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: «Обеспечение национальной безопасности в информационной сфере»

Студент Е.В. Подзорова
(И.О. Фамилия) (личная подпись)

Руководитель к. ю. н., В.В. Романова.
(ученая степень, звание, И.О. Фамилия)

Тольятти 2021

Аннотация

Тема выпускной квалификационной работы: «Обеспечение национальной безопасности в информационной сфере».

Актуальность данной работы выражается в прогрессивном развитии информационной области, так как с появлением новых и усовершенствованием старых технологий, способов хранения, обработки и передачи информации, возникает все больше потенциальных уязвимостей, которые в последующем могут нанести ущерб личности, обществу и государству.

Целью работы является глубокое изучение и анализ теоретических и нормативных положений, касающихся национальной и информационной безопасности Российской Федерации.

Для реализации поставленной цели, необходимо решить такие задачи как:

– определить понятие национальной безопасности;

– выявить основные угрозы и классифицировать их;

– проанализировать основные направления государства в области обеспечения информационной безопасности;

– изучить нормативно-правовые акты, имеющие прямое влияние на обеспечение информационной безопасности;

– ознакомится с актами правового регулирования права на доступ к информации в иностранных государствах.

Структура выпускной квалификационной работы состоит из введения, двух глав, разделенных на восемь параграфов, заключения и списка используемой литературы и используемых источников. Работа состоит из 90 страниц.

Оглавление

Введение

Рассматривая данную тему, мы столкнёмся с проблемами, касающимися важных процессов, которые происходят в наше время, самой основной из них будет влияние информации, не только на все сферы нашей жизни, но и на национальную безопасность государства, что в свою очередь выражает всю важность и актуальность моей работы.

Информация представляет собой сведения, сообщения и данные независимо от формы их представления. Еще с древних времен, с появлением письменности, лица, обладающие какой-либо информацией, которая должна была остаться в секрете, прибегали к разным способам ее защиты, общеизвестными из них можно назвать шифрование или тайнопись.

Сейчас с учетом происходящей информатизации, многое зависит от информационно безопасности огромного количества систем, хранящих данные, которые могут повлиять на состояние защищенности личности, общества и государства, а также на возможность управления объектами, создающих угрозу национальной безопасности и контроль над данными объектами. К ним можно отнести системы телекоммуникаций, обработки и хранения секретной информации, атомные станции, систему управления наземным и воздушным транспортом, банковские системы, системы формирования общественного сознания и это не исчерпывающий перечень систем, дня нормального функционирования которых требуется поддержание их безопасности и целостности.

Из этого следует, что информационная безопасность должна развиваться также стремительно как информационные технологии, так как затрагивает все возможные сферы общества: политическую, экономическую, экологическую, военную, промышленную, научную, техническую, социальную и многие другие.

Так как тема моей выпускной квалификационной работы «Обеспечение национальная безопасности в информационной сфере», то основными объектом будут выступать общественные отношения, влияющие на безопасность в данной сфере, а также немаловажным объектом в данной теме является обеспечение и реализация конституционно-правовых и непосредственно связанных с ними норм, на доступ к информации.

В качестве предмета исследования выступают интересы и угрозы национальной безопасности, информационная безопасность и нормативно - правовое регулирование в данных областях.

Целью моей работы является глубокое изучение и анализ теоретических и нормативных положений, касающихся национальной и информационной безопасности Российской Федерации.

Для реализации поставленной цели, необходимо решить такие задачи как:

– определить понятие национальной безопасности;

– выявить основные угрозы и классифицировать их;

– проанализировать основные направления государства в области обеспечения информационной безопасности;

– изучить нормативно-правовые акты, имеющие прямое влияние на обеспечение информационной безопасности.

Проведен анализ трудов следующих ученых: Т.М. Бикташева, К.В. Бородина, Н.Б. Ельчаниновой, И.Л. Бачило, М. А. Федотова, Н.Е. Колобаевой, П.У. Кузнецова, А.С. Петречука, Т.А. Тимербаева и других.

Нормативно-правовой базой исследования являются: Конституция Российской Федерации, федеральные законы и другие нормативные правовые акты, регулирующие и информационную безопасность в Российской Федерации.

Выпускная квалификационная работа состоит из введения, двух глав, заключения и списка используемой литературы и используемых источников.

