие органы за получением оперативных разъяснений по тем или иным вопросам (например, в ситуации с короновирусной инфекцией при помощи деятельности данного органа удалось бы оперативно противодействовать ложной информации о ее распространении, путем публикации заявлений министерства здравоохранения относительно тех или иных данных, являющихся предметом обсуждения населения).

Можно утверждать, что указанные полномочия уже относятся к компетенции различных органов власти, но создание единого органа способствовало повышению оперативности в вопросах противодействия угрозам информационной безопасности.

Организационные основы обеспечения информационной безопасности включают в себя, в том числе и принципы, на которых основывается деятельность ее субъектов. Доктрина содержит указание только на принципы деятельности госорганов, направленной на обеспечение информационной безопасности. Однако круг субъектов обеспечения информационной безопасности шире. Обращаясь к научной литературе, мы встретили следующие принципы, выделяемые в рамках исследования вопросов обеспечения информационной безопасности.

В первую очередь необходимо обозначить, что информационная безопасность реализуется в рамках общеправовых принципов. К их числу мы можем отнести: законность, равенство всех перед законом и судом, справедливость, гуманизм, единство прав и обязанностей и так далее. Мы не будем подробно акцентировать на них внимание, а сразу перейдем к

специальным принципам, характеризующим специфику информационной безопасности.

Отдельные принципы обеспечения информационной безопасности мы можем найти в статье третьей Федерального закона «Об информации, информационных технологиях и о защите информации». К их числу законодатель относит:

- «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» [48].

Говоря об организационных основах, необходимо затронуть вопрос средств по обеспечению информационной безопасности. В доктрине средства обеспечения информационной безопасности делят на следующие группы: правовые, организационно-технические и экономические. В число экономических мер обеспечения информационной безопасности мы можем включить определение порядка финансирования программ, направленных на обеспечения информационной безопасности, финансирование работ, связанных с разработкой новых технических и программных методов зашиты информации, разработка, создание и поддержка системы страхования информационных рисков.

«Технические меры направлены на аппаратное и программное обеспечение информационной безопасности. То есть, они отражают непосредственную сторону обеспечения информационной безопасности. Но необходимо отметить, как показала практика, возможность построить эффективную и бесперебойно функционирующую систему на основе одних технических средств защиты исключена. Эффективность системы обеспечения информационной безопасности зависит от совокупности всех видов мер, каждый из которых выступает уникальным элементом, выполняющим свою задачу на пути достижения единой цели» [6, с. 117].

«В свою очередь правовые меры представляют собой положения действующего отечественного законодательства, направленные на обеспечение информационной безопасности» [20, с. 65]. Сюда мы можем отнести уже ранее рассмотренные положения Конституции Российской Федерации, положения и специализированные федеральные законы, а также подзаконные акты. Важное место в подсистеме правовых мер обеспечения информационной безопасности занимают меры ответственности за нарушение информационного законодательства. С их помощью государство препятствует распространению вредоносного программного обеспечения, несущего угрозу информационной безопасности, разглашению информации, составляющих тайну, а также сведений, которые могут причинить вред человеку, обществу и

государству. Подробно данный вопрос был рассмотрен нами в предыдущей главе.

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» [28, с. 46]. Указанные меры схожи с теми, которые применяются при обеспечении антикоррупционной безопасности. Безусловно, при развитой правовой культуре и должном уровне правосознания граждан число правонарушений (в том числе и направленных на дестабилизацию информационной безопасности) может сократиться. Однако, проводя аналогию с противодействием коррупции, указанные меры широко не применяются в процессе обеспечения информационной безопасности. Хотя можно отметить, что имеют место быть активные проявления применения морально-этических мер. Так, они активно применялись при противодействие распространению ложной информации в период разгара пандемии, и активно применяются сейчас для снижения распространения ложной информации относительно специальной военной операции на Украине. Мы придерживаемся мнения, что в нынешних условиях информационной войны, необходимо широкое применение морально-этических мер обеспечения информационной безопасности, направленных на укрепление в сознании граждан установки о недопустимости распространения ложной или непроверенной информации, а также совершения иных правонарушений в области информационного права, поскольку на фоне происходящих событий

(например, частичной мобилизации) они могут вызвать панику в обществе и привести к существенным негативным последствиям.

