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 О.А. Кананыкина
(Инициалы Фамилия) (личная подпись)

Руководитель канд. юрид. наук, доцент А.А. Мусаткина
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Актуальность темы исследования обусловлена тем, что на сегодняшний день на общество оказывается активное информационное влияние со стороны других государств с целью дестабилизировать обстановку внутри страны. В этих условиях вопросы обеспечения информационной безопасности приобретают особую значимость и требуют дополнительного исследования в целях выработки мер, направленных на совершенствование механизмов обеспечения информационной безопасности.

Объектом выпускного исследования являются общественные отношения, складывающиеся по поводу обеспечения информационной безопасности в Российской Федерации.

Предмет выпускного исследования – нормы отечественного законодательства, а также научные публикации и материалы судебной практики, способствующие всестороннему исследованию вопросов обеспечения информационной безопасности в Российской Федерации.

Цель выпускного исследования заключается в формировании целостного представления о механизмах обеспечения информационной безопасности в Российской Федерации.

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

Оглавление

Введение

За последние десятилетия с учетом развития технологий и повышения уровня их доступности резко возросло число активных пользователей сети интернет. Высокий спрос на получение информации в сети «Интернет» породил не менее высокое предложение. В сети с каждым годом растет число интернет-изданий, новостных блогеров и сообществ, которые размещают различную информацию для свои подписчиков. В этих условиях особое значение обрело обеспечение информационной безопасности, поскольку уполномоченные лица и органы не всегда обладают необходимыми полномочиями для предотвращения информационной угрозы. Задача осложняется, в том числе, и тем обстоятельством, что деятельность субъектов по обеспечению информационной безопасности должна соответствовать принципам демократического государства, одним из которых является полный запрет какой-либо цензуры. Все это в совокупности создает определенные сложности, которые препятствуют и в определенные моменты делают попросту невозможной обеспечение информационной безопасности.

Актуальность темы исследования обусловлена тем, что на сегодняшний день на общество оказывается активное информационное влияние со стороны других государств с целью дестабилизировать обстановку внутри страны. В этих условиях вопросы обеспечения информационной безопасности приобретают особую значимость и требуют дополнительного исследования в целях выработки мер, направленных на совершенствование механизмов обеспечения информационной безопасности.

В доктрине обеспечения информационной безопасности отмечается, что специальные службы враждебно настроенных государств осуществляют воздействие на общество с целью дестабилизировать обстановку внутри страны при помощи растущих возможностей информационных технологий. На сегодняшний день указанная угроза приобрела еще большую

актуальность в условиях проведения специальной военной операции. На население Российской Федерации активное воздействие в интернете оказывает ЦИПсО. Это специальное подразделение, целью которого является проведение психологических атак на противника. Так, в условиях частичной мобилизации действия ЦИПсО были направлены на то, чтобы вызвать панику и волнения среди населения. В результате проведенных атак массовые беспорядки были замечены в южных регионах России, а также увеличилось число граждан мужского пола, которые покинули территорию страны.

Объектом выпускного исследования являются общественные отношения, складывающиеся по поводу обеспечения информационной безопасности в Российской Федерации.

Предмет выпускного исследования – нормы отечественного законодательства, а также научные публикации и материалы судебной практики, способствующие всестороннему исследованию вопросов обеспечения информационной безопасности в Российской Федерации.

Цель выпускного исследования заключается в формировании целостного представления о механизмах обеспечения информационной безопасности в Российской Федерации.

Определив цель выпускного исследования, мы можем выделить следующие задачи необходимые для ее реализации:

– рассмотреть общие положения системы обеспечения национальной безопасности в Российской Федерации;

– изучить понятие и признаки информационной безопасности в отечественном праве;

– проанализировать конституционно-правовые основы обеспечения информационной безопасности в Российской Федерации;

– изучить организационные основы обеспечения информационной безопасности;

– рассмотреть вопросы привлечения к ответственности за совершение правонарушений в сфере обеспечения информационной безопасности;

– выявить актуальные проблемы обеспечения информационной безопасности в Российской Федерации.

Теоретическую базу исследования составляют работы следующих ученых юристов: Ф.А. Азимов, М.Г. Адылханов, И.Р. Аминов, Я.С. Артамонова, А.И. Ахметов, С.В. Баринов, Е.В. Безручко, А.А. Васютин, М.С. Власенко, Е.В. Емельянова, М.А. Ефремова, С.В. Казанцев, Н.Е. Колобаева, С.В. Корнакова, А.П. Кочетков, Ю.Е. Кулавская, В.А. Мазуров, О.М. Манжуева, Л.С. Михайлова, Н.А. Молчанов, А.Я. Неверов, С.Э. Несмеянова, К.Д. Озимко, А.В. Петрянин, В.А. Плотников, А.В. Понеделков, А.И. Пономарев, Е.В. Пономаренко, Б.Г. Рысай, Д.Е. Свистунов, А.В. Степанов, Л.К. Терещенко, Ш.Г. Утарбеков, А.Д. Чесноков, Г.И. Шахворостов, А.В. Шободоева.

Нормативную базу выпускного исследования составляют следующие акты: Конституция Российской Федерации, Закон Российской Федерации «О государственной тайне», Закон Российской Федерации «О средствах массовой информации», Кодекс Российской Федерации об административных правонарушениях, Семейный кодекс Российской Федерации, Трудовой кодекс Российской Федерации, Уголовный кодекс Российской Федерации, Уголовно-процессуальный кодекс Российской Федерации, Федеральный закон «Об архивном деле в Российской Федерации», Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон «Об информации, информационных технологиях и о защите информации», Федеральный закон «Об оперативно-розыскной деятельности», Федеральный закон «Об основах охраны здоровья граждан в Российской Федерации», Федеральный закон «О государственной гражданской службе Российской Федерации», Указ Президента Российской Федерации «Об утверждении Доктрины информационной безопасности

Российской Федерации», Указ Президента Российской Федерации «Об утверждении Перечня сведений, отнесенных к государственной тайне», Указ Президента Российской Федерации «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.

Глава 1 Понятие, признаки и место информационной безопасности в системе интересов национальной безопасности

1.1 Общие положения системы обеспечения национальной безопасности в Российской Федерации

С момента возникновения государства одной из основных стоящих перед ним задач являлась защита от внешних и внутренних угроз. На сегодняшний день охрана национальной безопасности определяется применением различных методов и средств. Осложняет процесс обеспечения национальной безопасности тот факт, что вся система ее обеспечения должна быть «гибкой» и соответствовать тем или иным актуальным реалиям. Например, в действующих условиях, в которых находится Российская Федерация, важно уделять внимание не только военной безопасности, но и информационной безопасности, поскольку при помощи той или иной информации возможно влияние на сознание граждан и дестабилизации ситуации внутри государства. Другой проблемный аспект обеспечения национальной безопасности заключается в соотношении применяемых мер и допустимости ограничения прав и свобод. Можно отметить, что на сегодняшний день обеспечение национальной безопасности является приоритетным вопросом, как в контексте глобального характера, так и в рамках конкретного государства. Особенно остро данный вопрос стоит в актуальных условиях проведения специальной операции и назревающего экономического кризиса в России.

Основы обеспечения безопасности в Российской Федерации определяются Федеральным законом «О безопасности». Однако в указанном нормативно-правовом акте отсутствует понятие национальной безопасности, а также не рассматриваются его основные составные элементы. Относительно данного обстоятельства в научной литературе можно встретить различные точки зрения. Так, А.В. Степанов утверждает, что «в

отсутствие законодательного закрепления механизмов национальной безопасности система мер по ее обеспечению не будет иметь необходимой эффективности. Законодателю необходимо закрепить такие понятия как «национальная безопасность», «национальные интересы», «система обеспечения национальной безопасности». Нынешнее положение вещей указывает на то обстоятельство, что законодатель относится к данному вопросу без должного внимания» [36, с. 76]. Стоит обратить внимание, что не все ученые согласны с данной точкой зрения и не видят необходимости закрепления в Федеральном законе «О безопасности» перечисленных выше понятий. Например, А.П. Кочетков, рассматривая данный вопрос, говорит о том, что «понятие «национальная безопасность» является слишком абстрактным и размытым, поэтому его включение в федеральное законодательство не возымеет того эффекта, о котором пишут сторонники первой точки зрения. Автор отмечает, что использование рассматриваемой категории подходит больше для научного анализа, конференций и дискуссий, но не для законодательной базы» [20, с. 26].

