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

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

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

Государственно-правовая
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему «Информационные правонарушения как угроза национальной безопасности»

Обучающийся И.Е. Наделяева _____
(Инициалы Фамилия) (личная подпись)

Руководитель к.э.н., В.Ю. Моисеева
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Аннотация

Тема выпускной квалификационной работы – «Информационные правонарушения как угроза национальной безопасности».

Актуальность темы выпускной квалификационной работы определяется важностью, которую имеет информация в жизни современного общества. Саму современную цивилизацию иногда называют «информационной». Функционирование современных государств, деятельность бизнеса, разного рода организаций, существование практически каждого обычного человека – все это самым непосредственным образом бывает связано с обменом самого разного рода информации. Правонарушения, посягающие на информацию, таким образом, посягают на сами основы существования современного общества.

Целью настоящего исследования является рассмотрение проблематики информационных правонарушений, выступающих в качестве угроз национальной безопасности, формирование выводов и рекомендаций, касающихся обозначенного вопроса.

Для достижения обозначенной цели необходимо будет выполнить такие задачи, как:

- определение понятия правонарушения, посягающего на информацию;
- определение законодательных основ противодействия информационным угрозам национальной безопасности;
- изучение особенностей государственного регулирования в сфере противодействия правонарушениям, посягающим на информацию;
- формулирование выводов и рекомендаций, призванных нормализовать обстановку в рассматриваемой области.

Структура выпускной квалификационной работы включает введение, три главы, заключение, список используемой литературы и используемых источников. Работа включает 82 страницы.

Оглавление

Введение

Актуальность темы выпускной квалификационной работы определяется важностью, которую имеет информация в жизни современного общества. Саму современную цивилизацию иногда называют «информационной». Функционирование современных государств, деятельность бизнеса, разного рода организаций, существование практически каждого обычного человека – все это самым непосредственным образом бывает связано с обменом самого разного рода информации.

Дополнительную актуальность обозначенной проблематике придает развитие современных компьютерных технологий и технологий, используемых в сфере обращения «больших данных» (big data).Различными субъектами в настоящее время собираются огромные объемы информации, касающиеся как социально-экономических процессов, так и жизнедеятельности каждого отдельного человека. Обработанные программным образом, подобного рода данные позволяют предсказывать будущее развитие событий, а злоумышленники могут использовать их для манипулирования поведением как личности, так и общества. Это обуславливает необходимость защиты соответствующей информации, что выражается, например, в развитии законодательства о персональных данных.

Развитие современных технологий вызывает к жизни и появление новых разновидностей данных, с которыми законодатель не имел дела ранее. Речь может идти, например, о биометрических данных гражданина, которые используются для его идентификации в кредитных организациях и которые тоже подлежат правовой охране. Проблема в данном случае может заключаться в том, что деятельность законодателя в данном случае часто может отставать от развития технического прогресса и от деятельности злоумышленников, причиняющих вред другим субъектам посредством доступа к относящимся к ним информации. С момента появления компьютеров и начала их использования в хозяйственной деятельности

человека, злоумышленники стали использовать современные технологии в своих интересах, получая неправомерный доступ к не принадлежащей им информации, уничтожая или модифицируя информацию посредством разработки компьютерных вирусов и т.д. И всегда происходило несколько лет прежде чем законодателю удавалось разработать адекватные нормы и процедуры, способствующие борьбе с подобного рода деструктивными социальными явлениями.

В настоящее время также еще не получили адекватного ответа законодателя действия злоумышленников, которые посягают, например, на аккаунты других людей в социальных сетях, в он-лайн играх и т.д. Даже сама правомочность отнесения подобного рода правонарушений к правонарушениям в сфере информации, а не, например, к правонарушениям в сфере оборота интеллектуальной собственности до сих пор вызывает сомнения у специалистов. Изучение информации об организуемых в настоящее время юридических научных конференциях позволяет прийти к выводу, что очень большое их количество посвящены именно обсуждению проблем информационного права, цифровизации, организации защиты информации и иным одно порядковым проблемам, которые еще не получили своего разрешения ни на теоретическом ни на практическом уровнях.

Особое значение надлежащие защита и оборот информации в настоящее время имеют в сфере обеспечения национальной безопасности. Речь в СМИ идет о целых «информационных войнах», которые развязывают современные государства и которые по своим последствиям, по воздействию, оказываемому ими на экономику и социальную сферу, могут не отличаться от традиционных войн прошлого. Большое значение в настоящее время имеет также противодействие корпорациям, осуществляющим деятельность в сфере Интернет-технологий и разного рода социальных сетей. Реальность показывает, что деятельность подобного рода организаций, многие из которых действуют из-за рубежа, бывает связана с организацией социальных беспорядков, с целенаправленным воздействием на общественное мнение,

осуществляемым для того, чтобы общество изменило свои взгляды относительно существа того или иного вопроса. Подобного рода деятельность также нуждается в своем законодательном определении.

Целью настоящего исследования является рассмотрение проблематики информационных правонарушений, выступающих в качестве угроз национальной безопасности, формирование выводов и рекомендаций, касающихся обозначенного вопроса.

Для достижения обозначенной цели необходимо будет выполнить такие задачи, как:

- определение понятия правонарушения, посягающего на информацию;
- определение законодательных основ противодействия информационным угрозам национальной безопасности;
- изучение особенностей государственного регулирования в сфере противодействия правонарушениям, посягающим на информацию;
- формулирование выводов и рекомендаций, призванных нормализовать обстановку в рассматриваемой области.

Объектом исследования выступают общественные отношения, складывающиеся в области противодействия правонарушениям, посягающим на информацию.

Предметом исследования выступают нормы отечественного законодательства, направленные на противодействие правонарушениям, которые посягают на информацию, а также материалы соответствующей юридической практики.

Методологию исследования представляют такие общеправовые методы, как анализ и синтез, индукция и дедукция. Сущность изучаемого вопроса заставила нас широко использовать метод прогнозирования, призванный помочь предсказать будущее развитие соответствующих общественных отношений.

Глава 1. Понятие и сущность информационных правонарушений, их место в системе угроз национальной безопасности

1.1 Определение информационного правонарушения

Усложнение общественных отношений, которое непрерывно сопровождает человеческую цивилизацию, заставляет законодателя реагировать посредством принятия соответствующих нормативно-правовых актов, призванных регулировать и охранять изменившиеся отношения в обществе.

Подобная дифференциация и повышение эффективности нормативного материала сопровождает человечество на протяжении всей его истории. В частности, в древнее и средневековое время, законодатель мог урегулировать общественные отношения посредством издания немногочисленных нормативно-правовых актов. Число норм, предусматривающих обязанность правонарушителя понести меры юридической ответственности, также в этот период было невелико и вполне достаточно было единого закона («Русской правды», «Судебника» или «Соборного уложения») для того, чтобы защитить соответствующее общество от противоправных посягательств.

В последующем, следуя за усложнившийся жизнью общества, вынуждаемый появлением новых объектов, нуждающихся в правовой охране, законодатель вынужден был принимать новые нормы, предполагающие наличие института юридической ответственности и наказания. Институт юридической ответственности претерпевал свою отраслевую дифференциацию, в связи с чем была выделена ответственность уголовная и административная, гражданская и дисциплинарная. Данный процесс в настоящее время опрометчиво было бы считать законченным – в последние годы появилось множество научных исследований, в рамках которых учеными предлагается дополнить межотраслевой институт юридической ответственности новыми отраслевыми разновидностями (например,

ответственностью финансовой или природоохранной). В рамках отдельных правовых институтов также прослеживается дифференцирование соответствующего закона; например, ранее единый уголовный закон , в условиях принятия современного уголовного кодекса был разделен на части, разделы и главы. Увеличивается и количество статей, входящих в соответствующую отрасль права. Сравнение современного текста законов, предполагающих нормы юридической ответственности с тем текстом, которым был при данных законов принятии, позволяет говорить о постоянно идущих процессах гуманизации действующих нормативно-правовых актов, а также о том, что количество правовых норм, включенных в действующие законы и кодексы после их принятия, значительно превышают количество норм, из соответствующих законов исключенных в связи с изменениями соответствующих общественных отношений и утраты этими отношениями нуждаемости в их охране и защите.

Для того, чтобы государство признало необходимость фиксации в исходящих от государства актах института юридической ответственности за совершение того или иного деяния, само данное деяние не должно быть для государства безразличным, оно (в лице своих служащих) должно понимать опасность совершение конкретного правонарушения и эта опасность должна быть настолько явной и системной, что это может подвигнуть государство на разработку и принятие соответствующих правовых норм. Нормы права призваны регулировать только систематические общественные отношения – правило поведения не может вводится ради одного какого-то конкретного или эпизодического случая. Таким образом, для того, чтобы какие-то (например, информационные) правонарушения послужили основой для разработки самостоятельного и уникального института права, они должны носить частный характер на практике и приносить потери, которые государство может счесть нежелательными.

Таким образом, даже если какое-то правонарушение, влечет нарушение прав граждан и организаций, не затрагивая прямым образом вопросы

обеспечения национальной безопасности, подобные вопросы все равно могут возникнуть, если правонарушение негативным образом влияет на складывающийся в обществе социально-духовный климат. Если граждане, индивидуальные предприниматели и юридические лица несут материальные потери от правонарушений того или иного рода, это опосредованным образом отражается и на государстве (например, падает его налоговая база). Таким образом, вопросы обеспечения национальной безопасности носят весьма широкий характер и не охватываются задачей, например, предотвращения именно государственных преступлений.

Процесс становления нового института права вообще и института юридической ответственности за новое правонарушение в частности, всегда представляет собой трудности самого разного рода. В качестве важнейшей сложности в данном отношении можно говорить о проблеме формализации нового правового института и даже о проблеме выборе его названия.

Так, например, нарушение правил функционирования информационного комплекса Российской Федерации мы планируем называть информационными правонарушениями, но количество возможных подходов здесь является достаточно большим. Проведенное нами исследование, например, показывает, что очень многие авторы обозначают данное явление словосочетанием «правонарушение в информационной сфере». В качестве подобного рода работ можно назвать труды А.И. Марушак [24], В.М. Матвеевой [25], Н.А. Ноздриной [27], К.В. Осенькиной [28], Я.В. Порбиной [31], Д.Д. Савенковой [35], Д.Б. Савчишкина [36], В.Ю. Стромова [38], А.Г. Суханова [39] и многих других исследователей. В целом, можно говорить о том, что подобный подход к обозначению данной категории правонарушений является очень распространенным в правовой литературе.