Обобщая все вышеизложенное, нами будут сделаны следующие выводы в рамках данного параграфа.

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. В доктрине средства обеспечения информационной безопасности делят на следующие группы: правовые, организационно-технические и экономические. Важное место в подсистеме правовых мер обеспечения информационной безопасности занимают меры ответственности за нарушение информационного законодательства. С их помощью государство препятствует распространению вредоносного программного обеспечения, несущего угрозу информационной безопасности, разглашению информации, составляющих тайну, а также сведений, которые могут причинить вред человеку, обществу и государству.

Нам кажется возможным в нынешних реалиях рассмотреть возможность создания специализированного органа, деятельность которого будет полностью направлена на обеспечение информационной безопасности. В частности к его полномочиям могут быть отнесены: контроль за распространением ложной информации, которая подрывает интересы Российской Федерации, нарушает права и свободы человека, а также наносит вред духовным и нравственным ориентирам общества (культура, история и так далее); противодействие организациям, созданным иностранными государствами, чья деятельность направлена на реализацию информационно-психологического воздействия на население Российской Федерации; мониторинг за наиболее актуальными темами и обращение в соответствующие органы за получением оперативных разъяснений по тем или иным вопросам (например, в ситуации с короновирусной инфекцией при помощи

деятельности данного органа удалось бы оперативно противодействовать ложной информации о ее распространении, путем публикации заявлений министерства здравоохранения относительно тех или иных данных, являющихся предметом обсуждения населения). Можно утверждать, что указанные полномочия уже относятся к компетенции различных органов власти, но создание единого органа способствовало повышению оперативности в вопросах противодействия угрозам информационной безопасности.

2.3 Особенности правового регулирования информационной безопасности в сети «Интернет»

На сегодняшний день интернет плотно вошел в жизнь практически каждого жителя нашей страны. С его помощью люди поддерживают связь, проводят досуг, работают и получают информацию. По данным исследования, которое ежегодно проводит Global Digital, в среднем в интернете человек проводит около семи часов. Учитывая, что восемь часов необходимо для сна, выходит, что половину своего времени человек проводит в интернете [60]. Подобный масштаб свидетельствует о том, что вопросам регулирования правоотношений внутри сети «Интернет» необходимо уделять особое внимание.

Государство принимает участие в регулировании отношений связанных с интернетом. Так, порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной 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» [43].

Помимо этого, в целях обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети «Интернет», установлено, что:

- «подключение информационных систем, информационно-телекоммуникационных 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» [42].

Анализ научной литературы позволил нам выявить следующие актуальные проблемы правового регулирования в сети «Интернет»:

Основными проблемами в сети Интернет, нуждающимися в скорейшем нормативно-правовом урегулировании, являются:

- «распространение экстремистских материалов в сети» [57, с. 161];
- «проблемы, связанные с защитой прав интеллектуальной собственности в сети» [33, с. 10];
- «проблемы правового регулирования исключительных прав на сетевой адрес (доменное имя)» [34, с. 383];
- защита персональных данных;
- пропаганда, незаконная реклама наркотических средств и психотропных веществ;
- незаконное распространение порнографических материалов в сети;
- мошенничество в сети.

Говоря об экстремистских движениях и экстремистской деятельности в сети «Интернет», стоит сразу указать, что Федеральный закон «О противодействии экстремистской деятельности» устанавливает «недопущение использования сетей связи общего пользования для осуществления экстремистской деятельности» [53]. Нарушение запрета предусматривает привлечение к административной и уголовной ответственности. Здесь стоит обратить внимание, что в отдельных случаях наблюдается чрезмерная бдительность сотрудников правоохранительных органов. В результате чего, практика знает случаи, когда граждане привлекались к ответственности по статье 282 Уголовного кодекса за размещение, лайки, репосты изображений, которые с точки зрения представителей отдельных социальных групп, являлись оскорбительными и унизительными. Реализация указанной нормы в части применения ее к отношениям в сети «Интернет» имеет слишком субъективный характер.