В свою очередь, обращаясь к статье первой Федерального закона «О безопасности», мы видим, что законодатель перечисляет основные виды безопасности (например: государственная безопасность, экологическая безопасность), а по завершению перечисления указывает, что далее по тексту совокупность указанных действий обобщенно будет именоваться как безопасность или национальная безопасность. Другими словами, законодатель отождествляет указанные понятия, поскольку «ставит их в один ряд». Причем мы видим, что при его использовании законодатель ограничивается одним лишь перечислением его структурных элементов, оставляя без внимания иные сущностные признаки рассматриваемой категории. Учитывая фундаментальное значение категории «национальная безопасность» для Федерального закона «О безопасности», на наш взгляд, не совсем корректным является отсутствие в положениях ее законодательной дефиниции. Ввиду всего вышесказанного, мы придерживаемся точки зрения,

что в тексте Федерального закона «О безопасности» необходимо отразить содержания понятия «национальная безопасность», так как, законодатель использует понятия «безопасность» и «национальная безопасность» в качестве тождественных, но при этом не раскрывает ни одно из них в тексте закона.

В свою очередь легальное закрепление понятия «национальная безопасность» имеет место быть в подзаконном нормативном правовом акте. Представленное в Стратегии национальной безопасности определение рассматриваемого понятия выглядит следующим образом: «состояние защищенности от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны» [44]. Однако далеко не все ученые-юристы согласны с представленной формулировкой и предлагают свои авторские определения.

Так, С.Е. Свистунов раскрывая понятие национальной безопасности следующим образом: «состояние, которое обеспечивает благоприятные условия для развития личности, общества и государства и ограничивает любую возможность возникновения угроз национальным интересам страны» [34, с. 80]. Мы считаем, что такое определение не отражает наиболее значимые признаки исследуемого понятия, поэтому не характеризует национальную безопасность в достаточной степени.

Более подробное определение дается А.Я. Неверовым, который понимает национальную безопасность следующим образом. «Качественное и количественное состояние российского общества, государства, его граждан, российских народов и всего многонационального народа, которая находит свое отражение в закрепленной в законе согласованности их интересов, защищенных от внешних и внутренних угроз» [26, с. 90]. Несмотря на попытку создать расширенное определение, которое отражает все аспекты

категории «национальная безопасность», автор избыточно использует абстрактные термины по типу «качественное состояние» или «согласованность интересов». Такой подход не позволяет достичь какой-либо конкретики. Скорее наоборот создает еще больше возможностей для вольного толкования.

На фоне рассмотренных выше определений куда более полным и конкретным выглядит дефиниция, предложенная С.В. Казанцевым. В его понимании «национальная безопасность - состояние государства, которое характеризуется отсутствием или своевременной нейтрализацией внешних и внутренних угроз ее единству, а также обеспечением защиты наиболее значимых интересов общества и государственной власти» [15, с. 9]. Следует обратить внимание, что существенное упущение данного определения заключается в том, что автор акцентирует внимание исключительно на защите интересов общества и государства, оставляя без внимания охрану основных интересов человека. На наш взгляд, такой подход не совсем корректен, поскольку национальная безопасность обеспечивает охрану интересов не только общества и государства, но и охрану интересов личности в частности.

Куда более схоже с легальным определением вариант, предложенный А.В. Шободаевым. «Национальная безопасность представляет собой состояние защищенности интересов личности, общества и государства» [54, с. 17]. Анализируя представленное определение, мы можем отметить, что оно представляет собой сокращенную версию легального определения понятия «национальная безопасность».

В целом можно отметить, что легальная конструкция, предусмотренная Указом Президента, является наиболее полной и отражает основные сущностные признаки рассматриваемой категории. Далее необходимо рассмотреть признаки национальной безопасности, предусмотренные легальным определением.

В Стратегии национальная безопасность определяется как конкретное состояние. В научной литературе указанный признак подвергается критике среди отдельных исследователей. Так, А.В. Степанов акцентирует внимание на следующем обстоятельстве. «Состояние» означает статичное положение, однако государство, активно действует, а не пассивно следит за состоянием защищенности [37, с. 10]. На наш взгляд, с данной точкой зрения сложно согласиться. Национальная безопасность является, своего рода, конечной целью, то есть, именно к этому состоянию защищенности государство стремится, реализуя совокупность конкретных мероприятий. Для достижения указанной цели принимаются соответствующие нормативно-правовые акты, а государственными органами и должностными лицами предпринимаются определенные действия. Соответственно, государство не находится в статичном состоянии, наоборот, субъекты обеспечения национальной безопасности постоянно осуществляют ту или иную деятельность для того, чтобы достичь состояния национальной безопасности.

Исходя из этимологического значения категории «национальная безопасность», следует не оставлять без внимания важное для нее понятие «нация». Необходимо понимать, что данное понятие можно рассматривать с различных позиций, например, с философской или этнической точек зрения. При этом в контексте данной работы наибольший интерес для нас представляет понятие нация с юридической точки зрения. В этом случае нация представляет собой «совокупность граждан одного государства». Это понятие можно рассматривать как определение нации в узком смысле. Если же раскрывать его более развернуто, то нация есть единство общества и государства, где общество является составной частью, а государство является стержнем, основой нации.

Далее стоит отметить, что национальная безопасность представляет собой состояние защищенности от конкретных негативных факторов, а именно, от внутренних и внешних угроз. В контексте исследуемого определения угроза выступает непосредственное или готовящееся

посягательство на отношения, входящие в объект защиты национальной безопасности. «К внешним необходимо отнести такие глобальные проблемы, как военная угроза, финансовые риски, место России в международной системе разделения труда (опасность остаться сырьевой державой), наркотрафик, незаконная торговля оружием, глобальное изменение климата и другие. Внутренние факторы угроз национальной безопасности можно классифицировать по разным основаниям. Если говорить о внутренних ресурсах страны и их безопасности, то можно перечислить экологическую, энергетическую безопасность природных ресурсов; технологическую безопасность материально-технических ресурсов; информационную безопасность - информационных ресурсов; финансовую безопасность в области финансовых ресурсов страны. И одна из наиболее болезненных проблем России - социально-экономическая безопасность, обеспечиваемая сохранением человеческого капитала (демография, здоровье нации, ее духовный потенциал, образование, культура)» [31, с. 110].

Говоря об угрозах национальной безопасности, следует обратить внимание и на те отношения, которые охраняются посредством обеспечения национальной безопасности. В этой связи стоит обратиться к Стратегии национальной безопасности, где перечислены стратегические национальные приоритеты. В их число входят:

– «сбережение народа и развитие человеческого потенциала;

– оборона государства;

– государственная и общественная безопасность;

– информационная безопасность;

– экономическая безопасность;

– научно-технологическое развитие;

– экологическая безопасность;

– защита духовно-нравственных ценностей, культуры и исторической памяти;

– стратегическая стабильность и взаимовыгодное международное сотрудничество» [44].

Стоит обратить внимание, что на первое место среди всех приоритетов вынесено «сбережение народа и общественного потенциала», а уже только за ним располагается оборона государства и его безопасность. На наш взгляд, подобный порядок перечисления обусловлен тем, что Конституция провозглашает человека, его права и свободы высшей ценностью. Именно поэтому в Стратегии на первое место выходит именно этот приоритет, тем самым, свидетельствуя о том, что отечественная нормативно-правовая база соответствует принципам демократизма и гуманизма.

Несмотря на то обстоятельство, что в действующей Стратегии определены основные вопросы обеспечения национальной безопасности, а также конкретизированы специфические особенности обеспечения отдельных видов безопасности (экономическая безопасность, экологическая безопасность и так далее), отдельные исследователи обращают внимание, что предыдущая Стратегия была более проработанной. Среди ее преимуществ в научной литературе выделяют следующие факторы:

– «стратегия определяла национальные приоритеты, раскрывала механизмы совместной работы органов государственной власти при обеспечении национальной безопасности и регламентировалась процедура выявления угроз национальной безопасности. Совокупность указанных положений позволяла выявить критерии, при помощи которых можно было определить актуальное состояние национальной безопасности» [1, с. 80];

– «стратегия задала конкретное направление деятельности, а именно, «возвращение статуса мировой державы, осуществление устойчивого развития страны, сохранение территориальной целостности и суверенитета» [30, с. 115];

– «концепцией не были учтены многие направления безопасности, в том числе, осталась без внимания идеология государства, регламентация деятельности субъектов. Концепция имеет больше декларативный характер и

не может полноценно способствовать реализации задач по обеспечению национальной безопасности» [25, с. 30];

– «стратегия объединяла вопросы внешней политики, безопасность и военную политику с вопросами внутреннего развития государства, таким образом, создавалось взаимозависимость и устойчивое взаимодействие между национальной безопасностью и развитием государства» [32, с. 47];

– «стратегия рассматривала обеспечение национальной безопасности посредством достижения высокого уровня социально-экономического развития государства. Именно рост уровня жизни граждан, развития науки и техники, улучшение качества образования рассматривались в качестве одних из основных условий обеспечения национальной безопасности» [11, с. 12].

Среди перечисленных выше отличий, на наш взгляд, наибольшую проблему составляет отсутствие детализированности при регламентации вопросов взаимодействия между субъектами обеспечения национальной безопасности, а также непосредственно самой процедуры выявления негативных факторов, которые создают угрозу стабильности национальной безопасности. Отсутствие конкретики по данным вопросам в основополагающем акте для всей нормативно-правовой базы по обеспечению национальной безопасности препятствует эффективной реализации данного процесса. Поскольку реализация любых правовых средств требует в первую очередь наличие устойчивой нормативно-правовой базы, которая бы исключала любые пробелы и коллизии юридических норм.