Некоторые авторы говорят не про «информационную сферу», а про информационное пространство, такова, например, работа О.А. Шувалова [51].

Говорится рядом ученых также про правонарушения в области информационных технологий, в этом отношении можно выделить, например,

А.А. Макарову [22] или М.Е. Трофимову [40].

Подобная же формулировка использовалась в названии кандидатской диссертации О.Г. Юрченкова [52].

Возможен также на практике вариант обозначения данного рода правонарушений, как деяний, направленных на информационную безопасность. По данному пути пошла, например, С.А. Кручинина [19].

В данном случае мы предлагаем остановиться на названии «информационные правонарушения» как наиболее кратком, емком и должным образом раскрывающем противоправную сущность соответствующего рода деяний. Именно на информацию и посредством информации в данном случае происходит противоправное посягательство, в связи с чем выбранный вариант названия выглядит логичным и заслуживающим своего применения на практике.

«Информационными правонарушениями» соответствующие противоправные деяния были названы в работах М.У. Байсаевой (которая предлагает разграничивать категории информационных и компьютерных правонарушений в качестве самостоятельных) [2], Л.А. Букалеровой (рассматривающей сущность соответствующих информационных правонарушений, совершаемых в сфере публичного управления) [4], А.В. Кравцова (рассматривающего проблематику совершения информационных правонарушений в сфере административного права и реализацию в отношении нарушителей института административной ответственности) [18], О. Заярного (рассматривающего субъективные элементы состава административного информационного правонарушения) [10].

Термин «информационное правонарушение» используется также в диссертации А.В. Полушкина, которая защищалась в 2009 году [29].

Можно прийти к выводу, таким образом, что присутствует значительная дискуссионность этого явления, которая продолжает сохраняться в настоящее время. Отсутствие единства среди ученых относительно названия соответствующей группы правонарушений может означать отсутствие

единства и по поводу перечня соответствующих противоправных деяний. Подобная несогласованность в юридической науки самым негативным образом отражается на законотворчестве и практике применения соответствующего института юридической ответственности, что позволяет говорить о важности достижения задачи скорейшего достижения ясности в рассматриваемой сфере общественных отношений.

В настоящем исследовании информационные правонарушения предлагается рассматриваться в качестве различного рода деликтов (гражданско-правовых, дисциплинарных, административных, уголовных) направленных на информационную безопасность государства, выступающую в качестве неотъемлемого элемента национальной безопасности.

1.2 Информационные правонарушения в системе угроз национальной безопасности

Большое внимание в последние годы уделяется государственной деятельности в сфере обеспечения стратегического планирования. Не обошла собой данная деятельность и информационную сферу. Был принят Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», главной целью которого выступает укрепление и обеспечение информационной безопасности в Российской Федерации.

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть «Интернет»), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

Угроза информационной безопасности Российской Федерации (или информационная угроза) – это совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере.

В качестве информационной безопасности Российской Федерации (или просто информационной безопасности) законодателем рассматривается 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.

Обеспечение информационной безопасности в данном случае это осуществление взаимоувязанных правовых, организационных, оперативно-разыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

Силы обеспечения информационной безопасности - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности.

Средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности.

Система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

Информационная инфраструктура Российской Федерации понимается законодателем, как совокупность объектов информатизации, информационных систем, сайтов в сети "Интернет" и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

В Доктрине информационной безопасности на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов Российской Федерации.

Национальными интересами в информационной сфере являются:

- обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;
- обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;
- развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также

совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

- доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;
- содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих

международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации. Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Наращивается информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских

духовно-нравственных ценностей.

Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз

применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обусловливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

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

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

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети "Интернет", не позволяет реализовать совместное

справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

В соответствии с военной политикой, осуществляемой в настоящее время, Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

- стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;
- совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;
- прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;
- содействие обеспечению защиты интересов союзников Российской

Федерации в информационной сфере;

- нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности, которые можно было бы выделить в настоящее время являются:

- противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;
- пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;
- повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты

критической информационной инфраструктуры;

- повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;
- повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;
- повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;
- обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;
- совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;
- повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;
- нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных

ценностей [43].

Многочисленные посягательств на информационную сферу, которые наблюдались в последнее время, вынуждают государственные власти в принятии ответных действий, в выделении в общем массиве требований, направленных на обеспечение национальной безопасности государства, требований, преследующих вопросы обеспечения именно информационной безопасности страны.

Так, совершенно недавно Президент России Владимир Путин подписал указ о дополнительных мерах по обеспечению информационной безопасности России, сообщается на официальном интернет-портале правовой информации.

«В целях повышения устойчивости и безопасности функционирования информационных ресурсов Российской Федерации постановляю: руководителям федеральных органов исполнительней власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций и иных организаций... возложить на заместителя руководителя органа полномочия по обеспечению информационной безопасности органа, в том числе по обнаружению, предупреждению и ликвидаций последствий компьютерных атак, реагированию на компьютерные инциденты», - говорится в сообщении.

Отмечается, что президент постановил создать в организации структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа. Также в случае необходимости принимать решения о привлечении организаций к осуществлению действий по обеспечению информационной безопасности органа. Кроме того, при необходимости организации будут привлечены к обнаружению, предупреждению и ликвидации последствий компьютерных атак, реагированию на компьютерные инциденты [43].

В данном отношении следует выделить такой правовой акт, как Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

Данный закон специальным образом посвящен противодействию такой разновидности информационных правонарушений, как правонарушения компьютерные. Законодателем, в частности, в рамках данного нормативно-правового акта дается определение того, что из себя представляет компьютерная атака.

Безопасность критической информационной инфраструктуры определяется в рассматриваемом законе, как состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак.

Критическая информационная инфраструктура подразумевает включение в свой состав объектов критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов [45].

В этом отношении можно упомянуть также исследование А.А. Галушкина, большое внимание уделившему проблеме формализации и институционализации понятия информационной безопасности, его соотношению с понятием национальной безопасности [6].

Как писал В.П. Шерстюк, «информация является основой деятельности органов законодательной, исполнительной и судебной властей, всей системы государственного управления, управления Вооруженными Силами. Информационная сфера в настоящее время стала системообразующим фактором жизни общества, и чем активней эта сфера общественных отношений развивается, тем больше политическая, экономическая, оборонная и другие составляющие национальной безопасности любого государства будут зависеть от информационной безопасности, и в ходе развития технического прогресса эта зависимость будет все более возрастать» [50].

Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» содержит раздел IV. «Обеспечение национальной безопасности», в котором в качестве отдельно

структурного элемента содержится часть «Информационная безопасность».

Касательно темы нашего исследования, в данной части заостряется внимание на том обстоятельстве, что быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

Расширяется использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности.

Увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств. Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве.

Активизируется деятельность специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве. Вооруженные силы таких государств отрабатывают действия по выведению из строя объектов критической информационной инфраструктуры Российской Федерации.

В целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов. В информационно-телекоммуникационной сети «Интернет» размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, осуществляется пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ, размещается иная

противоправная информация. Основным объектом такого деструктивного воздействия является молодежь.

Стремление транснациональных корпораций закрепить свое монопольное положение в сети «Интернет» и контролировать все информационные ресурсы сопровождается введением такими корпорациями (при отсутствии законных оснований и вопреки нормам международного права) цензуры и блокировкой альтернативных интернет-платформ. По политическим причинам пользователям сети «Интернет» навязывается искаженный взгляд на исторические факты, а также на события, происходящие в Российской Федерации и в мире.

Анонимность, которая обеспечивается за счет использования информационно-коммуникационных технологий, облегчает совершение преступлений, расширяет возможности для легализации доходов, полученных преступным путем, и финансирования терроризма, распространения наркотических средств и психотропных веществ.

Использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов, включая объекты критической информационной инфраструктуры Российской Федерации, к воздействию из-за рубежа.

Целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве.

Достижение цели обеспечения информационной безопасности осуществляется путем реализации государственной политики, направленной на решение следующих задач:

- формирование безопасной среды оборота достоверной информации, повышение защищенности информационной инфраструктуры Российской Федерации и устойчивости ее функционирования;
- развитие системы прогнозирования, выявления и предупреждения

угроз информационной безопасности Российской Федерации, определения их источников, оперативной ликвидации последствий реализации таких угроз;

- предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы, включая объекты критической информационной инфраструктуры Российской Федерации;
- создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий;
- повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети «Интернет», иных значимых объектов информационно-коммуникационной инфраструктуры, а также недопущение иностранного контроля за их функционированием;
- снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных, а также уменьшение количества нарушений установленных российским законодательством требований по защите такой информации и персональных данных;
- предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки;
- обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий;
- укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной

техники;

- развитие сил и средств информационного противоборства;
- противодействие использованию информационной инфраструктуры Российской Федерации экстремистскими и террористическими организациями, специальными службами и пропагандистскими структурами иностранных государств для осуществления деструктивного информационного воздействия на граждан и общество;
- совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;
- обеспечение приоритетного использования в информационной инфраструктуре Российской Федерации российских информационных технологий и оборудования, отвечающих требованиям информационной безопасности, в том числе при реализации национальных проектов (программ) и решении задач в области цифровизации экономики и государственного управления;
- укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности, в том числе в целях установления международно-правового режима обеспечения безопасности в сфере использования информационно-коммуникационных технологий;
- доведение до российской и международной общественности достоверной информации о внутренней и внешней политике Российской Федерации;
- развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации.

Из приведенного перечня, можно сделать вывод, что основная часть информационных угроз национальной безопасности видится законодателем снаружи, а не внутри российского государства. Деятельность иностранных государств, иностранных и международных организаций часто носит деструктивный характер и посягает на национальную безопасность Российской Федерации. Использование информации и информационных технологий для создания угроз национальной безопасности и достижения своих деструктивных целей получило подобное распространение среди этих субъектов в связи с тем обстоятельством, что информационные технологии помогают осуществлять воздействие на территории другого государства не обращая внимание на наличие соответствующих государственных границ.