Необходимо совершенствовать данный механизм, добавляя в него элементы объективной оценки.

Одним из основных способов обеспечения информационной безопасности в сети «Интернет» является блокировка нежелательного и вредоносного контента. Процедура блокировки начинается с подачи административного искового заявления. Если судом будет принято решение о том, что информация, которая является предметом административного иска, противоречит законодательству Российской Федерации, то судом выносится соответствующее решение. После этого решение направляется в Роскомнадзор. На основании судебного решения Роскомнадзор вносит запись в соответствующий реестр и уведомляет об этом владельца сайта. Владельцу сайта надлежит после уведомления удалить противоправную информацию в установленный законом срок. Если тот не подчинится законным требованиям, то «Интернет» ресурс блокируется полностью. При этом для применения указанной меры обеспечения информационной безопасности характерен ряд проблем. В первую очередь необходимо отметить, что в сети существуют средства для доступа к заблокированным на территории Российской Федерации сайтам. Для этого мы предлагаем, запретить на законодательном уровне сервисы для доступа к запрещенным на территории Российской Федерации информационным ресурсам. Кроме того, как правило, злоумышленники сохраняют копии блокируемых сайтов и в дальнейшем запускают их под другим именем.

В завершении темы данной главы мы можем сделать следующие выводы.

Конституция содержит в себе ряд положений, которые можно рассматривать в качестве конституционно-правовых основ формирования системы информационной 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. В доктрине средства обеспечения информационной безопасности делят на следующие группы: правовые, организационно-технические и экономические.

Кажется возможным в нынешних реалиях рассмотреть возможность создания специализированного органа, деятельность которого будет полностью направлена на обеспечение информационной безопасности. В частности к его полномочиям могут быть отнесены: контроль за распространением ложной информации, которая подрывает интересы Российской Федерации, нарушает права и свободы человека, а также наносит вред духовным и нравственным ориентирам общества (культура, история и так далее); противодействие организациям, созданным иностранными государствами, чья деятельность направлена на реализацию информационно-психологического воздействия на население Российской Федерации; мониторинг за наиболее актуальными темами и обращение в соответствующие органы за получением оперативных разъяснений по тем или иным вопросам (например, в ситуации с короновирусной инфекцией при помощи деятельности данного органа удалось бы оперативно противодействовать ложной информации о ее распространении, путем публикации заявлений министерства здравоохранения относительно тех или иных данных, являющихся предметом обсуждения населения). Можно утверждать, что указанные полномочия уже относятся к компетенции различных органов власти, но создание единого органа способствовало повышению оперативности в вопросах противодействия угрозам информационной безопасности.

С целью обеспечения единства правоприменительной практики мы предлагаем конкретизировать понятия «личная тайна» и «семейная тайна» посредством принятия соответствующего федерального закона, в котором будут конкретизированы указанные понятия, перечислены их сущностные признаки, а также определены правила их правоприменения.

Рекомендуется внести изменения в статью 28 Конституции Российской Федерации. Рекомендованная редакция выглядит следующим образом. «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».

Предлагается также внести изменения в действующее определение цензуры, в новой редакции оно будет выглядеть следующим образом: «Цензура массовой информации, то есть требование от редакции средства массовой информации непосредственно со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений или по их инициативе через третьих лиц 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».

Глава 3 Проблемы правового регулирования информационной безопасности в Российской Федерации

В процессе исследования реализации правовой политики в сфере обеспечения информационной безопасности уже были обозначены определенные проблемы, характерные для данной отрасли. Отдельно стоит обратить внимание, что ряд проблем вызван, во-первых, быстрым развитием технологий, которые упрощают совершение правонарушений в сфере информационной безопасности, а также повышают их латентность, во-вторых, противостоянием Российской Федерации с недружественными государствами, которое характеризуется участием большого числа организаций, предпринимающих попытки оказать на население страны информационно-психологическое давление.