Следует также отметить, что действующая Стратегия позволила ученым-юристам выделить следующие структурные элементы системы национальной безопасности. В их число входят:

– «государственную безопасность;

– общественную безопасность;

– информационная безопасность;

– экологическая безопасность;

– экономическая безопасность;

– транспортная безопасность;

– энергетическая безопасность;

– безопасность личности» [4, с. 200].

Каждый из элементов имеет одинаковое значение и в его отсутствии невозможно говорить о достижении состояния национальной безопасности. Представленная совокупность элементов позволяет нам сделать вывод, что каждый из них сопутствует категориям безопасность личности, безопасность общества и безопасность государства. При этом не имеет значения, о каком именно виде безопасности идет речь, каждый из них обеспечивает безопасность всех трех компонентов (личности, общества, государства). Среди перечисленных элементов однозначно нельзя выделить какой-то один и заявить, что он имеет приоритет над остальными. Однако мы можем отметить, что при определенных обстоятельствах, те или иные элементы приобретают особую важность и требуют дополнительного внимания и ресурсов. Например, в условиях обостренной внешней политики особого внимания заслуживает государственная и экономическая безопасность. В нынешних условиях агрессии со стороны европейских государств и применения ими пропагандистских методов воздействия на граждан Российской Федерации, особое значение приобретает обеспечение информационной безопасности, о которой мы подробно поговорим в следующем параграфе.

1.2 Понятие и признаки информационной безопасности

За последние десятилетия с учетом развития технологий и повышения уровня их доступности резко возросло число активных пользователей сети интернет. По данным опроса, проведенным ВЦИОМ в конце 2021 года, одним из основных источников информации для граждан стал интернет. Примерно 42% граждан ответили, что узнают новости и другую информацию

из социальных сетей, блогов и новостных сайтов [28]. Увеличение числа пользователей свидетельствует о том, что увеличился рост спроса на получение информации. Высокий спрос породил не менее высокое предложение. В сети с каждым годом растет число интернет-изданий, новостных блогеров и групп, которые размещают различную информацию для свои подписчиков. В этих условиях особое значение обрело обеспечение информационной безопасности, поскольку уполномоченные лица и органы не всегда обладают необходимыми полномочиями для предотвращения информационной угрозы. Задача осложняется, в том числе, и тем обстоятельством, что деятельность субъектов по обеспечению информационной безопасности должна соответствовать принципам демократического государства, одним из которых является полный запрет какой-либо цензуры. Все это в совокупности создает определенные сложности, которые препятствуют и в определенные моменты делают попросту невозможной обеспечение информационной безопасности.

В первую очередь необходимо рассмотреть понятие исследуемой категории и определить, что следует понимать под «информационной безопасностью» в современных отечественных реалиях. Легальное определение понятия «информационная безопасность» мы можем найти, обратившись к Указу Президента Российской Федерации «Об утверждении Доктрины информационной безопасности Российской Федерации». В документе исследуемое понятие раскрывается следующим образом: «информационная безопасность - 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» [42]. В целом можно отметить, что указанное понятие практически полностью идентично понятию «национальная безопасность»,

которое было детально рассмотрено нами в предыдущем параграфе. Небольшие отличия связаны со спецификой термина, так, акцентируется внимание именно на информационных угрозах. Безусловно, «национальная безопасность» и «информационная безопасность» сопоставляются между собой как целое и часть, как родовые и видовые понятия. Именно этим можно объяснить их практически полную идентичность. При этом возникает вопрос о необходимости включение в структуру данного понятия какого-либо другого сущностного признака, отражающего специфику информационной безопасности. Для того чтобы ответить на него, мы обратимся к работам ученых-юристов, исследовавших понятие и признаки информационной безопасности.

А.Д. Чесноков определяет информационную безопасность как «невозможность причинения вреда свойствам объекта безопасности, которые обусловлены информацией и информационной инфраструктурой» [52, с. 485]. На наш взгляд, представленное определение является слишком лаконичным. Кроме того, автором акцентируется внимание именно на защите объектов безопасности, в то время как при определении информационной безопасности, как структурного элемента национальной безопасности, следует говорить в первую очередь о защите личности, общества и государства.

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» [3, 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. Однако стоит заметить, что автор уводит на второй план аналогичную потребность государства, что на наш взгляд не совсем корректно. Ранее мы уже отмечали, что национальная безопасность, равно как и информационная безопасность, одинаково обеспечивается для человека, общества и государства. Поэтому, мы придерживаемся мнения, что определенно стоило учесть потребность государства и упомянуть его в рассмотренное нами определение.

В свою очередь при определении информационной безопасности В.А. Мазуров акцентирует внимание на другом аспекте – защите информации. По мнению автора, «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» [22, с. 59]. В данном определении автор уделяет внимание способам обеспечения информационной безопасности, отдавая предпочтение техническим средствам. Однако, рассматривая представленное определение с точки зрения юриспруденции, подход автора не совсем уместен, поскольку не уделяет внимание, скорее даже не рассматривает, применение правовых мер обеспечения информационной безопасности.

Рассмотренные определения позволили нам сделать вывод, что информационную безопасность можно рассматривать в двух основных направлениях. Во-первых, состояние защищенности информации от неправомерного завладения, использования, распространения. В этом случае, например, мероприятия направлены на охрану информации, составляющую тайну частной жизни, государственную или коммерческую тайну. Во-вторых, защита от информации, распространение которой может привести к негативным последствиям. Например, информация об игре «синий кит» привела к росту числа детский самоубийств, напротив, ложная информация о

короновирусной инфекции привела к панике среди населения и иным негативным последствиям.

Учитывая рассмотренные выше обстоятельства, можно раскрыть понятие информационной безопасности следующим образом. Информационная безопасность - состояние защищенности личности, общества и иных социальных групп, а также государства в лице государственных органов и должностных лиц от противоправного воздействия на охраняемую законом информацию, а также от информационного воздействия, которое может повлечь неблагоприятные последствия, при котором обеспечиваются реализация приоритетов, предусмотренных Стратегией национальной безопасности.

Обеспечение национальной безопасности, равно как и любая другая деятельность основана на специфических принципах. Принципы информационной безопасности представляет собой основополагающие начала, положения, идеи, которые лежат в основе обеспечения информационной безопасности. В научной литературе можно встретить следующие принципы обеспечения национальной безопасности.

Большинство ученых выделяют принцип обоснованности информационной безопасности [45, с. 34]. Данный принцип характеризуется тем, что применения мер информационной безопасности основывается на экспертной оценке необходимости ограничения информации. 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.

Отдельно в научной литературе выделяют принцип своевременности 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].

К числу рассматриваемой группы принципов можно также отнести принцип прогноза информационной безопасности. Его значение заключается в оценке потенциальных внешних и внутренних угроз и проработке возможных сценариев развития событий. Таким образом, путем реализации указного принципа удается выявить потенциальную угрозу информационной безопасности уже на стадии ее формирования. Прогноз обеспечения информационной безопасности осуществляется на основе сложившейся отечественной и зарубежной практики о работе специализированных органов по предотвращению угроз информационной безопасности, а так же апробации научных разработок в различных областях науки, особенно в сфере возможностей электронно-вычислительных машин.

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.

Ю.Е. Кулаская в своем исследовании выделяет принцип глубокой защиты [21, с. 254]. Указанный принцип несколько схож с принципом прогноза обеспечения информационной безопасности. Он основывается на

прогнозировании ситуаций, когда механизмы защиты информации не сработали должным образом, либо их обошли и так далее. То есть, система мер обеспечения информационной безопасности не сработала должным образом, на этот случай должны быть предусмотрены механизмы глубокой защиты. Например, это может быть комплекс мер по оперативному выявлению нарушителя или минимизации негативных последствий противоправного посягательства.

Рассмотренные выше принципы имеют наиболее широкое распространение в научной литературе, однако их перечень не является исчерпывающим. Так, к принципам информационной безопасности в первую очередь мы можем отнести общеправовые принципы, такие как: законность, приоритет прав и свобод человека и так далее. В эту же группу мы можем отнести принципы, перечисленные 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;

– ограничение доступа к информации только посредством федерального законодательства;

– открытость сведений о работе государственных органов и органов местного самоуправления;

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

– достоверность информации» [48].

В целом можно отметить, что система принципов обеспечения информационной безопасности построена вокруг соблюдения и охраны прав и законных интересов граждан. Что является особенно важным, при определении принципов информационной безопасности

законодатель уделяет особое внимание прогнозированию и выявлению возможных угроз еще на первоначальных этапах их формирования. При этом объективно принимается во внимание, что сама система мер обеспечения информационной безопасности неидеальна, поэтому в ее основу закладывается принцип глубокой защиты, определяющий меры воздействия на угрозу, уже причинившую определенный вред объектам охраны информационной безопасности.