В данном случае возможно наступление ситуации, когда существующие механизмы и способы обеспечения национальной безопасности не смогут распознать существующую угрозу и окажутся бессильными. Кроме собственно технической стороны вопроса, информационные угрозы также могут затрагивать вопросы культурологии, психологии, социологии и иных дисциплин гуманитарного цикла, посредством знания которых противник может пытаться дестабилизировать ситуацию внутри государственных границ нашего государства. Данное обстоятельство послужило причиной того, что «традиционные» информационные угрозы, связанные, например, с похищением объектов интеллектуальной собственности или разглашением охраняемой законом тайны хотя и продолжают выделяться законодателем в настоящее время, но по степени своей актуальности уступают место угрозам иного рода, связанным с распространением и развитием движений экстремисткой и террористической направленности.

Существующие угрозы международного характера обусловили разработку и принятие Указа Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» [44].

Данный акт имеет своей целью обеспечение реализации

государственной политики Российской Федерации в области международной информационной безопасности.

Основы являются документом стратегического планирования Российской Федерации и отражают официальные взгляды на сущность международной информационной безопасности, определяют основные угрозы международной информационной безопасности, цель, задачи государственной политики Российской Федерации в области международной информационной безопасности (далее - государственная политика в области международной информационной безопасности), а также основные направления ее реализации.

Государственная политика в области международной информационной безопасности представляет собой совокупность скоординированных мер, направленных на формирование с учетом национальных интересов Российской Федерации системы обеспечения международной информационной безопасности.

Нормативно-правовую базу настоящих Основ составляют Конституция Российской Федерации, международные договоры Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности, федеральные законы и иные нормативные правовые акты Российской Федерации.

Основами конкретизируются отдельные положения Стратегии национальной безопасности Российской Федерации, Доктрины информационной безопасности Российской Федерации, Концепции внешней политики Российской Федерации и других документов стратегического планирования.

Основы направлены:

– на продвижение на международной арене российских подходов к формированию системы обеспечения международной информационной безопасности и российских инициатив в области международной информационной безопасности;

– на содействие созданию международно-правовых механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
– на организацию межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности.

Международная информационная безопасность определяется в Основах как такое состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности.

Система обеспечения международной информационной безопасности представляет собой совокупность международных и национальных институтов, регулирующих деятельность в глобальном информационном пространстве в целях предотвращения (минимизации) угроз международной информационной безопасности.

Основными угрозами международной информационной безопасности являются:

– использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;
– использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
– использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

– использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества и т.д.

Основными направлениями реализации государственной политики в области международной информационной безопасности по развитию на глобальном, региональном, многостороннем и двустороннем уровнях сотрудничества Российской Федерации с иностранными государствами по вопросам формирования системы обеспечения международной информационной безопасности являются:

– создание условий для принятия государствами - членами Организации Объединенных Наций (ООН) Конвенции об обеспечении международной информационной безопасности;
– содействие организации под эгидой ООН регулярного институционального диалога с участием всех государств - членов ООН для обеспечения демократического, инклюзивного и транспарентного переговорного процесса по вопросам безопасности в сфере использования информационно-коммуникационных технологий;
– содействие выработке с учетом специфики информационно-коммуникационных технологий новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве;
– достижение и выполнение двусторонних и многосторонних договоренностей международно-правового и иного характера между Российской Федерацией и иностранными государствами о сотрудничестве в области обеспечения международной информационной безопасности;
– проведение на регулярной основе двусторонних и многосторонних

экспертных консультаций, согласование позиций и основных направлений сотрудничества в области обеспечения международной информационной безопасности с государствами – участниками Содружества Независимых Государств (СНГ), объединения БРИКС, государствами – членами Организации Договора о коллективной безопасности (ОДКБ), Шанхайской организации сотрудничества (ШОС), Ассоциации государств Юго-Восточной Азии (АСЕАН), «Группы двадцати», другими государствами и международными организациями;

- организация международных конференций и семинаров по вопросам международной информационной безопасности;
- проведение организационно-штатных мероприятий, направленных на создание (укрепление) структурных подразделений федеральных органов исполнительной власти, участвующих в реализации государственной политики в области международной информационной безопасности, а также совершенствование координации деятельности и взаимодействия федеральных органов исполнительной власти в данной области и т.д.

Основными направлениями реализации государственной политики в области международной информационной безопасности по противодействию угрозе использования информационно-коммуникационных технологий в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности, являются:

- развитие сотрудничества с иностранными государствами в целях предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;
- содействие развитию региональных систем обеспечения международной информационной безопасности и формированию

соответствующей глобальной системы на основе общепризнанных принципов и норм международного права с учетом специфики информационно-коммуникационных технологий, а также на основе новых принципов и норм международного права, разработанных в целях предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;

- выработка на глобальном, региональном, многостороннем и двустороннем уровнях мер укрепления доверия в области противодействия использованию информационно-коммуникационных технологий для осуществления в глобальном информационном пространстве действий, представляющих угрозу международному миру, безопасности и стабильности;
- развитие переговорного процесса и повышение эффективности взаимодействия с иностранными государствами в интересах совместного противодействия вызовам и угрозам, возникающим в связи с масштабным использованием информационно-коммуникационных технологий в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, а также в целях осуществления в глобальном информационном пространстве других действий, представляющих угрозу международному миру, безопасности и стабильности;
- содействие совершенствованию под эгидой ООН принципов и норм международного гуманитарного права применительно к сфере использования информационно-коммуникационных технологий с учетом специфики данных технологий.

Основными направлениями реализации государственной политики в области международной информационной безопасности по формированию механизмов международного сотрудничества в сфере противодействия угрозе использования информационно-коммуникационных технологий в террористических целях являются:

– развитие сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, международными организациями по вопросам противодействия использованию информационно-коммуникационных технологий в террористических целях, использованию информационно-телекоммуникационной сети "Интернет" и других информационно-телекоммуникационных сетей для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;
– содействие разработке на межгосударственном уровне комплекса мер, направленных на противодействие угрозе использования информационно-коммуникационных технологий в террористических целях;
– совершенствование на глобальном, региональном, многостороннем и двустороннем уровнях механизма обмена информацией о фактах использования информационно-коммуникационных технологий в террористических целях, повышение эффективности взаимодействия уполномоченных государственных органов.

Основными направлениями реализации государственной политики в области международной информационной безопасности по созданию условий для противодействия угрозе использования информационно-коммуникационных технологий в экстремистских целях, а также в целях вмешательства во внутренние дела суверенных государств являются:

– содействие разработке и реализации на глобальном, региональном, многостороннем и двустороннем уровнях комплекса мер, направленных на противодействие угрозе использования информационно-коммуникационных технологий в экстремистских целях;
– развитие сотрудничества с иностранными государствами, их правоохранительными органами и специальными службами, а также с международными организациями, осуществляющими борьбу с

экстремизмом, по вопросам противодействия угрозе использования информационно-коммуникационных технологий в экстремистских целях;

- содействие созданию эффективного международного механизма контроля за использованием информационно-коммуникационных технологий для предотвращения их использования в экстремистских целях, а также в целях вмешательства во внутренние дела суверенных государств;
- содействие выработке порядка межгосударственного обмена информацией о распространении материалов запрещенных экстремистских организаций, а равно иной информационной продукции, содержащей материалы данных организаций.

Основными направлениями реализации государственной политики в области международной информационной безопасности по повышению эффективности международного сотрудничества, направленного на противодействие угрозе использования информационно-коммуникационных технологий в преступных целях, и по созданию необходимого для этого международно-правового режима являются:

- содействие разработке специальным межправительственным комитетом экспертов открытого состава всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также создание условий для последующего принятия государствами - членами ООН данной конвенции;
- развитие сотрудничества с государствами – участниками СНГ, объединения БРИКС, государствами - членами ОДКБ, ШОС, АСЕАН, "Группы двадцати", другими государствами и международными организациями по вопросам противодействия угрозе использования информационно-коммуникационных технологий в преступных целях;

– повышение эффективности информационного обмена между правоохранительными органами государств в ходе расследования преступлений в сфере компьютерной информации, а также случаев мошенничества с использованием информационно-коммуникационных технологий;
– совершенствование механизма обмена информацией о методиках расследования преступлений в сфере компьютерной информации, случаев мошенничества с использованием информационно-коммуникационных технологий, а также о судебной практике рассмотрения уголовных дел о таких преступлениях;
– организация международных конференций и семинаров по вопросам противодействия использованию информационно-коммуникационных технологий в преступных целях.

Основными направлениями реализации государственной политики в области международной информационной безопасности по совершенствованию межгосударственного взаимодействия, направленного на противодействие угрозе использования информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также межгосударственного взаимодействия в области реагирования на компьютерные инциденты являются:

– развитие сотрудничества с иностранными государствами, международными, международными неправительственными организациями и организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, в целях выработки механизма обмена информацией о таких инцидентах и повышения эффективности взаимодействия уполномоченных органов;
– развитие сотрудничества с государствами - участниками СНГ, объединения БРИКС, государствами - членами ОДКБ и ШОС,

другими государствами и международными организациями по вопросам реагирования на компьютерные инциденты, обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

- содействие созданию на глобальном, региональном, многостороннем и двустороннем уровнях эффективного механизма межгосударственного взаимодействия, направленного на предотвращение компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;
- содействие выработке на глобальном, региональном, многостороннем и двустороннем уровнях порядка обмена информацией о передовых практиках обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также реагирования на компьютерные инциденты;
- совершенствование взаимодействия между Национальным координационным центром по компьютерным инцидентам и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на компьютерные инциденты.