Одной из актуальных проблем, на наш взгляд, является слабая защита персональных данных. Например, за последние несколько месяцев имело место быть несколько утечек персональных данных пользователей сервиса «Яндекс.Еда», а также магазина бытовой техники «ДНС». Кроме того, базы данных некоторых государственных учреждений оказались в сети, и любой желающий в свободном доступе мог с ними ознакомиться. Следует также обратить внимание, что в интернете можно найти «специалистов», которые за вознаграждение могут по номеру телефона, автомобиля или по имени, фамилии и отчеству предоставить пакет персональных данных гражданина. Объяснить такое положение вещей, на наш взгляд, можно следующими обстоятельствами. Во-первых, граждане обладают низким уровнем информационной грамотности. В основном это касается лиц пожилого возраста, но и не только они передают свои данные в руки мошенникам. Во-вторых, в государственных органах имеет место быть коррупционная составляющая. Имеется вероятность, что за вознаграждение госслужащий может передать информационные базы, содержащие персональные данные, третьим лицам. В-третьих, низкая мотивация IT специалистов, вызывает отток

профессиональных кадров, в результате чего наблюдается низкая эффективность технической системы информационной безопасности. В связи с этим, в первую очередь необходимо реализовать комплекс мероприятий, направленный на повышение информационной грамотности населения. Также важно разъяснить населению значение сохранности своих персональных данных и вероятные последствия распространения такой информации.

«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» [30, с. 54]. Однако оперативность при выявлении указанных правонарушений осложняется следующими обстоятельствами. Данные противоправные деяния, как правило, подпадают под признаки составов преступлений, предусмотренных ст. 138, 138.1 Уголовного кодекса. Согласно пункту первому части второй статьи 151 Уголовно-процессуального кодекса указанные преступления относятся к компетенции Следственного комитета Российской Федерации [40]. В данном случае отсутствует альтернативная подследственность, что не позволяет задействовать ресурс следственных подразделений правоохранительных органов для противодействия угрозе 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 в своем исследовании выделяет следующую проблему, характерную обеспечению информационной безопасности в

нынешних реалиях. «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» [55, с. 30]. Представляется, что для решения указанной проблемы необходимо исходить именно из общих интересов, которые являются предметом совместного ведения, и уже на основе этого определять, какие направления затрагивают обеспечение информационной безопасности. Говоря же о разработке политики по обеспечению информационной безопасности внутри субъекта, следует ориентироваться на исключительные полномочия субъекта, к которым можно отнести: распространение информации внутри региона; работа с региональными информационными ресурсами, формирование и развитие информационной структуры внутри региона.

Отдельного внимания заслуживают вопросы обеспечение информационной безопасности несовершеннолетних в сети «Интернет». «Причем речь идет не только о материале, который предназначен исключительно для совершеннолетних пользователей, но и о публикациях, которые могут привести к самоубийству несовершеннолетнего, совершении

им террористического акта или другим ужасным последствиям. Вопрос о необходимости ограничить возможности несовершеннолетних в интернете является дискуссионным и уже неоднократно обсуждался среди юристов, политиков, психологов и обычных граждан. Использование ресурсов сети является одним из условий социализации в современном мире» [23, с. 15]. В целом, можно согласиться с автором, поскольку в сети содержится огромное количество информации, способное расширить кругозор и представление об окружающем мире. При этом нельзя забывать, что информацию все-таки необходимо уметь фильтровать, чего несовершеннолетние пользователи, как правило, не делают в силу отсутствия навыка или желания. М.С. Власенко предлагает для обеспечения безопасности несовершеннолетних блокировать продвижение на рынок интернет-услуг ресурсов, в которых исключен доступ к нелегальной и вредной информации [11, с. 100]. Представляется, что такой подход представляется весьма спорным. Нелегальная информация априори должна блокироваться после обнаружения. «Что касается ограничения «вредной» информации, здесь необходимо исходить из того, что, по мнению автора, она не является противоправной, поскольку он использовал эти категории при перечислении, поэтому они не являются взаимозаменяемыми. Вероятно, речь идет о материале для совершеннолетних, который может причинить вред психике ребенка. Тогда предложенное ограничение размещения подобных материалов будет прямым нарушением конституционного права граждан на информацию (речь идет о совершеннолетних гражданах)» [54, с. 365].