Глава 1 Понятие национальной безопасности. Интересы и угрозы национальной безопасности

1.1 Правовые основы национальной безопасности РФ

Национальная безопасность имеет особое значение для всего государства, так как охватывает особо значимые аспекты. Впервые в нашей стране термин «национальная безопасность», был представлен в Федеральном законе от 20 февраля 1995 г. N 24-ФЗ «Об информации, информатизации и защите информации» [52], но его сущность и содержание не были раскрыты. Послание Президента РФ Федеральному Собранию от 23.02.1996 определило, что «Национальная безопасность понимается как состояние защищенности национальных интересов от внутренних и внешних угроз, обеспечивающее прогрессивное развитие личности, общества и государства» [27].

Следующим важным шагом стал Указ Президента РФ от 17 декабря 1997 г. N 1300 «Об утверждении Концепции национальной безопасности Российской Федерации» [41]. Данная Концепция представляет собой «Политический документ, отражающий совокупность официально принятых взглядов на цели и государственную стратегию в области обеспечения безопасности личности, общества и государства от внешних и внутренних угроз политического, экономического, социального, военного, техногенного, экологического, информационного и иного характера с учетом имеющихся ресурсов и возможностей». В ней так же дается определение Национальной безопасности, под ней понимается «безопасность ее многонационального народа как носителя суверенитета и единственного источника власти в Российской Федерации». Судя по вышеуказанному, можно сделать вывод о том, что безопасность личности легла в основу данной Концепции.

28 декабря 2010 года был подписан новый Федеральный закон N 390-ФЗ (ред. От 09.11.2020) «О безопасности» [61], его основное отличие состоит в том, что он не содержит элементов раскрытия понятийного аппарата, вместе с тем, в нем конкретизированы принципы обеспечения безопасности, а также элементы процесса деятельности различных институтов власти по обеспечению безопасности Российской Федерации.

Основываясь на Конституции, Федеральном законе от 28 декабря 2010 г. N 390-ФЗ «О безопасности», и от 28 июня 2014 г. N 172-ФЗ «О стратегическом планировании в Российской Федерации», а также иных нормативно правовых актах, был введен, действующий в наше время Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» [44].

В общих положениях данной Стратегии, Национальная безопасность Российской Федерации представлена как «состояние защищенности личности, общества и государства от внутренних и внешних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан Российской Федерации, достойные качество и уровень их жизни, суверенитет, независимость, государственная и территориальная целостность, устойчивое социально-экономическое развитие Российской Федерации. Национальная безопасность включает в себя оборону страны и все виды безопасности, предусмотренные Конституцией Российской Федерации и законодательством Российской Федерации, прежде всего государственную, общественную, информационную, экологическую, экономическую, транспортную, энергетическую безопасность, безопасность личности».

Из данного определения можно выделить 3 вида объекта национальной безопасности:

- личность, ее права и свободы;
- общество и его уровень жизни;

– государство и его суверенитет, независимость, территориальная целостность и т.д.

Для эффективности сохранения в безопасности этих трёх объектов в Указе Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации» [44], указаны национальные интересы, то есть объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития и важнейшие направления обеспечения национальной безопасности, которые также называют – стратегические национальные приоритеты.

Национальные интересы на долгосрочную перспективу:

– укрепление обороны страны, обеспечение незыблемости конституционного строя, суверенитета, независимости, государственной и территориальной целостности Российской Федерации;

– укрепление национального согласия, политической и социальной стабильности, развитие демократических институтов, совершенствование механизмов взаимодействия государства и гражданского общества;

– повышение качества жизни, укрепление здоровья населения, обеспечение стабильного демографического развития страны;

– сохранение и развитие культуры, традиционных российских духовно-нравственных ценностей;

– повышение конкурентоспособности национальной экономики;

– закрепление за Российской Федерацией статуса одной из лидирующих мировых держав, деятельность которой направлена на поддержание стратегической стабильности и взаимовыгодных партнерских отношений в условиях полицентричного мира.

Из этого можно сделать вывод, что национальные интересы многоаспектны и затрагивают все необходимые сферы для нормального функционирования личности, общества и государства. Но для обеспечения

национальных интересов необходима реализация следующих стратегических национальных приоритетов:

- оборона страны;
- государственная и общественная безопасность;
- повышение качества жизни российских граждан;
- экономический рост;
- наука, технологии и образование;
- здравоохранение;
- культура;
- экология живых систем и рациональное природопользование;
- стратегическая стабильность и равноправное стратегическое партнерство.