Основными направлениями реализации государственной политики в области международной информационной безопасности по созданию условий для обеспечения технологического суверенитета государств в области информационно-коммуникационных технологий и преодоления

информационного неравенства между развитыми и развивающимися странами являются:

- создание условий для противодействия использованию отдельными государствами технологического доминирования и монополизации ими различных сегментов рынка информационно-коммуникационных технологий, включая основные информационные ресурсы, критическую информационную инфраструктуру, ключевые технологии, продукты и услуги;
- содействие обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети "Интернет" на основе равноправного участия государств - членов мирового сообщества в управлении данной сетью и повышению роли Международного союза электросвязи в таком управлении;
- содействие обеспечению равного доступа государств к новейшим информационно-коммуникационным технологиям и предотвращению технологической зависимости в сфере информатизации и информационного неравенства;
- содействие разработке и реализации на глобальном, региональном, многостороннем и двустороннем уровнях международных программ, направленных на преодоление информационного неравенства между развитыми и развивающимися государствами;
- содействие развитию национальных информационных инфраструктур и равноправному участию государств в создании и использовании современных глобальных информационных сетей и систем, в том числе на основе реформирования протоколов функционирования глобальной сети связи;
- содействие обеспечению равных прав национальных коммерческих организаций - производителей товаров и услуг в сфере

информационно-коммуникационных технологий и информационной безопасности;

– повышение эффективности государственно-частного партнерства в сфере информационной безопасности, содействие участию национальных коммерческих организаций - производителей товаров и услуг в указанной сфере в международном сотрудничестве в интересах укрепления информационной безопасности Российской Федерации и формирования системы обеспечения международной информационной безопасности.

Можно прийти к выводу, что в настоящее время отечественным законодателем в полной степени были осознаны опасности, которые несут посягательства на информационную сферу. В действующих нормативно-правовых актах в сфере стратегического планирования довольно подробно были расписаны как те угрозы, которые несут посягательства на информационную сферу, так и конкретные действия, которые должны быть предприняты органами государственной власти для того, чтобы свести опасность в этом отношении к минимуму. В актах, предусматривающих санкции юридической ответственности, прежде всего, в Кодексе Российской Федерации об административных правонарушениях и в Уголовной кодексе Российской Федерации были зафиксированы соответствующие составы информационных правонарушений, которые будут рассмотрены в дальнейшем. Можно говорить о том, что в настоящее время перед государством стоит насущная задача самым непосредственным образом поменять подходы к регулированию информационных отношений и разработать новые положения, в том числе, в сфере реализации юридической ответственности, которые бы соответствовали реалиям существующих угроз и информационных опасностей.

Глава 2. Правовое регулирование в области противодействия информационным угрозам национальной безопасности

2.1 Законодательные основы противодействия информационным угрозам национальной безопасности

Задачи обеспечения информационной безопасности самым непосредственным образом проистекают из текста Конституции РФ, но прямым образом в Основном законе не были указаны. Однако, поскольку информация в настоящее время рассматривается в качестве охраняемого объекта, то в данном отношении действует статья 15 Конституции РФ [16], в соответствии с которой каждый должен соблюдать законы, а, следовательно, воздерживаться от покушений на информацию, которая данными законами охраняется.

Основополагающим нормативно-правовым актом, определяющим должный порядок поведения индивида и меры государственно-правового воздействия в виду наличия угроз для национальной безопасности со стороны информационных правонарушений, является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [46].

Указывается в рассматриваемом федеральном законе, что он регулирует отношения, возникающие при:

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

Положения этого Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, поскольку

правоотношения указанных групп базируются на нормативной базе, содержащейся в российском законодательстве.

Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

- информацию, свободно распространяемую;
- информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
- информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
- информацию, распространение которой в Российской Федерации ограничивается или запрещается.

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя. В качестве обладателя информации рассматривается гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

Обладатель информации вправе:

- разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;
- использовать информацию, в том числе распространять ее, по своему усмотрению;
- передавать информацию другим лицам по договору или на ином установленном законом основании;
- защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;
- осуществлять иные действия с информацией или разрешать осуществление таких действий.

Обладатель информации при осуществлении своих прав обязан:

- соблюдать права и законные интересы иных лиц;
- принимать меры по защите информации;
- ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

Информация в форме открытых данных размещается в сети «Интернет» с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

Граждане (физические лица) и организации (юридические лица) вправе осуществлять поиск и получение любой информации в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

Гражданин имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

Не может быть ограничен доступ к:

- нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;
- информации о состоянии окружающей среды (экологической информации);
- информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);
- информации, накапливаемой в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;
- информации, содержащейся в архивных документах архивных фондов (за исключением сведений и документов, доступ к которым ограничен законодательством Российской Федерации);
- иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо,

желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

Предоставляется бесплатно информация:

- о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;
- затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;
- иная установленная законом информация.

Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые

Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, а также требования к

размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица. Владелец сайта в сети "Интернет" обязан разместить на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, адресе электронной почты для направления заявления, , а также вправе предусмотреть возможность направления этого заявления посредством заполнения электронной формы на сайте в сети «Интернет».

При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Запрещается распространение сообщений и материалов иностранного средства массовой информации, выполняющего функции иностранного агента

и определенного в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-I «О средствах массовой информации» [8], и (или) учрежденного им российского юридического лица без указания на то, что эти сообщения и материалы созданы и (или) распространены такими лицами. Форма, требования к размещению и порядок размещения такого указания устанавливаются уполномоченным федеральным органом исполнительной власти.

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на таких принципах:

- свобода поиска, получения, передачи, производства и распространения информации любым законным способом;
- установление ограничений доступа к информации только федеральными законами;
- открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;
- равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;
- обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;
- достоверность информации и своевременность ее предоставления;
- неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;
- недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных

технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

В качестве примера рассмотрим обязанности организатора распространения информации в сети «Интернет», которые предусмотрены статьей 10.1 основополагающего в данном отношении федерального закона.

Организатором распространения информации в сети «Интернет» является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет».

Организатор распространения информации в сети «Интернет» обязан в установленном Правительством Российской Федерации порядке уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых

коммуникаций, информационных технологий и связи, о начале осуществления соответствующего вида деятельности.

Организатор распространения информации в сети «Интернет» обязан хранить на территории Российской Федерации:

- информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;
- текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети "Интернет" до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

Организатор распространения информации в сети «Интернет»обязан предоставлять информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

Организатор распространения информации в сети «Интернет» обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации

возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий. Порядок взаимодействия организаторов распространения информации в сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается Правительством Российской Федерации.

Организатор распространения информации в сети «Интернет» обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети "Интернет" возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

Организатор распространения информации в сети «Интернет» в случае осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения, не предусматриваются размещение пользователями сети «Интернет» общедоступной информации в сети «Интернет» и передача электронных сообщений неопределенному кругу лиц (далее - организатор сервиса обмена мгновенными сообщениями), также обязан:

– осуществлять идентификацию пользователей сети «Интернет», передачу электронных сообщений которых осуществляет

организатор сервиса обмена мгновенными сообщениями (далее - пользователи сервиса обмена мгновенными сообщениями), по абонентскому номеру оператора подвижной радиотелефонной связи в порядке, установленном Правительством Российской Федерации, на основании договора об идентификации, заключенного организатором сервиса обмена мгновенными сообщениями с оператором подвижной радиотелефонной связи, за исключением случаев, предусмотренных настоящим Федеральным законом;

- в течение суток с момента получения соответствующего требования уполномоченного федерального органа исполнительной власти ограничить возможность осуществления пользователем сервиса обмена мгновенными сообщениями, указанным в этом требовании, передачи электронных сообщений, содержащих информацию, распространение которой в Российской Федерации запрещено, а также информацию, распространяемую с нарушением требований законодательства Российской Федерации, в порядке, определенном Правительством Российской Федерации;
- обеспечивать техническую возможность отказа пользователей сервиса обмена мгновенными сообщениями от получения электронных сообщений от других пользователей;
- обеспечивать конфиденциальность передаваемых электронных сообщений;
- обеспечивать возможность передачи электронных сообщений по инициативе государственных органов в соответствии с законодательством Российской Федерации;
- не допускать передачу электронных сообщений пользователям сервиса обмена мгновенными сообщениями в случаях и в порядке, которые определены Правительством Российской Федерации.

Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации,

вправе осуществлять идентификацию пользователей сервиса обмена мгновенными сообщениями самостоятельно путем определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями. Правительством Российской Федерации могут устанавливаться требования к порядку определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями организатором сервиса обмена мгновенными сообщениями, являющимся российским юридическим лицом или гражданином Российской Федерации.

Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, обязан хранить сведения об идентификации абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями (далее - идентификационные сведения об абонентском номере) только на территории Российской Федерации. Предоставление третьим лицам идентификационных сведений об абонентском номере может осуществляться только с согласия пользователя сервиса обмена мгновенными сообщениями, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами. Обязанность предоставить доказательство получения согласия пользователя сервиса обмена мгновенными сообщениями на предоставление третьим лицам идентификационных сведений об абонентском номере данного пользователя сервиса обмена мгновенными сообщениями возлагается на организатора сервиса обмена мгновенными сообщениями.

Обязанности не распространяются на операторов государственных информационных систем, операторов муниципальных информационных систем, операторов связи, оказывающих услуги связи на основании соответствующей лицензии, в части лицензируемой деятельности, а также не распространяются на граждан (физических лиц), осуществляющих указанную деятельность для личных, семейных и домашних нужд. Правительством

Российской Федерации в целях применения положений настоящей статьи определяется перечень личных, семейных и домашних нужд при осуществлении информационной деятельности.

Состав информации, подлежащей хранению, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, а также порядок осуществления контроля за деятельностью организаторов распространения информации в сети «Интернет», связанной с хранением такой информации, и федеральный орган исполнительной власти, уполномоченный на осуществление этого контроля, определяются Правительством Российской Федерации.

Организатор распространения информации в сети «Интернет», имеющий уникальный идентификатор совокупности средств связи и иных технических средств в сети «Интернет», обязан выполнять требования и обязанности, предусмотренные Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи» [48] и предъявляемые к лицам, имеющим номер автономной системы.

Можно прийти к выводу, что в настоящее время законодательство, в сфере обеспечения информационных аспектов национальной безопасности, представляет собой уже довольно сложную систему, обращенную к правоотношениям, регулируемым различными отраслями российского права. Эта отрасль законодательства находится в процессе становления в отрасль российского права и в скором времени может встать в один ряд с такими «традиционными» отраслями права, как административное, гражданское, земельное или семейное. Вместе с тем, институт правового регулирования в данной области общественных отношений является в достаточной степени «новым» - он появился в советское время в качестве института охраны конфиденциальных сведений в рамках административного права, но в настоящее время содержание правового регулирования в информационной

сфере было законодателем значительно расширено.