Для разрешения указанной проблемы требуется комплексный подход. Необходимо прививать информационную грамотность с ранних лет. В первую очередь это должны быть правила информационного этикета (запрет на оскорбление других пользователей, запрет на переход по ссылкам, где стоит обозначение «18+» и так далее. Реализовать данные мероприятия можно в рамках курс «информатика», также можно ввести отдельные курсы «информационная безопасность в сети «Интернет». При этом важно отметить

важность участия родителей в рамках повышения информационной грамотности и процессе обеспечения информационной безопасности детей в сети «Интернет». В первую очередь необходимо использовать механизмы технического контроля (родительский контроль, детский аккаунт, привязанный к родительскому и так далее). Вполне возможно было бы перенести систему семейных аккаунтов на сим-карты. То есть, приобретая сим-карту ребенку, родитель может контролировать его звонки, исходящий трафик в сети «Интернет» и другие взаимодействия посредством использования устройства.

«Отдельного внимания заслуживают сайты, которые являются общедоступными, но при этом содержат вредную для детей информацию. Примером таких площадок являются ВКонтакте, Тик-ток, Одноклассники. Ранее отдельными общественными деятелями высказывались предложения о запрете посещения таких сайтов малолетними, путем идентификации личности при помощи паспорта» [3, с. 105]. На наш взгляд, такой способ является слишком радикальным. Необходимо исходить из того, что социальные сети используется в том числе, как инструмент взаимодействия с родителями, а также для учебы (чаты учеников, взаимодействие с преподавателем и так далее). Поэтому нам видится возможным другой способ решения проблемы. Вполне логичным кажется обязать крупные социальные сети требовать верификацию по паспорту. При его отсутствии или же возрасте пользователя до 16 лет, профиль должен быть ограничен в функционале в части посещения отдельных сообществ. Например, можно проводить проверку сообществ и ставить на них отметку «доступно для детей младше шестнадцати лет». Это позволит ограничить взаимодействие с вредоносной информацией. Кроме того, действия такого пользователя должны отслеживаться администраторами сайта (проверка комментариев, взаимодействие с другими пользователями и так далее).

«Другая проблема обеспечения информационной безопасности заключается в том, что специальные службы враждебно настроенных

государств осуществляют воздействие на общество с целью дестабилизировать обстановку внутри страны при помощи растущих возможностей информационных технологий» [16, с. 40]. В условия проведения специальной военной операции попытки деморализовать население участились. Как правило, деятельность таких служб направлена на провокацию массовых беспорядков, создания волнения в массах, негативного отношения к действующим органам власти и проводимой ими политике. В актуальной действительности выполнить поставленные цели сотрудники таких служб пытаются следующими способами: давление на жалость (рассказы о воздействии вооруженных сил на мирное население), призывы свергнуть власть (проведение митингов, восстаний, терактов), угрозы. Кроме того, посредством информации с личной страницы, комментариев и записей родственников, службы получают информацию о военнослужащих, находящихся в зоне действия спецоперации и используют ее в своих противоправных целях.

Обобщая все вышеизложенное, мы можем сделать следующие выводы.

Одной из актуальных проблем в рамках реализации правовой политики по обеспечению информационной безопасности является слабая защита персональных данных. Объяснить такое положение вещей, на наш взгляд, можно следующими обстоятельствами. Во-первых, граждане обладают низким уровнем информационной грамотности. В основном это касается лиц пожилого возраста, но и не только они передают свои данные в руки мошенникам. Во-вторых, в государственных органах имеет место быть коррупционная составляющая. Имеется вероятность, что за вознаграждение госслужащий может передать информационные базы, содержащие персональные данные, третьим лицам. В-третьих, низкая мотивация IT специалистов, вызывает отток профессиональных кадров, в результате чего наблюдается низкая эффективность технической системы информационной безопасности. В связи с этим, в первую очередь необходимо реализовать комплекс мероприятий, направленный на повышение информационной

грамотности населения. Также важно разъяснить населению значение сохранности своих персональных данных и вероятные последствия распространения такой информации.