Проанализировав принципы информационной безопасности, мы ни разу не встретили упоминания об анонимности в сфере обеспечения информационной безопасности. Соответственно, можно сделать вывод, что анонимность не является элементом системы обеспечения информационной безопасности. Однако нельзя отрицать, что она является одним из условий, при которых реализуются меры и осуществляет функционирование сама система информационной безопасности. Анонимность имеет настолько дискуссионный характер, что она указывается в Стратегии в качестве одного из проблемных аспектов обеспечения информационной безопасности. Ее негативное воздействие обусловлено тем, что с ее помощью облегчается совершение преступлений и в целом создаются благоприятные условия для повышения латентности определенных преступлений. С другой стороны, пользователями сети Интернет анонимность рассматривается как один из инструментов реализации права на свободу слова. Так, при помощи анонимных аккаунтов гражданин может выразить недовольство относительно неправомерных действий тех или иных лиц (например: главы администрации городского округа) и привлечь внимание общественности и вышестоящих органов. Именно указанными обстоятельствами можно объяснить дискуссионный характер анонимности.

Завершая обсуждение по теме данной главы, нами были сделаны следующие выводы. Одним из основных структурных элементов системы национальной безопасности является информационная безопасность. В федеральном законодательстве отсутствует легальное определение понятия

«информационная безопасность». Информационную безопасность можно рассматривать в двух основных направлениях. Во-первых, состояние защищенности информации от неправомерного завладения, использования, распространения. В этом случае, например, мероприятия направлены на охрану информации, составляющую тайну частной жизни, государственную или коммерческую тайну. Во-вторых, защита от информации, распространение которой может привести к негативным последствиям. В-третьих, анализ научной литературы позволил нам уточнить и дополнить легальное определение понятия «информационная безопасность». Информационная безопасность - состояние защищенности личности, общества и иных социальных групп, а также государства в лице государственных органов и должностных лиц от противоправного воздействия на охраняемую законом информацию, а также от информационного воздействия, которое может повлечь неблагоприятные последствия, при котором обеспечиваются реализация приоритетов, предусмотренных Стратегией национальной безопасности. В-четвертых, система принципов обеспечения информационной безопасности построена вокруг соблюдения и охраны прав и законных интересов граждан. Что является особенно важным, при определении принципов информационной безопасности законодатель уделяет особое внимание прогнозированию и выявлению возможных угроз еще на первоначальных этапах их формирования. В-пятых, одной из основных угроз информационной безопасности является анонимность в сети «Интернет», осуществляемая посредством специальных технических средств.

Глава 2 Механизм обеспечения информационной безопасности

2.1 Конституционно-правовые гарантии обеспечения информационной безопасности

Права и обязанности граждан в информационной сфере регулируются различными нормативно-правовыми актами. Основу правового статуса граждан в контексте информации и обеспечения информационной безопасности составляют положения, закрепленные в Конституции Российской Федерации. В первую очередь необходимо обратить внимание на часть четвертую статьи 29 основного закона. В ней установлено: «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом» [19]. При этом законодатель сразу делает оговорку и вводит понятие государственной тайны. То есть, конституционное право на свободный поиск, получение и передачу информации могут быть ограничены в зависимости от того, о какой именно информации идет. Используемое законодателем понятие «государственная тайна» раскрывается в статье второй Закона Российской Федерации «О государственной тайне». «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» [13]. Законодатель в определении перечисляет, какие виды сведений закон относит к государственной тайне, более того, в статье пятой рассматриваемого закона подробно раскрывается перечень таких данных. Например, военная государственная тайна включает в себя сведения о дислокации военных объектов и разработке военных технологий, а экономическая государственная тайна ограничивает доступ к сведениям о планах оборонных заказов и силах и средствах гражданской обороны.

Несмотря на то обстоятельство, что институт государственной тайны выступает в роли ограничения конституционного права граждан на свободный поиск, получение и распространение информации, сам он также ограничивается законодателем. Так, статья седьмая указанного закона содержит закрытый перечень сведений, которые не могут быть засекречены и отнесены к государственной тайне. К их числу законодатель относит информацию:

– «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)» [13].

Анализ представленного перечня позволяет нам сделать вывод, что указанная информация, так или иначе, затрагивает права и законные интересы граждан Российской Федерации. Именно по этой причине законодатель устанавливает уголовную, административную или дисциплинарную ответственность за засекречивание такой информации. Должностное лицо привлекается к ответственности в зависимости от степени вреда, причиненного обществу, государству или конкретному лицу такими действиями. Следует отметить, что в отдельных случаях госслужащие

напрямую не засекречивают информацию, но утаивают ее от граждан, не сообщают ее своевременно. Например, информация о возможных компенсациях и социальных гарантиях, как правило, сообщается не всегда, в таких случаях граждане остаются не осведомлены о возможности получить те или иные блага. Кроме того, стоит обратить внимание на формулировку «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам». Из ее содержания мы можем сделать вывод, что запрет на засекречивание такой информации распространяется только на привилегии, компенсации, гарантии, предоставляемые государством, то есть, органами государственной власти. Мы можем расширительно истолковать данное положение, поскольку государственная власть подразумевает федеральную государственную власть и государственную власть субъектов. Но даже в этом случае без внимания остаются меры социальной поддержки, предоставляемые из бюджета муниципального образования. С целью исключить указанную неточность, мы предлагаем изменить редакцию абзаца четвертого статьи седьмой Закона Российской Федерации «О государственной тайне» так, чтобы в новом изложении она выглядела следующим образом: «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством и муниципальными образованиями гражданам».

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. Поэтому 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» [29]. 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 [10]. 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.

Обязательным условием реализации любого права является корреспондирующей обязанности у другого участника правоотношений. Так, часть вторая статьи 24 Конституции Российской Федерации закрепляет обязанность органов государственной власти и местного самоуправления обеспечить возможность ознакомиться с документами и материалами, затрагивающими его права и свободы. Соответственно, мы делаем вывод, что каждый имеет право на допуск к информации, содержащейся в документах, относительно его прав и свобод, если это не противоречит федеральному законодательству.

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 мы можем 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 [40]. Поэтому мы считаем возможным, изменить редакцию статьи 28 Конституции Российской Федерации 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».

Отдельно стоит обратить внимание, что частью пятой статьи 29 Конституции Российской Федерации установлена гарантия свободы массовой информации. Отдельно отмечается, что цензура запрещена. Вопросу цензуры в современном обществе следует уделить отдельное внимание, поскольку он имеет дискуссионный характер в нынешних реалиях. Действующее законодательство определяет цензуру следующим образом. «Цензура массовой информации, то есть требование от редакции средства массовой информации со стороны должностных лиц, государственных органов, организаций, учреждений или общественных объединений предварительно согласовывать сообщения и материалы (кроме случаев, когда должностное лицо является автором или интервьюируемым), а равно наложение запрета на распространение сообщений и материалов, их отдельных частей» [14]. Стоит обратить внимание, что в действующем определении отсутствует упоминание опосредованного воздействия на средства массовой информации. Так, практика знает случаи, когда представители средств массовой информации получают сообщения с требованием ограничить распространение той или иной информации, в

противном случае им угрожают проблемами с законом. Ярким примером указанной ситуации является «дело Голунова», где журналист Иван Голунов получал угрозы со стороны правоохранительных органов через третьих лиц. После публикации своего расследования в его квартире нашли нарко лабораторию. Впоследствии было подтверждено, что действия правоохранительных органов в его адрес имели незаконный характер. Указанный случай является ярким примером опосредованной цензуры. 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».

А.А. Васютин, рассматривая вопросы цензуры в современной России, говорит о наличии негласной цензуры. Свою позицию автор аргументирует случаями, когда отдельные СМИ, поддерживающие оппозиционные движения, были заблокированы по весьма сомнительным основаниям. Как правило, такими основаниями являлись призывы к противоправному участию в массовых мероприятиях [7, с. 7]. Нам известны случаи, когда оппозиционные издания или сами оппозиционеры подвергались блокировке, признавались иностранными агентами, а также претерпевали санкции. Стоит ли это называть цензурой с точки зрения законодательства? Определенно нет. В подобных случаях органы власти действуют исключительно в рамках действующего законодательства, поэтому юридически их действия нельзя назвать цензурой. В целом можно отметить, что при помощи силового воздействия и давления можно оказывать влияние на средства массовой информации, определенная практика имеет место быть в ряде государств.

Заявлять же о наличии негласной цензуры в современной России, на наш взгляд, не совсем корректно, особенно в условиях информационного противостояния с государствами-агрессорами, при которых на население пытаются воздействовать при помощи различных способов.