2.2 Государственное управление в сфере противодействия информационным угрозам национальной безопасности

В качестве механизмов реализации государственной политики в области международной информационной безопасности, выделенных Президентом РФ, выступают подготовка предложений Президенту Российской Федерации по формированию, совершенствованию и реализации государственной политики в области международной информационной безопасности, контроль за реализацией федеральными органами исполнительной власти и организациями решений Президента Российской Федерации по вопросам координации деятельности в области международной информационной безопасности, решений Совета Безопасности Российской Федерации в указанной области, а также организация взаимодействия федеральных органов исполнительной власти и организаций при реализации государственной политики в области международной информационной безопасности осуществляются рабочими органами Совета Безопасности Российской Федерации.

Министерство иностранных дел Российской Федерации участвует в пределах своей компетенции во взаимодействии с федеральными органами исполнительной власти в разработке и реализации основных направлений государственной политики в области международной информационной безопасности, осуществляет координацию деятельности федеральных органов исполнительной власти по реализации указанной политики, продвижение на международной арене позиции Российской Федерации по вопросу обеспечения международной информационной безопасности, а также реализует иные полномочия в области международной информационной безопасности.

Иные федеральные органы исполнительной власти и организации

реализуют государственную политику в области международной информационной безопасности в соответствии с их компетенциями, в том числе на основе государственно-частного партнерства.

В соответствии с решением отечественного законодателя, вопросы обеспечения информационной безопасности были переданы в компетенцию Федеральной службы безопасности Российской Федерации.

В Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности» была включена статья 11.2. «Обеспечение информационной безопасности», в которой законодателем было отмечено, что «Обеспечение информационной безопасности – деятельность органов федеральной службы безопасности, осуществляемая ими в пределах своих полномочий:

- при формировании и реализации государственной и научно-технической политики в области обеспечения информационной безопасности, в том числе с использованием инженерно-технических и криптографических средств;
- при обеспечении криптографическими и инженерно-техническими методами безопасности информационно-телекоммуникационных систем, сетей связи специального назначения и иных сетей связи, обеспечивающих передачу шифрованной информации, в Российской Федерации и ее учреждениях, находящихся за пределами Российской Федерации» [47].

Нами был осуществлен поиск научных исследований, посвященных проблеме государственного управления в сфере обеспечения информационной безопасности. В качестве подобного рода работы можно выделить статью А.М-С. Бенмерабет [3]. Систему данных органов власти указанный автор предлагает обозначать следующим образом.

Федеральный орган исполнительной власти в области связи: осуществляет функции по выработке государственной политики и нормативно-правовому регулированию в области связи; осуществляет

правовое регулирование в области связи и информатизации; выполняет функции администрации связи Российской Федерации при осуществлении международной деятельности Российской Федерации в области связи. Подобным органом в настоящий момент является Министерство цифрового развития, связи и массовых коммуникаций.

Правительством Российской Федерации определяется порядок осуществления федеральным органом исполнительной власти по надзору в области связи государственного надзора за деятельностью в области связи.

Правовое положение федеральных органов исполнительной власти, осуществляющих управление в информационной сфере, закреплено Указом Президента РФ «О структуре федеральных органов исполнительной власти»

и соответствующими подзаконными нормативными правовыми актами.

Федеральными органами исполнительной власти, осуществляющими государственное управление в области информационных технологий и связи, выступают являются Федеральная служба по надзору в сфере СМИ, массовых коммуникаций, информационных технологий и связи (Роскомнадзор).

В сфере информационным технологий данным органом выполняются такие функции, как контроль за деятельностью организаторов распространения информации в сети «Интернет», связанный как с началом осуществления ими своей деятельности, так и хранением информации о фактах сообщений пользователей сети «Интернет». Кроме того, Роскомнадзор также осуществляет контроль за предоставлением обязательного экземпляра электронного издания.

Можно прийти к выводу, что в настоящее время в Российской Федерации была сформирована необходимая система органов управления в сфере обеспечения информационной безопасности и задача в настоящее время заключается в наработке ими соответствующей практики деятельности по обеспечению защиты от информационных правонарушений, а также разработка соответствующего нормативного материала в соответствующей области государственного управления.

Глава 3. Проблемы противодействия информационным правонарушениям в сфере обеспечения национальной безопасности

3.1 Проблема реализации юридической ответственности за информационные правонарушения, посягающие на национальную безопасность

Современные исследователи не могли оставить своим вниманием проблематику правонарушений в сфере защиты информации.

Проблема юридической ответственности за правонарушения в сфере информационной деятельности рассматривается в работах П.Н. Алешина [1], А.М. Воронова [5], Л.П. Коваленко [17], И.И. Костюченко, В.Н. Наконечного, П.О. Середы, А.Ю. Гуськова, А.Г. Тутубалина [17].

В качестве примера можно назвать работы некоторых исследователей, разрабатывающих проблемы обеспечения информационной безопасности.

Так, в работе А.А. Кодинец [15] осуществлен теоретический подход к юридической ответственности за информационные правонарушения.

В.А. Максименковым рассматриваются проблемы реализации института уголовной ответственности за правонарушения в информационной сфере [23], а Д.К. Жидковой, Е.С. Маркеловой [7], а также А.Г. Суханова [39] – вопросы административной ответственности за указанные посягательства. В.М. Матвеева рассматривает возможность привлечения субъектов к дисциплинарной ответственности за совершение подобных правонарушений [25].

Н.Н. Ковалева [12] пытается спрогнозировать тенденции развития административной ответственности за административные правонарушения в будущем.

Т.М. Занина и Е.И. Лукина [9] анализируют в своей работе проблематику юридической ответственности за посягательство на ифнормационную безопасность несовершеннолетних лиц.

А.А. Лосева пытается осуществить общую систематизацию противоправных деяний, совершаемых в сфере информационных технологий [21]. Подобным же образом построено и исследование А.Х Кипкеева [11].

Все же, несмотря на наличие определенного рода научных работ по рассматриваемому предмету, представляется, что количество проводимых в настоящее время исследований рассматриваемой проблемы в целом невелико и не соответствуют важности посягательств на информационную сферу. Современную человеческую цивилизацию часто называют информационной, поскольку информация лежит в основе не только производства товаров, оказания работ и выполнения услуг, но и имеет определяющее влияние на жизнь каждого отдельного человека. Совершая информационные правонарушения, тем самым, нарушители посягают на сами основы существования нашей цивилизации, в связи с чем количество исследований, в которых бы рассматривались эти проблемы, должно быть гораздо большим.

Кроме того, несмотря на наличие в современной литературе работ, в которых бы рассматривалась угроза, исходящая от посягательств на информационную сферу, практически никто из ученых, занимающихся этим вопросом, не связывает данные правонарушения с угрозой национальной безопасности, что в создавшихся в настоящее время условиях выглядит необъяснимым.

В данном отношении можно было бы выделить труд О.А. Федотовой, но он был написан около двадцати лет назад и успел значительно устареть [49].

Из современных исследований можно назвать статью В.В. Мочалова, который анализирует вопросы безопасности критической информационной инфраструктуры [26].

Незначительным является и количество диссертационных (в этом отношении можно назвать также уже устаревшее исследование А.В. Полушкина [30]) и монографических исследований рассматриваемой области.

Нами было проведено исследование судебной практики, которое показало, что подобного рода посягательства довольно часто выступают

предметом рассмотрения в судах различного уровня.

Так, например, Волгоградский областной суд в 2020 году [32] рассмотрев в открытом судебном заседании жалобу Баринова А.А. на определение судьи Ленинского районного суда Волгоградской области от 20 июля 2020 года о возврате жалобы без рассмотрения по существу на постановление заместителя начальника отдела ФСБ России войсковая часть 62094 от 9 июня 2020 года по делу об административном правонарушении, предусмотренном частью 7 статьи 13.12 Кодекса Российской Федерации об административных правонарушениях, в отношении охранника, обеспечивающего охрану груза в пути следования, Баринова А.А.

В Решении № 2А-989/2020 2А-989/2020~М-801/2020 М-801/2020 от 22 июля 2020 г. по делу № 2А-989/2020 Железнодорожный районный суд г. Рязани [34].

За нарушение требований о защите информации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, предусмотрена административная ответственность по ст. 13.12 КоАП РФ. Проследим, какими наказаниями может быть представлена ответственность за нарушение информационной безопасности. В Решении № 2А-989/2020 2А-989/2020~М-801/2020 М-801/2020 от 22 июля 2020 г. по делу № 2А-989/2020 Железнодорожный районный суд г. Рязани, рассмотрев в открытом судебном заседании в здании суда административное дело по административному исковому заявлению Рязанского транспортного прокурора, поданному в интересах неопределенного круга лиц, к Краснову И.В. о признании информации запрещенной к распространению,установил:, что Рязанский транспортный прокурор, действуя в интересах неопределенного круга лиц, обратился в суд с административным иском к Краснову И.В. о признании информации запрещенной к распространению. Исковые требования мотивированы тем, что Рязанской транспортной прокуратурой в рамках осуществления мероприятий по надзору за соблюдением таможенного

законодательства в ходе мониторинга информации, размещенной в сети «Интернет», установлен факт размещения в сети «Интернет» информации о приобретении базы данных таможенных органов по экспортно-импортным операциям участников внешнеэкономической деятельности.

На данном сайте приводится ссылка на демо-версию базы данных таможенных органов, пройдя по которой любой пользователь получает доступ к файлу в exel-формате, содержащему исчерпывающие сведения о поставках, декларантах по различным параметрам. В базе данных таможенных органов содержатся сведения об оформленных товарах, с указанием номеров деклараций, ИНН отправителя, получателя, декларанта, страны происхождения товаров, номеров транспортных средств, фамилий, имен, отчеств их представителей, контактных телефонов, а также иная информация.

Вход на сайт является свободным, демо-версии базы предлагаются любому пользователю.

Между тем, предлагаемые на сайте к приобретению базы данных таможенных органов содержат в себе информацию ограниченного доступа о декларантах, отправителях, получателях и иных участниках таможенных отношений, составляют информационные ресурсы таможенных органов и носят ограниченный характер.

Более того, ст. 7 Федерального закона от 27.07.2006 № 125-ФЗ «О персональных данных» установлен запрет лицам, получившим доступ к персональным данным, раскрывать их третьим лицам и распространять персональные данные без согласия субъекта персональных данных. База данных таможенных органов содержит сведения о представителях организаций-декларантов, отправителей и иных участников таможенных отношений, а именно - их фамилии, имена, отчества, телефоны, что в силу ст. 3 названного закона является персональными данными и носит ограниченный характер.