Для повышения эффективности обеспечения безопасности несовершеннолетних в сети «Интернет» требуется комплексный подход. Необходимо прививать информационную грамотность с ранних лет. В первую очередь это должны быть правила информационного этикета (запрет на оскорбление других пользователей, запрет на переход по ссылкам, где стоит обозначение «18+» и так далее. Реализовать данные мероприятия можно в рамках курс «информатика», также можно ввести отдельные курсы «информационная безопасность в сети «Интернет». При этом важно отметить важность участия родителей в рамках повышения информационной грамотности и процессе обеспечения информационной безопасности детей в сети «Интернет». В первую очередь необходимо использовать механизмы технического контроля (родительский контроль, детский аккаунт, привязанный к родительскому и так далее). Вполне возможно было бы перенести систему семейных аккаунтов на сим-карты. То есть, приобретая сим-карту ребенку, родитель может контролировать его звонки, исходящий трафик в сети «Интернет» и другие взаимодействия посредством использования устройства. Кроме того, нам кажется, вполне логичным обязать крупные социальные сети требовать верификацию по паспорту. При его отсутствии или же возрасте пользователя до 16 лет, профиль должен быть ограничен в функционале в части посещения отдельных сообществ. Например, можно проводить проверку сообществ и ставить на них отметку «доступно для детей младше шестнадцати лет». Это позволит ограничить взаимодействие с вредоносной информацией. Кроме того, действия такого пользователя должны отслеживаться администраторами сайта (проверка комментариев, взаимодействие с другими пользователями и так далее).

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. Можно сделать вывод, что определение информационной безопасности, предусмотренное соответствующей доктриной, в целом раскрывает основные характеристики рассматриваемой категории и не требует внесения существенных изменений. Отдельно нами было обращено внимание, что информационная безопасность может быть рассмотрена в двух аспектах. С одной стороны информационная безопасность направлена на защиту охраняемой законом информации от противоправного завладения, использования, распространения. Такими сведениями является информация отнесенная законом к категории государственная тайна, коммерческая тайна, тайна частной жизни и так далее. С другой стороны информационная безопасность направлена на достижение состояния защищенности от вредоносной информации. Вредоносная информация характеризуется тем, что ее распространение потенциально несет вред или опасность общественным отношениям. В ходе проведенного исследования нами были предложены следующие изменения в законодательстве.

Одной из актуальных проблем в рамках реализации правовой политики по обеспечению информационной безопасности является слабая защита персональных данных. Объяснить такое положение вещей, на наш взгляд, можно следующими обстоятельствами. Во-первых, граждане обладают низким уровнем информационной грамотности. В основном это касается лиц пожилого возраста, но и не только они передают свои данные в руки мошенникам. Во-вторых, в государственных органах имеет место быть

коррупционная составляющая. Имеется вероятность, что за вознаграждение госслужащий может передать информационные базы, содержащие персональные данные, третьим лицам. В-третьих, низкая мотивация IT специалистов, вызывает отток профессиональных кадров, в результате чего наблюдается низкая эффективность технической системы информационной безопасности. В связи с этим, в первую очередь необходимо реализовать комплекс мероприятий, направленный на повышение информационной грамотности населения. Также важно разъяснить населению значение сохранности своих персональных данных и вероятные последствия распространения такой информации.

Отдельное внимание в ходе данного исследования было уделено вопросам безопасности несовершеннолетних в интернет пространстве. Для повышения эффективности обеспечения безопасности несовершеннолетних в сети «Интернет» требуется комплексный подход. Необходимо прививать информационную грамотность с ранних лет. В первую очередь это должны быть правила информационного этикета (запрет на оскорбление других пользователей, запрет на переход по ссылкам, где стоит обозначение «18+» и так далее. Реализовать данные мероприятия можно в рамках курс «информатика», также можно ввести отдельные курсы «информационная безопасность в сети «Интернет». При этом важно отметить важность участия родителей в рамках повышения информационной грамотности и процессе обеспечения информационной безопасности детей в сети «Интернет». В первую очередь необходимо использовать механизмы технического контроля (родительский контроль, детский аккаунт, привязанный к родительскому и так далее). Вполне возможно было бы перенести систему семейных аккаунтов на сим-карты. То есть, приобретая сим-карту ребенку, родитель может контролировать его звонки, исходящий трафик в сети «Интернет» и другие взаимодействия посредством использования устройства. Кроме того, нам кажется, вполне логичным обязать крупные социальные сети требовать верификацию по паспорту. При его отсутствии или же возрасте пользователя

до 16 лет, профиль должен быть ограничен в функционале в части посещения отдельных сообществ. Например, можно проводить проверку сообществ и ставить на них отметку «доступно для детей младше шестнадцати лет». Это позволит ограничить взаимодействие с вредоносной информацией. Кроме того, действия такого пользователя должны отслеживаться администраторами сайта (проверка комментариев, взаимодействие с другими пользователями и так далее).