Часть третья статьи 41 Конституции Российской Федерации содержит положение об ответственности за сокрытие должностными лицами фактов и обстоятельств, создающих угрозу для жизни и здоровья людей. Таким образом, мы делаем вывод, что граждане имеют право получать оперативную информацию об обстоятельствах, которые создают опасность для их жизни и здоровья. За сокрытие такое информации должностное лицо привлекается к ответственности по статье 237 Уголовного кодекса Российской Федерации. Если в результате сокрытия такой информации человеку причиняется вред или наступают иные тяжкие последствия, то максимальное наказание может назначаться в виде лишения свободы на срок до пяти лет с лишением права заниматься определенной деятельностью.

Отдельные авторы относят 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 [24, с. 18]. В целом с данной позицией можно согласиться. 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.

Следующее право на получение достоверной информации о состоянии окружающей среды, по сути, провозглашает публичность и общедоступность сведений о состоянии окружающей среды как в целом по стране, так и в рамках конкретного муниципального образования. Свое выражение, указанное положение находит, например, в Законе «О государственной» тайне, где предусмотрен запрет на сокрытие информации об окружающей среде и отнесения ее к категории «государственная тайна».

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.

Обобщая все вышеизложенное по теме данного параграфа, мы делаем следующие выводы. Во-первых, Конституцией Российской Федерации предусмотрен ряд положений, которые легли в основу формирования категории «информационная безопасность». Во-вторых, стоит обратить внимание на перечень информации, которая не может быть отнесена к категории «государственная тайна», а именно на формулировку «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам». Из ее содержания мы можем сделать вывод, что запрет на засекречивание такой информации распространяется только на привилегии, компенсации, гарантии, предоставляемые государством, то есть, органами государственной власти. Мы можем расширительно истолковать данное положение, поскольку государственная власть подразумевает

федеральную государственную власть и государственную власть субъектов. Но даже в этом случае без внимания остаются меры социальной поддержки, предоставляемые из бюджета муниципального образования. С целью исключить указанную неточность, мы предлагаем изменить редакцию абзаца четвертого статьи седьмой Закона Российской Федерации «О государственной тайне» так, чтобы в новом изложении она выглядела следующим образом: «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством и муниципальными образованиями гражданам». В-третьих, с целью обеспечения единства правоприменительной практики мы видим возможным следующее решение проблемы, связанной с отсутствием в законодательстве легального определения понятий личной и семейной тайны. 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.

2.2 Организационные основы обеспечения информационной безопасности

Как уже было отмечено нами в предыдущей главе, система обеспечения информационной безопасности является составным элементом отечественной системы обеспечения национальной безопасности. Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных

органов во взаимодействии с органами местного самоуправления, организациями и гражданами. То есть, в процессе обеспечения информационной безопасности задействованы все уровни власти, а также общественный потенциал в лице граждан и их объединений.

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» [42].

Деятельность каждого из перечисленных субъектов может быть целиком и полностью не связана с обеспечением информационной безопасности, но они обладают отдельными полномочиями в рамках достижения состояния защищенности от противоправного воздействия на охраняемую законом информацию, а также от информационного воздействия, которое может повлечь неблагоприятные последствия. 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, с целью обеспечить целостность понимания организационных основ обеспечения информационной безопасности, мы рекомендуем внести Президента Российской Федерации в указанный перечень, поскольку он обладает значительными полномочиями по вопросам обеспечения информационной безопасности.

В основе деятельности государственных органов, направленной на обеспечение информационной безопасности лежат следующие принципы:

– «законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

– конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

– соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

– достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

– соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации» [42].

Рассматривая представленные принципы, мы можем обратить внимание на следующие обстоятельства. Преподнося каждый пункт как отдельный принцип, авторы доктрины фактически перечислили в первом пункте сразу три принципа: законность, равенство всех перед законом и свобода информации. По сути, первые два принципа являются общеправовыми и не отражают особенности сферы информационной безопасности. Третий принцип дублирует положение Конституции Российской Федерации, но находится на своем месте, задавая базис всей системе принципов деятельности государственных органов при обеспечении информационной безопасности.

Принцип конструктивного взаимодействия означает, что все субъекты такого взаимодействия целенаправленно сотрудничают друг с другом для решения общих вопросов и проблем, урегулирования конфликтных ситуаций, а также с целью развития и совершенствования механизмов обеспечения информационной безопасности. Стоит обратить внимание, что в доктрине предусмотрено конструктивное взаимодействие между государственными органами, организациями и гражданами. Хотя выше в качестве элемента организационных основ были включены органы местного самоуправления. Мы не можем рассматривать их в качестве составной части государственных органов, поэтому считаем возможным, для полноты «картины» указать, что в основе деятельности по обеспечению информационной безопасности лежит принцип конструктивного взаимодействие государственных органов, органов местного

самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

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.

В свою очередь правовые меры представляют собой положения действующего отечественного законодательства, направленные на обеспечение информационной безопасности. 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. Более подробно вопросы ответственности за нарушение информационного законодательства мы рассмотрим в следующем параграфе.

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» [23, 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. Во-первых, с целью обеспечить целостность понимания организационных основ обеспечения информационной безопасности, мы рекомендуем внести Президента Российской Федерации в указанный перечень, предусмотренный Доктриной информационной безопасности, поскольку он обладает значительными полномочиями по вопросам обеспечения информационной безопасности. Во-вторых, в доктрине информационной безопасности предусмотрено конструктивное взаимодействие между государственными органами, организациями и гражданами. Хотя выше в качестве элемента организационных основ упоминаются органы местного самоуправления. Мы не можем рассматривать их в качестве составной части государственных органов, поэтому считаем возможным, для полноты «картины» указать, что в основе деятельности по обеспечению информационной безопасности лежит принцип конструктивного взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности. В-третьих, 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.

2.3 Ответственность как элемент механизма обеспечения информационной безопасности

Для успешной реализации любой правовой нормы требуется подкрепление в виде ответственности за ее нарушение. Нормы, направленные на обеспечение информационной безопасности, не являются исключением. В статье 17 Федерального закона «Об информации, информационных технологиях и о защите информации» установлено, что за нарушение законодательства об информации, информационных технологиях и о защите информации на нарушителя может быть возложена дисциплинарная, гражданско-правовая, административная или уголовная ответственность. Это можно объяснить тем, что различные правонарушения имеют разную степень общественной опасности (вредности). Мы делаем такую оговорку, поскольку в зависимости от вида правонарушения в научной литературе определяются его негативное воздействие на общественные отношения. Так, для преступлений это общественная опасность, а для административных правонарушений – общественная вредность. Перейдем к более детальному рассмотрению видов ответственности за правонарушения в сфере обеспечения информационной безопасности.

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» [40].

Рассмотрим отдельные проблемные аспекты отдельных преступлений в сфере обеспечения информационной безопасности. Так, в научной литературе ведутся дискуссии относительно необходимости закрепления в Уголовном кодексе ответственности за разглашение тайны усыновления (удочерения). Отдельные авторы отвечают, 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» [18, с. 819]. Мы не разделяем позицию автора и считаем, что разглашение тайны усыновления (удочерения) имеет высокую

степень общественной опасности, поскольку несет угрозы нормальному психическому развитию ребенка и его социализации.

При анализе нормы, предусматривающей уголовную ответственность за разглашение тайны усыновления (удочерения) нами было обращено внимание на следующие обстоятельства. Рассматриваемое преступление не предусматривает квалифицирующих составов. При этом субъектами преступления являются лица, на которые распространяется запрет в силу служебных обязанностей, а также иные лица. Законодатель никак не разграничивает ответственность указанных лиц. Очевидно, что разглашение тайны усыновления (удочерения) лицом, которое, в ходе исполнения служебных обязанностей узнало такую информацию, является более серьезным правонарушением, нежели частный разговор двух лиц, в ходе которого такая информация была разглашена. В связи с этим, мы считаем возможным, разделить статью 155 Уголовного кодекса на две части. В первой части рекомендуется установить ответственность за разглашение тайны усыновления (удочерения) лиц, для которых указанная информация не является служебной или профессиональной тайной. Во второй части рекомендуется отразить квалифицирующий признак, а именно обязанность хранить тайну усыновления (удочерения) в силу служебных или профессиональных обязанностей. Кроме того, нам кажется не совсем корректным указание на «корыстный или низменный мотив» разглашения тайны усыновления (удочерения). Не имеет никакого значения, какими именно мотивами руководствовалось лицо при разглашении тайны усыновления (удочерения), поскольку это несет угрозу интересам ребенка или его усыновителей. В связи с этим считаем необходимым исключить указание на мотивы преступника при разглашении им тайны усыновления (удочерения).