За нарушение требований о защите информации, установленных федеральными законами и принятыми в соответствии с ними иными

нормативными правовыми актами Российской Федерации, предусмотрена административная ответственность по ч. 6 ст. 13.12 КоАП РФ.

При таких обстоятельствах распространение в сети Интернет информации о продаже баз данных таможенных органов является незаконным, соответствующий интернет-ресурс подлежат включению в Реестр.

Прокурор просит суд:

- признать информацию, распространяемую посредством сети «Интернет» и размещенную на интернет-ресурсе о предоставлении бесплатно и за плату баз данных таможенных органов, информацией, распространение которой в Российской Федерации запрещено;
- направить копию решения суда в Управление Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций для включения в «Единые реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»;
- обязать владельца сайта удалить интернет-страницы, содержащие информацию, распространение которой запрещено;
- решение обратить к немедленному исполнению.

Исходя из смысла закона, злоупотребление свободой массовой информации – использование предоставленных средствами массовой информации гарантий прав и свобод во вред обществу или государству.

Судья по данному делу полностью удовлетворил требования прокурора.

Следующим проанализированным нами решением стало Решение № 12-279/2019 12-39/2020 от 6 февраля 2020 г. по делу № 12-279/2019 Ленинского районного суда г. Красноярска [33] по делу об административном правонарушении, предусмотренном ч. 3 ст. 13.12 КоАП РФ в отношении

должностного лица исполняющего обязанности заместителя генерального директора, директор по персоналу и общим вопросам АО «Красмаш» Остроушенко М.В.

Было установлено, что в соответствии с номенклатурой должностей работников, подлежащих оформлению на допуск к особой важности, совершенно секретным и секретным сведениям, должность начальника технологического бюро цеха № АО «Красмаш» предполагает наличие допуска к государственной тайне. Приказом заместителя генерального директора, директора по персоналу и общим вопросам АО «Красмаш» Остроушенко М.В. от 09.09.2019г., на период вакансии начальника бюро цеха № АО «Красмаш» исполнять обязанности в объеме должностной инструкции возложены на Б Н.В. не имеющего допуск к государственной тайне по установленной форме. что является нарушением требований п. 6 Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне, утвержденной постановлением Правительства РФ от 06.02.2010г. №631. В приказе от 09.09.2019г. подписанном Остроушенко М.В. об исполнении Б Н.В. обязанностей начальника бюро цеха № на период вакансии, отсутствует информация о наличии у нее допуска к государственной тайне по форме.Остроушенко М.В. обратился в суд с жалобой на постановление № от 29.10.2019г., просит обжалуемое постановление отменить и производство по делу прекратить, ссылаясь на то, что п.6 Инструкции о порядке допуска к гос.тайне утвержденный постановлением правительства РФ от 06.02.2010г. № не нарушал, поскольку должность начальника технологического бюро цеха № АО «Красмаш» предполагает наличие допуска к гос.тайне по установленной форме, но приказом от 09.09.2019 на период вакансии начальника цеха № АО «Красмаш» исполнение обязанности в объеме должностной инструкции возложены на Б Н.В. имеющий допуск к гос.тайне по другой форме.

Исследовав материалы дела об административном правонарушении, суд считает вина должностного лица не доказана.

Согласно ч. 1 ст. 19.7.13 КоАП РФ, предусмотрена административная

ответственность за нарушение условий, предусмотренных лицензией на проведение работ, связанных с использованием и защитой информации, составляющей государственную тайну, созданием средств, предназначенных для защиты информации, составляющей государственную тайну, осуществлением мероприятий и (или) оказанием услуг по защите информации, составляющей государственную тайну, что влечет наложение административного штрафа на должностных лиц в размере от двух тысяч до трех тысяч рублей.

Согласно п. 6 Инструкции о порядке допуска должностных лиц и граждан РФ к государственной тайне, утвержденной постановлением Правительства РФ от 06.02.2010г. №631, ели по характеру выполняемых должностных (специальных, функциональных) обязанностей предусматривается доступ к сведениям, составляющим государственную тайну, граждане могут быть назначены на эти должности только после оформления допуска к государственной тайне по соответствующей форме.

Допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, как это предусмотрено в ст.27 Закона РФ от 21.07.1993г. №5485-1 "О государственной тайне", осуществляется путем получения ими в порядке, устанавливаемом Правительством РФ, лицензий на проведение работ со сведениями соответствующей степени секретности.

Лицензия на проведение работ с использованием сведений, составляющих государственную тайну, выдается предприятию, учреждению, организации при выполнении ими следующих условий: выполнение требований нормативных документов, утверждаемых Правительством РФ, по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений; наличие в их структуре подразделений по защите государственной

тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны; наличие у них сертифицированных средств защиты информации.

Сотрудникам АО «Красмаш» при наличие допуска к государственной тайне по одной форме, предоставляется допуск к гос.тайне по иной форме, доказательств обратного не представлено, т.е. назначение на временную должность (в период отпуска, временной нетрудоспособности и т.д.), не изменяет форму допуска к государственной тайне, и к обратному выводу из приказа от 09.09.2019г. прийти нельзя.

Постановление начальника СЭБ УФСБ России по Красноярскому краю №6/164-19 от 29.10.2019г. по делу об административном правонарушении, предусмотренном ч. 3 ст. 13.12 КоАП РФ в отношении должностного лица исполняющего обязанности заместителя генерального директора, директор по персоналу и общим вопросам АО «Красмаш» Остроушенко МВ, отменить производство по делу прекратить, в связи с отсутствием состава административного правонарушения по п.2 ч.1 ст. 24.5 КоАП.

В плане противодействия информационным преступлениям Уголовный кодекс Российской Федерации [41] не содержит отдельной структурной единицы текста нормативно-правового акта, которая была бы посвящена указанному вопросу.

Так, в нем содержится Глава 28 УК РФ «Преступления в сфере компьютерной информации», которая включает в свой состав только четыре статьи:

- неправомерный доступ к компьютерной информации (статья 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-

телекоммуникационных сетей (статья 274 УК РФ);

– неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274.1 УК РФ).

Однако в других главах Уголовного кодекса РФ также можно обнаружить отдельные составы информационных преступлений.

Сюда можно отнести такие составы преступлений, как, например:

– клевета – в том числе, посредством использования сети «Интернет» (ст. 128.1 УК РФ);
– нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ);
– незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ);
– государственная измена, в том числе, посредством разглашения охраняемой законом тайны (ст. 275 УК РФ) и т.д.

Объект посягательства в данном случае различен. Можно прийти к выводу, что у создателей Уголовного кодекса РФ еще не укрепилось представление о необходимости выделения информационных составов преступления в отдельную главу Уголовного кодекса РФ.

Совершенно иным образом обстоит ситуация с административным законодательством. Кодекс Российской Федерации об административных правонарушениях [14] содержит отдельную главу 13, которая называется «Административные правонарушения в области связи и информации».

К правонарушениям в области информации в данной главе можно отнести

– нарушение законодательства Российской Федерации в области персональных данных (ст. 13.11 КоАП РФ);
– распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера (ст. 13.11.1 КоАП РФ);

- нарушение правил защиты информации (ст. 13.12 КоАП РФ);
- нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (ст. 13.12.1 КоАП РФ);
- незаконная деятельность в области защиты информации (ст. 13.13 КоАП РФ);
- разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ);
- незаконное получение информации с ограниченным доступом (ст. 13.14.1 КоАП РФ);
- злоупотребление свободой массовой информации (ст. 13.15 КоАП РФ);
- воспрепятствование распространению продукции средства массовой информации (ст. 13.16 КоАП РФ);
- нарушение правил распространения обязательных сообщений (ст. 13.17 КоАП РФ);
- непредоставление первичных статистических данных (ст. 13.19 КоАП РФ);
- нарушение порядка размещения информации в государственной информационной системе жилищно-коммунального хозяйства (ст. 13.19.1 КоАП РФ);
- неразмещение информации, размещение информации не в полном объеме или размещение недостоверной информации в государственной информационной системе жилищно-коммунального хозяйства (ст. 13.19.2 КоАП РФ);
- нарушение порядка размещения информации в единой информационной системе жилищного строительства (ст. 13.19.3 КоАП РФ);
- нарушение порядка представления сведений в федеральный реестр

инвалидов и размещения указанных сведений в данном реестре (ст. 13.19.4 КоАП РФ);

- нарушение правил хранения, комплектования, учета или использования архивных документов (ст. 13.20 КоАП РФ);
- нарушение порядка изготовления или распространения продукции средства массовой информации (ст. 13.21 КоАП РФ);
- нарушение порядка объявления выходных данных (ст. 13.22 КоАП РФ);
- нарушение требований законодательства о хранении документов и информации, содержащейся в информационных системах (ст. 13.25 КоАП РФ);
- нарушение сроков и (или) порядка доставки (вручения) адресату судебных извещений (ст.13.26 КоАП РФ);
- нарушение требований к организации доступа к информации о деятельности государственных органов и органов местного самоуправления и ее размещению в сети «Интернет» (ст. 13.27 КоАП РФ);
- нарушение требования о размещении на территории Российской Федерации технических средств информационных систем (ст. 13.27.1 КоАП РФ);
- нарушение порядка предоставления информации о деятельности государственных органов и органов местного самоуправления (ст. 13.28 КоАП РФ);
- неисполнение обязанностей организатором распространения информации в сети «Интернет» (ст. 13.31 КоАП РФ);
- неисполнение обязанностей владельцем новостного агрегатора (ст. 13.32 КоАП РФ);
- 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 (ст. 13.34 КоАП РФ);

- нарушение владельцем аудиовизуального сервиса установленного порядка распространения среди детей информации, причиняющей вред их здоровью и (или) развитию (ст. 13.36 КоАП РФ);
- 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 (ст. 13.37 КоАП РФ);
- неисполнение обязанностей организатором сервиса обмена мгновенными сообщениями (ст. 13.39 КоАП РФ);
- неисполнение обязанностей оператором поисковой системы (ст. 13.40 КоАП РФ);
- 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 (ст. 13.41 КоАП РФ);
- нарушение установленного федеральным законом запрета публичного отождествления целей, решений и действий руководства СССР, командования и военнослужащих СССР с целями, решениями

и действиями руководства нацистской Германии, командования и военнослужащих нацистской Германии и европейских стран оси в ходе Второй мировой войны, а также отрицания решающей роли советского народа в разгроме нацистской Германии и гуманитарной миссии СССР при освобождении стран Европы (ст. 13.48 КоАП РФ).