Нам кажется возможным в нынешних реалиях рассмотреть возможность создания специализированного органа, деятельность которого будет полностью направлена на обеспечение информационной безопасности. В частности к его полномочиям могут быть отнесены: контроль за распространением ложной информации, которая подрывает интересы Российской Федерации, нарушает права и свободы человека, а также наносит вред духовным и нравственным ориентирам общества (культура, история и так далее); противодействие организациям, созданным иностранными государствами, чья деятельность направлена на реализацию информационно-психологического воздействия на население Российской Федерации; мониторинг за наиболее актуальными темами и обращение в соответствующие органы за получением оперативных разъяснений по тем или иным вопросам (например, в ситуации с короновирусной инфекцией при помощи деятельности данного органа удалось бы оперативно противодействовать ложной информации о ее распространении, путем публикации заявлений министерства здравоохранения относительно тех или иных данных, являющихся предметом обсуждения населения). Можно утверждать, что указанные полномочия уже относятся к компетенции различных органов власти, но создание единого органа способствовало повышению оперативности в вопросах противодействия угрозам информационной безопасности.

В целях совершенствования правовой политики по вопросам информационной безопасности, нами были разработаны следующие рекомендации.

Уголовный состав неправомерного отказа в предоставлении информации отличается от аналогичного административного состава тем, что в Уголовном кодексе есть указание на последствия в виде вреда правам и законным интересам граждан. Оправданным будет весьма скептическое отношение к подобной формулировке, мы считаем ее неудачной, поскольку совершение любого правонарушения причиняет вред правам и законным интересам граждан. Для решения указанной проблемы мы рекомендуем два альтернативных способа. Во-первых, можно изменить формулировку «вред правам и законным интересам граждан» и указать конкретные последствия, которые должны последовать после неправомерного отказа для квалификации по указанной статье Уголовного кодекса. Во-вторых, можно исключить статью 5.39 из кодекса об административных правонарушениях и оставить только статью 140 Уголовного кодекса, исключив из ее редакции слова «вред правам и законным интересам граждан». Поскольку сам по себе неправомерный отказ несет вред правам и законным интересам, а наличие двух идентичных по своей сути статей в разных нормативно-правовых актах создает трудности при осуществлении правоприменителем деятельности, направленной на квалификацию деяния.

На наш взгляд, необходимо исключить статью 13.15 из Кодекса об административных правонарушениях и закрепить, предусмотренные ей конструкции в качестве отдельных, самостоятельных составов административных правонарушений. Нет никакой сложности в том, чтобы закрепить новое правонарушение в качестве самостоятельной статьи, а не заполнять постоянно одну статью новыми противоправными деяниями, которые, по мнению законодателя, являются проявлениями злоупотребления свободой массовой информации.

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. Александрова А.В., Образумов Е.И. Информационная безопасность и конституционные права личности // Наука. Общество. Государство. 2021. №1 (33). С. 63-70.
3. Али М.З. Ограничение доступа к информационным ресурсам в сети интернет (практические проблемы признания информации запрещенной к распространению) // Право в сфере интернета. 2018. №1. С. 104-118.
4. Артамонова Я.С. К вопросу о понятии «Информационная безопасность» // Социально-гуманитарные знания. 2018. №1. С. 319-321.
5. Баринов С.В. О правовом определении понятия «Информационная безопасность личности» // Актуальные проблемы российского права. 2016. №4 (65). С. 97-105.
6. Батаева И.П. Защита информации и информационная безопасность // НиКа. 2012. №1. С. 116-118.
7. Безручко Е.В., Рысай Б.Г. Некоторые проблемы административной ответственности в сфере связи и информации // ЮП. 2020. №1(92). С. 180-185.
8. Бецков А.В. О некоторых аспектах правового обеспечения информационной безопасности // Академическая мысль. 2018. №3 (4). С. 41-43.
9. Васютин А.А. Интернет-цензура как угроза свободе слова и информации в Российской Федерации // Конституционные права и свободы человека и гражданина в РФ: проблемы реализации и защиты: Материалы межвузовского студенческого круглого стола, Иркутск, 27 ноября 2015 года.