Наряду со спорами относительно целесообразности наличия статьи 150 в тексте Уголовного кодекса, среди ученых нет единого мнения относительно статьи 140 Уголовного кодекса, которая предусматривает

уголовную ответственность за неправомерный отказ в получении информации. Так, М.Г. Адылханов отмечает, что «с момента принятия УК РФ общее количество зарегистрированных преступлений по статье 140 УК РФ не превысило и десяти эпизодов, в определенном смысле, это позволяет утверждать, что в современных условиях уголовно-правовая норма, предусмотренная статьей 140 УК РФ, может быть причислена к категории так называемого символического уголовного законодательства и не имеет практической ценности» [2, с. 140]. Мы не разделяем позицию автора, поскольку указанная норма является логичным продолжением конституционного права граждан на свободное получение информации. Однако стоит обратить внимание, что статья 140 предусматривает наличие спорных формулировок. Например, законодатель в самом названии статьи указывает, что ответственность предусмотрена за отказ в предоставлении информации гражданину. Буквальное толкование позволяет сделать вывод, что Уголовный кодекс охраняет право на получение информации только при наличии устойчивой юридической связи с Российской Федерацией. Однако такое право гарантировано каждому, независимо от наличия у него гражданства.

Отдельно стоит обратить внимание, что состав преступления, предусмотренный статьей 140 Уголовного кодекса, является материальным, то есть, ответственность возникает с момента наступления общественно опасных последствий в форме вреда правам и законным интересам потерпевшего. Но само по себе совершение указанного деяния представляет собой нарушение, то есть, причинение вреда праву потерпевшего. С учетом того обстоятельства, что Кодекс Российской Федерации об административных правонарушениях предусматривает аналогичный состав, но уже без наступления каких-либо последствий [16], правоприменитель не может должным образом разграничить данные составы, поскольку для этого отсутствуют юридические критерии. Указную проблему можно решить либо путем закрепления в статье 140 Уголовного кодекса признаков, которые

позволят определить о каком именно вреде правам и законным интересам говорит законодатель, либо путем подготовки разъяснений Пленумом Верховного Суда.

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 [12, с. 56]. Данная позиция имеет место быть, поскольку законом предусмотрены случаи, когда нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений допускается законом. 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]. При этом само по себе это обстоятельство не может рассматриваться нами в качестве причины для внесения указанных изменений. Даже в самой статье 23

Конституции Российской Федерации, в которой закреплено право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, указано, что такое право может быть ограничено. То есть, при системном толковании норм мы понимаем, что в статье 138 Уголовного кодекса законодатель имеет именно на противоправное нарушение указанного права, поэтому указание в тексте рассматриваемой статьи указание на незаконность таких действий, на наш взгляд, является чрезмерным и излишним.

Следует обратить внимание, что проблемные аспекты имеют место быть и в составах преступлений, непосредственно связанных с угрозой государственной тайны. Так, при исследовании вопросов квалификации незаконного получения сведений, составляющих государственную тайну Е.В. Паноморенко обращает внимание на следующее обстоятельство. «Особенность рассматриваемого состава преступления кроется в его субъекте, им является физическое вменяемое лицо, достигшее 16-летнего возраста, которому государственная тайна не была доверена и не стала известна по службе, работе, учебе или в иных предусмотренных законодательством РФ случаях. Таким образом, субъект здесь общий, в связи с чем возникает вопрос: а может ли обычный человек знать, какие сведения относятся к государственной тайне, а какие нет?» [33, с. 195]. Для того, чтобы попытаться ответить на этот вопрос необходимо обратиться к нормативно-правовой базе в сфере информационного регулирования. Ранее нами уже был рассмотрен Федеральный закон «О государственной тайне». В нем содержится только общий перечень сведений, которые могут быть отнесены к государственной тайне. Поэтому, изучив только этот закон, обычный человек не сможет точно понять, какая именно информация является государственной тайной, а какая нет. Исходя из текста Указа Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» «назначается федеральный орган исполнительной власти, ответственный за ту или иную категорию государственной тайны,

после чего каждый орган принимает свои подзаконные акты, в которых определены перечни и категории государственных секретов в той или иной сфере» [43]. На сегодняшний день такие перечни также ограничены для изучения. Таким образом, простому человеку весьма сложно понять, какие именно сведения относятся к категории «государственная тайна». При этом такое понимание практически всегда будет построено на догадках и предположениях. При условии, что рассматриваемое преступление может быть совершено только с прямым умыслом, перед правоприменителем стоит сложная задача, доказать, что лицо знало о характере получаемых данных и осознавало противоправность своего деяния.

Административная ответственность в сфере информации предусмотрена главой 13 Кодекса Российской Федерации об административных правонарушениях. Хотя отдельные правонарушения можно найти и за ее пределами, например, уже ранее затронутая нами статья 5.39, в которой предусмотрена ответственность за отказ в предоставлении информации. В указанной главе можно встретить следующие составы правонарушений, относящихся к сфере обеспечения информационной безопасности:

– «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» [16].

Широкий перечень административных правонарушений в сфере обеспечения информационной безопасности характеризуется рядом проблем,

которые возникают в процессе правоприменительной деятельности. Так, Е.В. Безрученко обращает внимание, что «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» [6, с. 182]. Безусловно, указанные проблемы имеют место быть. Не совсем понятно, каким образом можно привлечь к ответственности гражданина другого государства, который распространял, например, в социальной сети «Вконтакте» высказывания с призывами дискриминировать какую-то из социальных групп по национальному признаку. Даже если удастся идентифицировать такого гражданина, то реально привлечь его к ответственности практически невозможно. Единственной санкцией в этом случае станет только блокировка его профиля на сайте. По поводу анонимности в интернете ранее уже нами были сделаны отдельные выводы, поэтому приводить их вновь, мы не считаем целесообразным.

Л.К. Терещенко обращает внимание, что определенные сомнения относительно целесообразности и эффективности возникают при анализе злоупотребления свободой массовой информации [38, с. 64]. Анализ статьи 13.15 Кодекса об административных правонарушениях показал, что злоупотребление свободой массовой информации представляет собой сложную конструкцию, которая включает в себя более десяти различных деяний, за совершение хотя бы одного из них предусмотрена административная ответственность по указанной статье. В целом можно отметить, что указанная статья является своего рода инструментом для закрытия пробелов в отечественном административном законодательстве в сфере информационной безопасности. При необходимости законодатель может внести в нее сколько угодно деяний, обозначив их в качестве злоупотребления свободой массовой информации. Возможно,

целесообразность указанной нормы вызвана актуальной обстановкой в обществе, поскольку с ее помощью можно ограничить свободу распространения любой неправомерной, по мнению законодателя, информации. Очевидным является тот факт, что столь широкое скопление различных составов правонарушений в рамках одной статьи создает определенные трудности при разграничении составов административных правонарушений между собой. Однако нельзя отрицать, что при помощи указанной нормы возможно привлечь к ответственности юридическое лицо за правонарушения, которые в силу специфики уголовного законодательства не могут быть им инкриминированы. Поэтому мы не разделяем позицию автора, что наличие указанной нормы не имеет практической ценности.

В целом можно отметить, что процедура привлечения к административной ответственности в сфере информационной безопасности осложнена высоким уровнем латентности таких правонарушений (она вызвана возможностью размещать противоправную информацию анонимно), местонахождением правонарушителя, а также техническими сложностями при определении места и времени, когда было совершено информационное правонарушение.

Дисциплинарная ответственность за нарушение в сфере информационной возникает только в том случае, когда на лицо возложена обязанность совершить определенные действия (например, предоставить гражданину информацию, затрагивающую его права и свободы) или воздержаться от совершения таких действий (например, медицинский сотрудник не должен разглашать информацию относительно диагноза и хода лечения пациента). То есть, дисциплинарная ответственность применяется при нарушении профессиональных или служебных обязанностей. По общему правилу, Трудовой кодекс позволяет применять в качестве дисциплинарных взысканий следующие меры ответственности: замечание, выговор, увольнение [39]. Для государственных служащих система дисциплинарных взысканий выглядит следующим образом: замечание, выговор,

предупреждение о неполном должностном соответствии, увольнение [51]. Дисциплинарная ответственность может быть наложена независимо от признаков в деянии лица состава уголовного или административного правонарушения. При этом материалы служебной проверки могут быть направлены в правоохранительные органы для привлечения лица, помимо дисциплинарной ответственности, к уголовной и административной ответственности.

Гражданско-правовая ответственность за правонарушения в сфере информационной безопасности может возникнуть за любое нарушение прав лица в информационной сфере, если в результате пострадавшему был причинен имущественный или личный неимущественный вред. Согласно Гражданскому и Уголовному кодексу, потерпевший вправе требовать возмещения ущерба от правонарушителя (преступника), причинившего материальный и моральный ущерб в результате действий, совершенных правонарушителем, исходя из правил деликтной ответственности [9]. Как правило, лицо в рамках рассмотрения дела о правонарушении подает гражданский иск с целью возместить причиненный ей имущественный, репутационный или моральный вред.