Из понятия, предложенного в Стратегии национальной безопасности, можно выделить основные виды безопасности:

- государственную и общественную безопасность, которые можно определить как важнейшие составляющие национальной безопасности, выражающиеся в защите конституционного строя, суверенитета, государственной и территориальной целостности Российской Федерации, основных прав и свобод человека и гражданина, сохранение гражданского мира, политической и социальной стабильности в обществе, защита населения и территорий от чрезвычайных ситуаций природного и техногенного характера;
- информационную безопасность, понятие которой содержится в утвержденной Указом Президента РФ от 5 декабря 2016 г. № 646 «Доктрине информационной безопасности Российской Федерации» [36], и представляет собой, «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»;

– экологическую безопасность, представляющая собой «состояние защищенности природной среды и жизненно важных интересов человека от возможного негативного воздействия хозяйственной и иной деятельности, чрезвычайных ситуаций природного и техногенного характера, их последствий», об этом сказано в ст.1 Федеральном законе «Об охране окружающей среды» от 10.01.2002 N 7-ФЗ [49];

– экономическую безопасность, содержание которой можно найти в Указе Президента РФ от 13.05.2017 N 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» [38], «Экономическая безопасность – состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов Российской Федерации»;

– транспортную безопасность, представляющую собой «состояние защищенности объектов транспортной инфраструктуры и транспортных средств от актов незаконного вмешательства», на первый взгляд данное определение является узким и может показаться, что оно не сможет охватить всё, что может повлиять на безопасное использование транспорта. Разберем данное понятие на составные части:

Во-первых, к объектам транспортной инфраструктуры, как к технологическому комплексу следует относить:

– железнодорожные вокзалы и станции, автовокзалы и автостанции;

– объекты инфраструктуры внеуличного транспорта. Перечень объектов можно найти в Постановление Правительства РФ от 22 декабря 2018 г. N 1636 «Об утверждении перечня объектов инфраструктуры

внеуличного транспорта (в части метрополитенов), являющихся объектами транспортной инфраструктуры» [29];

– тоннели, эстакады, мосты;

– морские терминалы, акватории морских портов;

– порты, которые расположены на внутренних водных путях и в которых осуществляются посадка (высадка) пассажиров и (или) перевалка грузов повышенной опасности;

– расположенные во внутренних морских водах, в территориальном море, исключительной экономической зоне и на континентальном шельфе Российской Федерации искусственные острова, установки, сооружения, в том числе гибко или стационарно закрепленные в соответствии с проектной документацией на их создание по месту расположения плавучие (подвижные) буровые установки (платформы), морские плавучие (передвижные) платформы, за исключением подводных сооружений (включая скважины);

– аэродромы и аэропорты;

– определяемые Правительством Российской Федерации участки автомобильных дорог, железнодорожных и внутренних водных путей, вертодромы, посадочные площадки, а также обеспечивающие функционирование транспортного комплекса здания, сооружения и помещения для обслуживания пассажиров и транспортных средств, погрузки, разгрузки и хранения грузов повышенной опасности и (или) опасных грузов, на перевозку которых требуется специальное разрешение;

– здания, строения, сооружения, обеспечивающие управление транспортным комплексом.

Вторым элементом данного определения выступает категория «транспортные средства», она представляет собой – устройства, предназначенные для перевозки физических лиц, грузов, багажа, ручной клади, личных вещей, животных или оборудования, установленных на

указанных транспортных средствах устройств, в значениях, определенных транспортными кодексами и уставами, и включающие в себя: транспортные средства автомобильного транспорта, используемые для регулярной перевозки пассажиров и багажа; воздушные суда гражданской авиации; воздушные суда авиации общего назначения; суда, используемые в целях торгового мореплавания; суда, используемые на внутренних водных путях для перевозки пассажиров, за исключением прогулочных судов, спортивных парусных судов, и (или) для перевозки грузов повышенной опасности, допускаемых к перевозке по специальным разрешениям; железнодорожный подвижной состав, осуществляющий перевозку пассажиров и (или) грузов повышенной опасности, допускаемых к перевозке по специальным разрешениям в порядке, устанавливаемом Правительством Российской Федерации; транспортные средства городского наземного электрического транспорта.