Иркутск: Иркутский институт (филиал) ВГУЮ (РПА Минюста России). 2016. №1. С. 5-9.

10. Вепренцева Т.А. Актуальные проблемы правового обеспечения информационной безопасности Российской Федерации // Национальная безопасность. 2022. №2. С. 59-73.

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

12. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 №51-ФЗ (ред. от 25.02.2022) // СЗ РФ. 1994. №32. Ст. 3301.

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

14. Гребеньков А.А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica. 2018. №4(137). С. 108-120.

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

16. Ежевская Т.И. Психологическое воздействие информационной среды на современного человека // Психопедагогика в правоохранительных органах. 2019. №2. С. 38-41.

17. Ефремова М. А. Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений // Вестник Казанского юридического института МВД России. 2015. №1 (19). С. 55-58.

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

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

20. Клименко С.Н. К вопросу о юридической ответственности за нарушения законодательства Российской Федерации в области информационной безопасности: проблемы, перспективы // Управленческое консультирование. 2015. №10(82). С. 87-94.

21. Кодекс административного судопроизводства Российской Федерации от 08.03.2015 №21-ФЗ (ред. от 11.06.2022) // СЗ РФ. 2015. №10. Ст. 1391.

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

23. 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.

24. 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.

25. Кулавская Ю.Е. Принципы обеспечения информационной безопасности // E-Scio. 2021. №5(56). С. 252-256.

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

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

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

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

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

31. 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.

32. Савоськин А.В. «Обращения граждан» как правовая категория // Антиномии. 2017. №3. С. 85-99.

33. 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.

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

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

36. Синцов Г.В., Феоктистов Д.Е. Свобода мысли и слова в контексте противодействия информационному экстремизму // Известия ВУЗов. Поволжский регион. Общественные науки. 2018. №4(48). С. 15-21.

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

38. Трудовой кодекс Российской Федерации от 30.12.2001 №197-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2002. №1. Ст. 3.

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

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

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

42. 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.

43. Указ Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») // СЗ РФ. 2015. № 21. Ст. 3092.

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

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

46. 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.

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

48. 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.

49. Федеральный закон «Об оперативно-розыскной деятельности» от 12.08.1995 №144-ФЗ (ред. от 28.06.2022) // СЗ РФ. 1995. №33. Ст. 3349.

50. 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.

51. Федеральный закон «О государственной гражданской службе Российской Федерации» от 27.07.2004 №79-ФЗ (ред. от 30.12.2021) // СЗ РФ. 2004. №31. Ст. 3215.

52. Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2004. №32. Ст. 3283.

53. Федеральный закон «О противодействии экстремистской деятельности» от 25.07.2002 №114-ФЗ (ред. от 14.07.2022) // СЗ РФ. 2002. №30. Ст. 3031.

54. Филиппов В.М., Насонкин В.В., Папачараламбоус Ч. Права и интересы детей в информационной сфере: реформирование законодательства // Вестник СПбГУ. Серия 14. Право. 2019. №2. С. 362-372.

55. 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.

56. Ширкин А.А., Ерашова О.С. Совершение деяния, подразумевающего клевету в сети Интернет. Проблемы доказывания и исчисления срока давности // Закон и право. 2019. №5. С. 107-109.

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

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

59. Юсупов М.З. О влиянии информационно-коммуникационных технологий на обеспечение национальной безопасности в условиях формирования информационного общества // Открытое образование. 2010. №1. С. 78-85.

60. Global Digital 2022 ежегодный отчет об интернете и социальных сетях // [Электронный ресурс]. - https://www.sostav.ru (дата обращения 01.10.2022)