В завершении темы данной главы, мы можем сделать следующие выводы. Во-первых, Конституцией Российской Федерации предусмотрен ряд положений, которые легли в основу формирования категории «информационная безопасность». Во-вторых, стоит обратить внимание на перечень информации, которая не может быть отнесена к категории «государственная тайна», а именно на формулировку «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам». Из ее содержания мы можем сделать вывод, что запрет на засекречивание такой информации распространяется только на привилегии, компенсации, гарантии, предоставляемые государством, то есть, органами государственной власти. Мы можем расширительно истолковать данное положение, поскольку государственная власть подразумевает федеральную

государственную власть и государственную власть субъектов. Но даже в этом случае без внимания остаются меры социальной поддержки, предоставляемые из бюджета муниципального образования. С целью исключить указанную неточность, мы предлагаем изменить редакцию абзаца четвертого статьи седьмой Закона Российской Федерации «О государственной тайне» так, чтобы в новом изложении она выглядела следующим образом: «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством и муниципальными образованиями гражданам». В-третьих, с целью обеспечения единства правоприменительной практики мы видим возможным следующее решение проблемы, связанной с отсутствием в законодательстве легального определения понятий личной и семейной тайны. 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. В-четвертых, с целью обеспечить целостность понимания организационных основ обеспечения информационной безопасности, мы рекомендуем внести Президента Российской Федерации в указанный перечень, предусмотренный Доктриной информационной безопасности, поскольку он обладает значительными полномочиями по вопросам обеспечения информационной безопасности. В-пятых, в доктрине информационной безопасности предусмотрено конструктивное взаимодействие между государственными органами, организациями и гражданами. Хотя выше в качестве элемента организационных основ упоминаются органы местного самоуправления. Мы не можем рассматривать их в качестве составной части государственных органов, поэтому считаем возможным, для полноты «картины» указать, что в основе деятельности по

обеспечению информационной безопасности лежит принцип конструктивного взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности. В-шестых, 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. В-седьмых, мы считаем возможным, разделить статью 155 Уголовного кодекса на две части. В первой части рекомендуется установить ответственность за разглашение тайны усыновления (удочерения) лиц, для которых указанная информация не является служебной или профессиональной тайной. Во второй части рекомендуется отразить квалифицирующий признак, а именно обязанность хранить тайну усыновления (удочерения) в силу служебных или профессиональных обязанностей. Кроме того, нам кажется не совсем корректным указание на «корыстный или низменный мотив» разглашения тайны усыновления (удочерения). Не имеет никакого значения, какими именно мотивами руководствовалось лицо при разглашении тайны усыновления (удочерения), поскольку это несет угрозу интересам ребенка или его усыновителей. В связи с этим считаем необходимым исключить указание на мотивы преступника при разглашении им тайны усыновления (удочерения). В-восьмых, мы предлагаем закрепить в статье 140 Уголовного кодекса признаки, которые позволят определить о каком именно вреде правам и законным интересам говорит законодатель, либо Пленуму Верховного Суда подготовить разъяснения по данному вопросу.

Глава 3 Актуальные проблемы обеспечения информационной безопасности в Российской Федерации

На сегодняшний день в условиях информационного противостояния нашего государства внешним угрозам со стороны недружественных стран вопросы обеспечения информационной безопасности приобретают особое значение. Поэтому мы считаем необходимым, подробней рассмотреть актуальные проблемы, характерные для данной сферы.

«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» [27, 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 [41]. 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» [53, с. 30]. На наш взгляд, 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.

При рассмотрении статьи 150 Уголовного кодекса нами было отмечено, что защита нормального психического развития ребенка является важной для государства задачей. Продолжая эту тему, стоит отметить, находясь в интернете, несовершеннолетний постоянно подвергается угрозе взаимодействия с нежелательным контентом. 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. Так, Н.Е. Колобаева обращает внимание, что использование ресурсов сети является одним из условий социализации в современном мире [17, с. 15]. В целом мы можем 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 [8, с. 100]. На наш взгляд, 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).

Решить рассматриваемую проблему применяя исключительно правовые запреты и ограничения, на наш взгляд, не представляется возможным. В этом случае требуется совокупность различных мер, направленных на обеспечение безопасности детей от информационных угроз в интернете. В первую очередь необходимо проводить с детьми уроки, направленные на повышение их грамотности по вопросам безопасного поведения в интернет пространстве. Это могут быть специальные курсы в рамках уроков информатики или отдельные дисциплины наряду с недавно введенными разговорами о важном. При этом важно вести такую работу не только с детьми, но и с их родителями. Требуется увеличить их вовлеченность в обеспечение информационной безопасности детей в сети. На сегодняшний день есть специально-технические механизмы родительского контроля, но, как правило, они не используются и легко обходятся. Помимо уже высказанных рекомендаций, мы предлагаем внедрение в широкое применение сим-карт для несовершеннолетних. Выход в интернет с них будет ограничен так, чтобы несовершеннолетний не мог случайно или намеренно столкнуться с вредным для него контентом.

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. 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. При создании профиля в социальной сети следует затребовать верификацию

при помощи паспорта, если пользователь отказывается пройти данную процедуру, его профиль автоматически признается «детским», после чего он не может посещать определенные сообщества, смотреть видео, видеть содержание постов, если автором установлена соответствующая возрастная отметку. В этих целях отдельно потребуется проводить проверки материалов, размещенных в социальных сетях, на наличие соответствующих возрастных отметок. На наш взгляд, подобное решение положительно скажется на информационной безопасности несовершеннолетних в интернете.

В доктрине обеспечения информационной безопасности отмечается, что специальные службы враждебно настроенных государств осуществляют воздействие на общество с целью дестабилизировать обстановку внутри страны при помощи растущих возможностей информационных технологий. На сегодняшний день указанная угроза приобрела еще большую актуальность в условиях проведения специальной военной операции. На население Российской Федерации активное воздействие в интернете оказывает ЦИПсО. Это специальное подразделение, целью которого является проведение психологических атак на противника. Так, в условиях частичной мобилизации действия ЦИПсО были направлены на то, чтобы вызвать панику и волнения среди населения. В результате проведенных атак массовые беспорядки были замечены в южных регионах России, а также увеличилось число граждан мужского пола, которые покинули территорию страны. В этих условиях очень важно постоянно поддерживать связь с населением, путем подготовки ежедневных сводок с актуальной информацией, а также разоблачения ложной информации, набравшей популярность в интернете. Только тогда получится минимизировать вероятность возникновения панических и агрессивных настроений в обществе и в целом стабилизировать состояние информационной безопасности.

Еще одна актуальная проблема обеспечения информационной безопасности заключается в росте компьютерной преступности в кредитно-

финансовом секторе, а также в сфере защиты персональных данных граждан. За 2022 год произошло несколько крупных утечек клиентских баз данных сервисов Яндекс.Еда, СДЭК и ДНС. Практика показывает, что персональные данные передаются, в том числе, и сотрудниками налоговых органов. Не редкими являются случаи, когда сразу после регистрации юридического лица или статуса индивидуального предпринимателя гражданин мгновенно попадает в поле зрения банков, которые пытаются навязать ему свои услуги. Еще один аргумент в пользу ненадежности хранения персональных данных заключается в том, что любой желающий посредством телеграмма (мессенджер) и за небольшую плату может по номеру телефона получить следующую информацию о человеке: фамилия, имя, отчество, предположительный адрес проживания, наличие счетов в банках, номер автомобиля, а в отдельных случаях и более подробную информацию. Хотя действующее законодательство предусматривает механизмы ответственности, как правило, реализуются они только в случаях крупных утечек. Объяснить такое положение вещей можно тем, что в нашей стране не достаточно высокий уровень правовой культуры, поэтому в большинстве случаев при обнаружение факта утечки своих или чьих-либо еще персональных данных, гражданин относится к этому нейтрально или негативно, но при этом не стремится обратиться в правоохранительные органы. В этой связи, нам кажется возможным проводить специальные мероприятия, направленные на информирование население о возможных угрозах утечки персональных данных, способах борьбы с ними, а также механизме обращения в правоохранительные органы в случае выявления утечки своих персональных данных.

В завершении данной главы, нами будут сделаны следующие выводы. Во-первых, для повышения оперативности расследования выявленных эпизодов использования на предприятиях специальных технических средств, предназначенных для негласного получения информации мы предлагаем внести статьи 138 и 138.1 Уголовного кодекса в часть пятую статьи 151

Уголовно-процессуального кодекса, обеспечив возможность проводить расследование по указанным преступлениям органам, которые выявили это преступление. Во-вторых, говоря 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. В-третьих, мы предлагаем внедрение в широкое применение сим-карт для несовершеннолетних. Выход в интернет с них будет ограничен так, чтобы несовершеннолетний не мог случайно или намеренно столкнуться с вредным для него контентом. В-четвертых, для защиты несовершеннолетних от вредоносной информации в социальных сетях нами были предложены следующие рекомендации. При создании профиля в социальной сети следует затребовать верификацию при помощи паспорта, если пользователь отказывается пройти данную процедуру, его профиль автоматически признается «детским», после чего он не может посещать определенные сообщества, смотреть видео, видеть содержание постов, если автором установлена соответствующая возрастная отметку. В-пятых, в условиях осуществления деятельности специальных организаций, в задачи которых входит психическое информационное воздействие на население очень важно постоянно поддерживать связь с населением, путем подготовки ежедневных сводок с актуальной информацией, а также разоблачения ложной информации, набравшей популярность в интернете. В-шестых, нам кажется возможным проводить специальные мероприятия, направленные на информирование население о возможных угрозах утечки персональных данных, способах борьбы с ними, а также механизме обращения в правоохранительные органы в случае выявления утечки своих персональных данных.