Третьим элементом, выступают «акты незаконного вмешательства», они представляют собой противоправное действие (бездействие), в том числе террористический акт, угрожающее безопасной деятельности транспортного комплекса, повлекшее за собой причинение вреда жизни и здоровью людей, материальный ущерб либо создавшее угрозу наступления таких последствий.

Теперь разобравшись с формулировками, используемыми в ст.1 Федерального закона «О транспортной безопасности» от 09.02.2007 N 16-ФЗ [47] с уверенностью можно сказать, что транспортная безопасность содержит в себе очень много объектов и видов транспорта, но законодательством урегулирована в полном объеме.

– энергетическая безопасность, согласно утвержденной распоряжением Правительства РФ от 13 ноября 2009 г. № 1715-р «Энергетическая стратегия России на период до 2030 года» представляет собой «состояние защищенности страны, ее граждан, общества, государства и экономики от угроз дефицита и обеспечения их потребностей в

энергоносителях экономически доступными энергетическими ресурсами приемлемого качества, от угроз нарушений бесперебойности энергоснабжения»;

– безопасность личности, можно определить как состояние защищенности конституционных прав и свобод человека и гражданина, которые являются обязанностью государства, так как согласно ст.2 «Конституции Российской Федерации» (принятой всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020) [16], «Человек, его права и свободы являются высшей ценностью. Признание, соблюдение и защита прав и свобод человека и гражданина – обязанность государства».

Также в определении национальной безопасности представленной в Стратегии, говорится о «защищенности личности, общества и государства от внутренних и внешних угроз». Угрозу, в обобщенном виде можно понимать, как намерение причинить кому-либо или чему-либо, тот или иной ущерб, вред. А угроза национальной безопасности является «совокупностью условий факторов, создающих прямую или косвенную возможность нанесения ущерба национальным интересам» это определение закреплено в вышеуказанной Стратегии национальной безопасности.

Угрозы можно классифицировать по разным основаниям, например, по месту зарождения:

– внутренние, к которым можно отнести: насильственное изменение конституционного строя, создание незаконных вооруженных формирований, социальное неблагополучие и низкий уровень жизни большей части населения, высокий коррупционный уровень, распространение вещей изъятых из гражданского оборота в Российской федерации, повсеместное нарушение правопорядка, терроризм и сепаратизм, ослабление технического и научно-технического потенциала, ухудшение

экологической ситуации, угрозы физического здоровья населению и многое другое;

– внешние, которые выражаются в снижении роли Российской Федерации в мировой экономике из-за действий иностранных государств; размещение около границ Российской Федерации вооруженных сил иностранных государств и протекающие вооружённые конфликты; международный терроризм; деятельность иностранных государств, объединений и организаций по сбору информации, которая в последующем может нанести ущерб национальным интересам; риск снижения политического, экономического, военного влияния Российской федерации в мировом сообществе; увеличение количества оружия массового поражения и нарушение договоров о сокращение вооружений; перечисленный мною список внешних угроз не является ограниченным и постоянно дополняется исходя из ситуации в мире.

По сферам воздействия можно разделить, на угрозы в:

– экономической сфере;
– экологической сфере;
– информационной сфере;
– оборонной сфере;
– социальной сфере;
– научно-технической сфере;
– политической сфере;
– и иных сферах.

Исходя из данной классификации, можно сделать вывод о том, что угрозы национальной безопасности имеют разный характер, степень опасности и сферы распространения, что приводит к различным последствиям, даже по их продолжительности и объему. Угрозы представляют собой очень изменчивый фактор, они могут усиливаться, уменьшаться, появляться и исчезать, изменять сферу воздействия и свою

масштабность, также одновременно может возникать неопределенное количество угроз разных по степени восприятия и вероятности осуществления. В зависимости от данных характеристик будет изменяться и значимость этих угроз для Российской Федерации. Именно поэтому правильное определение и прогнозирование приоритетов является очень важным направлением деятельности государственных органов, необходимыми для того, чтобы распределить имеющиеся силы, средства и ресурсы, позволяющие обеспечить высший уровень национальной безопасности от имеющихся угроз.