Приведенный в КоАП РФ обширный перечень административных правонарушений показывает, как широк с точки зрения законодателя, объект подобного рода противоправных деяний и сколь различны противоправные действия субъектов, которыми может осуществляться посягательство на информационную сферу.

Можно прийти к выводу, в связи с этим, что в настоящее время вопросам обеспечения информационной безопасности в российском государстве уделяется самое непосредственное внимание. Определены были органы, призванные функционировать в сфере обеспечения информационной безопасности. Обозначены многие процедуры и механизмы, непосредственно направленные на ее обеспечение. Государством ведется постоянная оценка новых угроз, возникающих в сфере обеспечения информационной безопасности, в этом отношении принимаются новые федеральные законы и подзаконные правовые акты, направленные на парирование соответствующих опасностей.

Развивая нормативное регулирование соответствующей сферы общественных отношений, законодатель пытается определить наилучшие механизмы их регулирования и защиты. Ранее с подобного рода общественными отношениями, проистекающими в информационной сфере, отечественный законодатель еще не сталкивался.

Вопросы реализации мер юридической ответственности за совершение противоправных деяний носят основополагающий характер при выделении отдельных институтов и отраслей российского права, поскольку они показывают на самостоятельную ценность соответствующей группы общественных отношений и необходимость их защиты. За информационные

правонарушения виновные лица могут быть привлечены как к административной и уголовной, так и к дисциплинарной и гражданско-правовой ответственности. Считаем, что большое внимание, которое уделяется информационной сфере в последние годы, позволяет говорить о зарождении такой новой разновидности или отрасли российского права, как право информационное, которое начало процесс своего выделения из административного права Российской Федерации. Не последнюю роль здесь имеет и выделение отдельной разновидности информационных правонарушений со своими специфическими санкциями и мерами государственного реагирования на их совершение.

3.2 Предложения в сфере противодействия информационным правонарушениям, посягающим на национальную безопасность

Законодательство об информационных правонарушениях начало формироваться по историческим меркам не так давно, в связи с чем сложившуюся систему норм в указанной сфере сложно признать оптимальной.

Многими исследователями, в числе которых можно назвать, например, А.В. Кравцова [18], А.А. Кудинову и Н.И. Соболева [20], Я.В. Порбину [31], Д.Б. Савчишкина [36], В.Е. Степенко и А.Г. Суханова [37], М.Е. Трофимову [40], отмечается, что, несмотря на достигнутые успехи в сфере теоретического изучения и законодательного закрепления института юридической ответственности за информационные правонарушения, данная сфера не является свободной и от определенного рода проблем, которые часто сводят на нет соответствующие усилия законодателя.

Представляется, что ряд из этих проблем проистекает из-за того, что информационное законодательство в настоящее время представляет собой совокупность нормативно-правовых актов различного уровня. Сталкиваясь с новыми аспектами, требующими обеспечить охрану информационной сферы, законодатель часто не дополняет существующие акты, а принимает новый акт

по указанному вопросу. И обывателю (в качестве которых в данном случае выступают как граждане, так и юридические лица) и представителям правоохранительной системы довольно сложно учесть все многообразие нормативно-правовых актов, существующих в данном отношении, в рамках своей повседневной профессиональной деятельности.

Представляется, что выход в данном случае может быть найден в проведении систематизации законодательства, касающегося оборота информации. Исторический опыт развития отечественной юриспруденции показывает, что после определенного момента в развитии законодательной отрасли, встает необходимость принятия кодифицированного акта (кодекса, «основ» или устава) посвященного рассматриваемому вопросу. Можно в данном случае провести аналогию с жилищным законодательством, которое, точно также как и информационное, вышло первоначально из административного права.

Первые жилищные правоотношения возникли в нашем государстве в момент Великой Октябрьской революции, когда появился институт договора социального найма и людей начали заселять в квартиры, которые не принадлежали им по праву собственности. Через шестьдесят пять лет – в 1983 году был принят Жилищный кодекс РСФСР, сейчас уже действует второй Жилищный кодекс в истории нашего государства (2004 года). Жилищные отношения развиваются также быстро, как и отношения информационные, но законодатель находит выход и включает целые главы и разделы в действующий текст Жилищного кодекса РФ.

Информационное право также начало формироваться довольно давно, в частности, посредством принятия нормативно-правовых актов, в которых бы содержался запрет на распространение сведений, составляющих конфиденциальную информацию и охраняемую законом тайну. Считаем, что в настоящее время настало время для принятие кодифицированного акта; данный процесс предлагается разбить на два этапа.

На первом этапе целесообразно собрать все существующие акты в сфере

защиты информации в один нормативно-правовой акт без изменения его содержания (консолидация). Это не потребует больших трудозатрат законодателя и позволит воочию наблюдать в одном нормативно-правовом акте всю совокупность нормативного материала, который был разработан к настоящему времени в сфере защиты информации.

На втором этапе следует провести систематизацию данного материала с тем, чтобы кодифицированный акт – Информационный кодекс РФ – пришел на смену существующему в настоящее время массиву правовой информации в рассматриваемой области. Те вопросы, которые в будущем должны быть закреплены в статусе федерального закона, целесообразно будет вводить в Информационный кодекс посредством новых глав и разделов; иные установления можно вводить посредством принятия подзаконных нормативно-правовых актов, издаваемых на основе и во исполнение Информационного кодекса.

Что касается ответственности за совершение информационных правонарушений, можно прийти к выводу, что разработка самостоятельного института юридической ответственность не является целесообразной. По аналогии, например, с Земельном кодексом РФ, в Информационном кодексе может содержаться норма, что «за нарушение требований данного кодекса следует уголовная, гражданско-правовая, административная и иная ответственность, предусмотренная законодательством Российской Федерации».

Считаем, что осуществление указанных действий позволит нормализовать ситуацию и повысить эффективность противодействия информационными правонарушениями, посягающим на национальную безопасность.

Заключение

Можно отметить значительную дискуссионность относительно понимания понятия «информационное правонарушение», которая продолжает сохраняться в настоящее время. Отсутствие единства среди ученых относительно названия соответствующей группы правонарушений может означать отсутствие единства и по поводу перечня соответствующих противоправных деяний. Подобная несогласованность в юридической науки самым негативным образом отражается на законотворчестве и практике применения соответствующего института юридической ответственности, что позволяет говорить о важности достижения задачи скорейшего достижения ясности в рассматриваемой сфере общественных отношений.

В настоящем исследовании информационные правонарушения предлагается рассматриваться в качестве различного рода деликтов (гражданско-правовых, дисциплинарных, административных, уголовных) направленных на информационную безопасность государства, выступающую в качестве неотъемлемого элемента национальной безопасности.

В настоящее время отечественным законодателем в полной степени были осознаны опасности, которые несут посягательства на информационную сферу. В действующих нормативно-правовых актах в сфере стратегического планирования довольно подробно были расписаны как те угрозы, которые несут посягательства на информационную сферу, так и конкретные действия, которые должны быть предприняты органами государственной власти для того, чтобы свести опасность в этом отношении к минимуму. Можно говорить о том, что в настоящее время перед государством стоит насущная задача самым непосредственным образом поменять подходы к регулированию информационных отношений и разработать новые положения, в том числе, в сфере реализации юридической ответственности, которые бы соответствовали реалиям существующих угроз и информационных опасностей.

В настоящее время законодательство, в сфере обеспечения информационных аспектов национальной безопасности, представляет собой уже довольно сложную систему, обращенную к правоотношениям, регулируемым различными отраслями российского права. Эта отрасль законодательства находится в процессе становления в отрасль российского права и в скором времени может встать в один ряд с такими «традиционными» отраслями права, как административное, гражданское, земельное или семейное. Вместе с тем, институт правового регулирования в данной области общественных отношений является в достаточной степени «новым» - он появился в советское время в качестве института охраны конфиденциальных сведений в рамках административного права, но в настоящее время содержание правового регулирования в информационной сфере было законодателем значительно расширено.

Можно отметить в связи с этим, что в настоящее время вопросам обеспечения информационной безопасности в российском государстве уделяется самое непосредственное внимание. Определены были органы, призванные функционировать в сфере обеспечения информационной безопасности. Обозначены многие процедуры и механизмы, непосредственно направленные на ее обеспечение. Государством ведется постоянная оценка новых угроз, возникающих в сфере обеспечения информационной безопасности, в этом отношении принимаются новые федеральные законы и подзаконные правовые акты, направленные на парирование соответствующих опасностей.

Развивая нормативное регулирование соответствующей сферы общественных отношений, законодатель пытается определить наилучшие механизмы их регулирования и защиты. Ранее с подобного рода общественными отношениями, проистекающими в информационной сфере, отечественный законодатель еще не сталкивался.

Вопросы реализации мер юридической ответственности за совершение противоправных деяний носят основополагающий характер при выделении

отдельных институтов и отраслей российского права, поскольку они показывают на самостоятельную ценность соответствующей группы общественных отношений и необходимость их защиты. За информационные правонарушения виновные лица могут быть привлечены как к административной и уголовной, так и к дисциплинарной и гражданско-правовой ответственности.

Считаем, что большое внимание, которое уделяется информационной сфере в последние годы, позволяет говорить о зарождении такой новой разновидности или отрасли российского права, как право информационное, которое начало процесс своего выделения из административного права Российской Федерации. Не последнюю роль здесь имеет и выделение отдельной разновидности информационных правонарушений со своими специфическими санкциями и мерами государственного реагирования на их совершение.

Информационные правонарушения, посягающие на информационную безопасность очень многообразны и закрепляются в настоящее время в различных институтах различных отраслей права, объема выпускной квалификационной работы далеко недостаточно, чтобы детально рассмотреть все существующие здесь составы правонарушений.

В настоящее время в Российской Федерации была сформирована необходимая система органов управления в сфере обеспечения информационной безопасности и задача в настоящее время заключается в наработке ими соответствующей практики деятельности по обеспечению защиты от информационных правонарушений, а также разработка соответствующего нормативного материала в соответствующей области государственного управления.