Заключение

Одним из основных структурных элементов системы национальной безопасности является информационная безопасность. Информационную безопасность можно рассматривать в двух основных направлениях. Во-первых, состояние защищенности информации от неправомерного завладения, использования, распространения. В этом случае, например, мероприятия направлены на охрану информации, составляющую тайну частной жизни, государственную или коммерческую тайну. Во-вторых, защита от информации, распространение которой может привести к негативным последствиям. Анализ научной литературы позволил нам уточнить и дополнить легальное определение понятия «информационная безопасность». Информационная безопасность - состояние защищенности личности, общества и иных социальных групп, а также государства в лице государственных органов и должностных лиц от противоправного воздействия на охраняемую законом информацию, а также от информационного воздействия, которое может повлечь неблагоприятные последствия, при котором обеспечиваются реализация приоритетов, предусмотренных Стратегией национальной безопасности.

Система принципов обеспечения информационной безопасности построена вокруг соблюдения и охраны прав и законных интересов граждан. Что является особенно важным, при определении принципов информационной безопасности законодатель уделяет особое внимание прогнозированию и выявлению возможных угроз еще на первоначальных этапах их формирования. При этом объективно принимается во внимание, что сама система мер обеспечения информационной безопасности неидеальна, поэтому в ее основу закладывается принцип глубокой защиты, определяющий меры

воздействия на угрозу, уже причинившую определенный вред объектам охраны информационной безопасности.

Рассматривая механизм обеспечения информационной безопасности, нами были предложены следующие рекомендации по его совершенствованию.

Во-первых, стоит обратить внимание на перечень информации, которая не может быть отнесена к категории «государственная тайна», а именно на формулировку «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам». Из ее содержания мы можем сделать вывод, что запрет на засекречивание такой информации распространяется только на привилегии, компенсации, гарантии, предоставляемые государством, то есть, органами государственной власти. Мы можем расширительно истолковать данное положение, поскольку государственная власть подразумевает федеральную государственную власть и государственную власть субъектов. Но даже в этом случае без внимания остаются меры социальной поддержки, предоставляемые из бюджета муниципального образования. С целью исключить указанную неточность, мы предлагаем изменить редакцию абзаца четвертого статьи седьмой Закона Российской Федерации «О государственной тайне» так, чтобы в новом изложении она выглядела следующим образом: «о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством и муниципальными образованиями гражданам».

Во-вторых, с целью обеспечения единства правоприменительной практики мы видим возможным следующее решение проблемы, связанной с отсутствием в законодательстве легального определения понятий личной и семейной тайны. 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.

В-третьих, с целью обеспечить целостность понимания организационных основ обеспечения информационной безопасности, мы рекомендуем внести Президента Российской Федерации в указанный перечень, предусмотренный Доктриной информационной безопасности, поскольку он обладает значительными полномочиями по вопросам обеспечения информационной безопасности.

В-четвертых, в доктрине информационной безопасности предусмотрено конструктивное взаимодействие между государственными органами, организациями и гражданами. Хотя выше в качестве элемента организационных основ упоминаются органы местного самоуправления. Мы не можем рассматривать их в качестве составной части государственных органов, поэтому считаем возможным, для полноты «картины» указать, что в основе деятельности по обеспечению информационной безопасности лежит принцип конструктивного взаимодействие государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

В-пятых, 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.

В-шестых, мы считаем возможным, разделить статью 155 Уголовного кодекса на две части. В первой части рекомендуется установить ответственность за разглашение тайны усыновления (удочерения) лиц, для

которых указанная информация не является служебной или профессиональной тайной. Во второй части рекомендуется отразить квалифицирующий признак, а именно обязанность хранить тайну усыновления (удочерения) в силу служебных или профессиональных обязанностей. Кроме того, нам кажется не совсем корректным указание на «корыстный или низменный мотив» разглашения тайны усыновления (удочерения). Не имеет никакого значения, какими именно мотивами руководствовалось лицо при разглашении тайны усыновления (удочерения), поскольку это несет угрозу интересам ребенка или его усыновителей. В связи с этим считаем необходимым исключить указание на мотивы преступника при разглашении им тайны усыновления (удочерения).

В-седьмых, мы предлагаем закрепить в статье 140 Уголовного кодекса признаки, которые позволят определить о каком именно вреде правам и законным интересам говорит законодатель, либо Пленуму Верховного Суда подготовить разъяснения по данному вопросу.

Список используемой литературы и используемых источников

1. Азимов Ф.А. Стратегия национальной безопасности Российской Федерации // Власть. 2021. №4. С. 79-83.
2. 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.
3. Артамонова Я.С. К вопросу о понятии «Информационная безопасность» // Социально-гуманитарные знания. 2018. №1. С. 319-321.
4. Ахметов А.И., Аминов И.Р. Понятие, цели и виды национальной безопасности // Международный журнал гуманитарных и естественных наук. 2020. №5-2. С. 199-201.
5. Баринов С.В. О правовом определении понятия «Информационная безопасность личности» // Актуальные проблемы российского права. 2016. №4 (65). С. 97-105.
6. Безручко Е.В., Рысай Б.Г. Некоторые проблемы административной ответственности в сфере связи и информации // ЮП. 2020. №1(92). С. 180-185.
7. 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.
8. Власенко М.С. Обеспечение информационной безопасности несовершеннолетних в сети Интернет: современное состояние и совершенствование правового регулирования // Вестник ВУиТ. 2019. №3. С. 98-105.

9. Гражданский кодекс Российской Федерации (часть вторая) от 26.01.1996 №14-ФЗ (ред. от 01.07.2021) // СЗ РФ. 1996. №5. Ст. 410.

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

11. Емельянова Е.В., Петрянин А.В. Стратегия национальной безопасности Российской Федерации: переоценка современных вызовов // Вестник БелЮИ МВД России. 2021. №4. С. 10-16.

12. 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.

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

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

15. Казанцев С.В. О новой Стратегии национальной безопасности Российской Федерации // Мир новой экономики. 2015. №3. С. 7-15.

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

17. 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.

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

19. 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.

20. Кочетков А.П. Доктринальные установки государственной политики России в области обеспечения национальной безопасности // Государственное и муниципальное управление. Ученые записки. 2019. №3. С. 22-26.

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

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

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

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

25. Молчанов Н.А., Егоров В.П., Матевосова Е.К. Новые аспекты правового регулирования государственного стратегического планирования в Российской Федерации // Актуальные проблемы российского права. 2015. №2. С. 28-34.

26. Неверов А.Я. Стратегия национальной безопасности Российской Федерации как политический приоритет // Социум и власть. 2016. №6 (62). С. 88-93.

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

28. Онлайн и офлайн: откуда получают информацию россияне // [Электронный ресурс]. - https://wciom.ru (дата обращения 07.09.2022)

29. 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.

30. Плотников В.А., Пролубников А.В., Рукинов М.В. Институционально-стратегические аспекты государственной политики в сфере обеспечения национальной безопасности Российской Федерации // Глобальная ядерная безопасность. 2020. №2 (35). С. 119-130.

31. Понеделков А. В., Кузина С. И. Система внешних и внутренних угроз национальной безопасности России // Государственное и муниципальное управление. Ученые записки . 2019. №3. С. 106-113.

32. Пономарев А.И. О стратегии и системе обеспечения национальных интересов // Национальная безопасность / nota bene. 2017. №1 (48). С. 43-51.

33. Пономаренко Е.В. Проблемы применения уголовной ответственности за незаконное получение сведений, составляющих государственную тайну // Вестник СГЮА. 2015. №2 (103). С. 193-197.

34. Свистунов Д.Е. Национальная безопасность в Российской Федерации: теоретико-правовое исследование // Вестник Марийского государственного университета. Серия «Исторические науки. Юридические науки». 2017. №1 (9). С. 78-83.

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

36. Степанов А.В. Безопасность, национальная безопасность, миграционная безопасность, национальная миграционная политика: анализ определений, соотношение категорий // Пенитенциарная наука. 2019. №2 (26). С. 75-78.

37. Степанов А.В. Понятие категории «Национальная безопасность»: теоретико-правовой анализ // Вестник Пермского университета. Юридические науки. 2015. №2 (28). С. 8-17.

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

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

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

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

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

43. Указ Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне» от 30.11.1995 №1203 (ред. от 25.03.2021) // СЗ РФ. 1995. №49. Ст. 4775.

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. Чесноков А.Д. Информационная безопасность // StudNet. 2022. №1. С. 478-489.

53. 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.

54. Шободоева А.В. Стратегия национальной безопасности РФ и ее вклад в развитие понятийного аппарата общей теории национальной безопасности РФ // Baikal Research Journal. 2016. №1. С. 17-19.