Список используемой литературы и используемых источников

1. Алешин П.Н. Совершенствование законодательства в профилактике правонарушений в сфере информационной безопасности // Проблемы укрепления законности и правопорядка в современном обществе. сборник научных статей. Стерлитамак, 2015. - С. 4-8.
2. Байсаева М. У. Компьютерные правонарушения и информационные правонарушения: аспекты соотношения // Международный журнал прикладных наук и технологий Integral. – 2020. – № 3. – С. 20.
3. Бенмерабет А.М-С. Государственное управление в области информации // Актуальные проблемы российского права, 2007, №2. – С. 102-108.
4. Букалерова Л. А. Специфика уголовной, административной, гражданско-правовой ответственности за информационные правонарушения в системе публичного управления // NB: Административное право и практика администрирования. – 2015. – № 1. – С. 81-94.
5. Воронов А.М. Административная ответственность за правонарушения в сфере информационного обеспечения общественной безопасности // Вестник Академии экономической безопасности МВД России. - 2007. - № 1. - С. 66-69.
6. Галушкин А. А. К вопросу о значении понятий "национальная безопасность", "информационную безопасность", "национальная информационная безопасность" // Правозащитник. – 2015. – № 2. – С. 8.
7. Жидкова Д.К., Маркелова Е.С. Проблемные вопросы административной ответственности за правонарушения в сфере информационной безопасности // Итоги научно-исследовательской деятельности 2016: изобретения, методики, инновации. сборник материалов XVII международной научно-практической конференции. - 2016. - С. 416-417.
8. Закон Российской Федерации от 27 декабря 1991 года № 2124-I «О средствах массовой информации» // СПС «КонсультантПлюс»

9. Занина Т.М., Лукина Е.И. Правовые проблемы привлечения к административной ответственности за правонарушения в сфере информационной безопасности несовершеннолетних // Наука и практика. - 2016. - № 2 (67). - С. 47-49.

10. Заярный О. Вина как конструктивный элемент состава административного информационного правонарушения: некоторые проблемы доктринального определения и практического установления // Юстиция Беларуси. – 2015. – № 12(165). – С. 37-41.

11. Кипкеев А.Х. Правонарушение в сфере информационных технологий // Современный мир: опыт, проблемы и перспективы развития. - 2016. - № 3. - С. 8-11

12. Ковалёва Н.Н. тенденции развития административной ответственности за информационные правонарушения в РФ // Научные записки Международного гуманитарного университета. сборник. Ответственный редактор К.В. Громовенко. - 2016. - С. 49-51.

13. Коваленко Л.П. Юридическая ответственность за правонарушения в сфере информационной деятельности // Проблемы законности.- 2012. - № 120. - С. 184-191

14. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ // СПС «КонсультантПлюс»

15. Кодинец А.А. Теоретические аспекты деликтной ответственности за правонарушения в информационной сфере // Известия Гомельского государственного университета имени Ф. Скорины. - 2015. - № 5 (92). - С. 81-86.

16. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020 г.) // Российская газета от 4 июля 2020 г. № 144

17. Костюченко И.И., Наконечный В.Н., Середа П.О., Гуськов А.Ю., Тутубалин А.Г. К вопросу о методах прогнозирования правонарушений в

информационных системах // Научная мысль Кавказа. Междисциплинарные и специальные исследования. - 2010. - № 2 (14). - С. 27-33.

18. Кравцов А.В. Административная ответственность за информационные правонарушения: позитивный опыт российского законотворчества // Развитие административного и финансового права. Сборник материалов 1-го ежегодного международного круглого стола. - 2017. - С. 75-79.

19. Кручинина С. А. Интеллектуализация системы управления расследованием правонарушений (инцидентов) информационной безопасности в финансовой сфере // Ресурсам области - эффективное использование : Сборник материалов XVII Ежегодной научной конференции студентов Технологического университета, Королёв, 01 ноября 2017 года. – Королёв: Общество с ограниченной ответственностью "Научный консультант", 2017. – С. 153-162.

20. Кудинова А.А., Соболева Н.И. К вопросу о правонарушениях в сфере информационных технологий // Новая наука: Современное состояние и пути развития. - 2017. - № 1-2. - С. 129-132.

21. Лосева А.А. Правонарушения в сфере информационных технологий // Теоретические и практические аспекты развития юридической науки. Сборник статей Международной научно-практической конференции. 2017. С. 185-187.

22. Макарова А. А. Некоторые вопросы ответственности за правонарушения в сфере информационных технологий // Актуальные проблемы и перспективы развития предварительного следствия в России, Волгоград, 14 июля 2020 года. – Волгоград: ИП Черняева Ю.И., 2020. – С. 226-229.

23. Максименков В.А. Уголовная ответственность за правонарушения в информационной сфере // Студенческий вестник. - 2020. - № 39-2 (137). - С. 6-8.

24. Марущак А. И. Европейский опыт по борьбе с правонарушениями в информационной сфере / А. И. Марущак // Безпека інформації. – 2019. – Т. 25. – № 1. – С. 13-17.

25. Матвеева В. М. Дисциплинарная ответственность за правонарушения в информационной сфере // Интернаука. – 2019. – № 45-2(127). – С. 37-38.

26. Мочалов В.В. Юридическая ответственность за правонарушения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Вестник Уральского института экономики, управления и права. - 2021. - № 1 (54). - С. 77-79.

27. Ноздрина Н. А. Виды юридической ответственности за правонарушения в информационной сфере / Н. А. Ноздрина // Закономерности и тенденции инновационного развития общества : сборник статей по итогам Международной научно-практической конференции, Стерлитамак, 28 января 2019 года. – Стерлитамак: Общество с ограниченной ответственностью "Агентство международных исследований", 2019. – С. 146-154.

28. Осенькина, К. В. К вопросу о привлечении к административной ответственности за правонарушения в информационной сфере / К. В. Осенькина, Е. В. Ширманов // Актуальные проблемы уголовного права и процесса, уголовно-исполнительного права и криминалистики : Материалы VIII научно-практической конференции, Саранск, 29 марта 2019 года / Редколлегия: Г.П. Кулешова [и др.]. – Саранск: Общество с ограниченной ответственностью "ЮрЭксПрактик", 2019. – С. 162-167.

29. Полушкин А. В. Информационное правонарушение: понятие и виды : : автореферат диссертации на соискание ученой степени кандидата юридических наук. – Екатеринбург, 2009. – 26 с.

30. Полушкин А.В. Информационное правонарушение: понятие и виды: диссертация на соискание ученой степени кандидата юридических наук - Екатеринбург, 2009. – 189 с.

31. Порбина Я.В. Ответственность за правонарушение в информационной сфере // Студенческий вестник. - 2020. - № 13-2 (111). - С. 71-72.

32. Решение № 07-1093/2020 от 9 сентября 2020 г. по делу № 07-1093/2020 Волгоградский областной суд [Электронный ресурс] // URL: sudact.ru

33. Решение № 12-279/2019 12-39/2020 от 6 февраля 2020 г. по делу № 12-279/2019 Ленинского районного суда г. Красноярска [Электронный ресурс] // URL: sudact.ru

34. Решение № 2А-989/2020 2А-989/2020~М-801/2020 М-801/2020 от 22 июля 2020 г. по делу № 2А-989/2020 Железнодорожный районный суд г. Рязани [Электронный ресурс] // URL: sudact.ru

35. Савенкова, Д. Д. Правовое обеспечение информационной безопасности в Российской Федерации и развитие института ответственности за правонарушения в информационной сфере // Динамика институтов информационной безопасности. Правовые проблемы : Сборник научных трудов, Москва, 03–04 февраля 2017 года. – Москва: Канон Плюс, РООИ "Реабилитация", 2018. – С. 118-124.

36. Савчишкин, Д. Б. Квалификация административных правонарушений в информационной сфере / Д. Б. Савчишкин // Полицейская деятельность. – 2011. – № 3. – С. 52-57.

37. Степенко В.Е., Суханов А.Г. Административная ответственность за правонарушения в информационной сфере // Юридический мир. - 2020. - № 8.- С. 49-53.

38. Стромов, В. Ю. Предупреждение совершения правонарушений в информационной сфере в контексте оптимизации противодействия организованной преступности // Проблемы изучения и противодействия организованной преступности : сборник статей по материалам Всероссийского круглого стола, Санкт-Петербург, 20 февраля 2015 года. – С. 121-127.

39. Суханов А.Г. Актуальные проблемы привлечения к административной ответственности за правонарушения в информационной сфере // Администратор суда. 2019. № 1. С. 23-27.

40. Трофимова М. Е. Правонарушения в области информационных технологий // Вестник научных конференций. – 2021. – № 4-2(68). – С. 122-123.

41. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ // Собрание законодательства Российской Федерации от 17 июня 1996 г. № 25 ст. 2954.

42. Указ Президента от 1 мая 2022 №250 «О дополнительных мерах по повышению информационной безопасности Российской Федерации»

43. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12 декабря 2016 г. N 50 ст. 7074

44. Указа Президента РФ от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности» // СПС «КонсультантПлюс»

45. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации от 31 июля 2017 г. № 31 (часть I) ст. 4736

46. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Собрание законодательства Российской Федерации от 31 июля 2006 г. N 31 (часть I) ст. 3448

47. Федеральный закон от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»// Собрание законодательства Российской Федерации от 10 апреля 1995 г. N 15 ст. 1269

48. Федеральный закон от 7 июля 2003 года № 126-ФЗ «О связи» // СПС «КонсультантПлюс»

49. Федотова О.А. Административная ответственность за правонарушения в сфере обеспечения информационной безопасности : диссертация на соискание ученой степени кандидата юридических наук – М.: 2003. – 203 с.

50. Шерстюк, В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. – 1999. – № 5. – С. 3-5.

51. Шувалов О. А. Роль общественных организаций правоохранительной направленности в сфере профилактики преступлений и правонарушений в информационном пространстве // Государство и право в России и мире. Правонарушение. Преступление. Ответственность. – 2014. – № 1. – С. 16.

52. Юренков О. Г. Социальные детерминанты правонарушений в сфере информационных технологий: социологический анализ : диссертация на соискание ученой степени кандидата социологических наук / Юренков Олег Григорьевич. – Санкт-Петербург, 2004. – 183 с.