В настоящее время в нашей стране, определение угроз и их прогнозирование, осуществляется своевременно и это увеличивает возможность предотвращения или уменьшение воздействия внутренних и внешних угроз на безопасность личности, общества и государства.

1.2 Информационная безопасность РФ

В настоящее время, информационная безопасность является одним из важнейших направлений в обеспечении национальной, так как с появлением новых и усовершенствованием старых технологий, способов хранения, обработки и передачи информации, возникает все больше потенциальных уязвимостей, которые в последующем могут нанести ущерб личности, обществу и государству. Исходя из этого, в данной сфере законодательством Российской федерации, разработан большой перечень нормативно-правовых актов, включающий в себя:

– Конституцию Российской Федерации, рассмотрев ее содержание, можно ознакомиться с большим количеством статей, которые составляют основу информационной безопасности. Закрепление данных прав в основном законе государства обеспечивает их приоритет и гарантирует реализацию, а равно контроль их надлежащего исполнения со стороны государства.

– Доктрину информационной безопасности Российской Федерации, утвержденную Указом Президента РФ от 5 декабря 2016 г. № 646, это документ представляющий систему официальных взглядов на обеспечение национальной безопасности в информационной сфере. Данный документ собрал в себе все важные элементы в этой области. В его состав вошли: понятийный аппарат, основные национальные интересы, касающиеся информационной безопасности, информационные угрозы, стратегические цели и основные направления обеспечения информационной безопасности, а также организационные основы обеспечения безопасности.

– Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 08.06.2020) «Об информации, информационных технологиях и о защите информации», названый закон призван регулировать отношения, возникающие при осуществлении прав на передачу, поиск, получение, производство и распространение информации, а равно применение информационных технологий и обеспечении защиты информации. Он приводит классификацию на такие категории как: общедоступная и информация с ограниченным доступом. По порядку предоставления можно разделить на свободно распространяемую, информацию обязательного предоставления, ограниченного распространения и запрещенную. Выделяются различные обязанности, меры, особенности, порядок ограничения информации в определенных ситуациях, защита информации и ответственность в случае совершения правонарушений в указанной сфере.

– Федеральный закон «О безопасности» от 28.12.2010 г. N 390-ФЗ, ранее сталкиваясь с этим нормативно-правовым актом, мы определили, что важнейшие направления его деятельности, определяются как «состояние защищенности личности, общества и государства» от различных угроз, информационные угрозы не исключение, следовательно, все, что содержится в данном законе, имеет большое значение для поддержания информационной безопасности.

– Закон РФ «О государственной тайне» от 21.07.1993 N 5485-1 [9], представляющий собой нормативно-правовой акт, содержащий в себе, защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной, и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Регулирует доступ к данной информации, порядок ее предоставления, сортирует по степени секретности, содержит перечень сведений составляющих государственную тайну, основные ограничения и дозволения, ответственность и контрольно-надзорные функции за соблюдением данного закона.

– Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ [59], регулирует отношения связанные с обработкой и доступом к персональным данным, с использованием автоматизированных систем или без таковых, осуществляемыми всеми уровнями государственной власти, местного самоуправления, юридическими лицами и физическими лицами. Настоящий закон устанавливает ограничения доступа к информации и обеспечивает защиту прав и свобод человека и гражданина при обработке его персональных данных, что в том числе, позволяет обеспечивать конституционные права граждан на неприкосновенность частной жизни, личную и семейную тайну.

– Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ [63], исходя из содержания ст.3 «коммерческая тайна - режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду», то есть сфера регулирования данного закона, направленна на общественные отношения в области установления, изменения и прекращения режима коммерческой

тайны, в отношении информации имеющей ценность в связи с ее недоступностью для третьих лиц. Закон четко регламентирует права на отнесение информации к коммерческой тайне, права обладателя такой информации, охрану конфиденциальности таких сведений по разным категориям, а также ответственность за нарушение норм данного нормативно-правового акта.

– «Уголовный кодекс Российской Федерации» от 13.06.1996 N 63-ФЗ [35], также содержит перечень статей, предусматривающих ответственность за нарушение информационной безопасности, так например, законодатель выделяет главу 28 «Преступления в сфере компьютерной информации», но помимо данной главы, можно выделить ст.138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст.159.6 УК РФ «Мошенничество в сфере компьютерной информации», ст.183 УК РФ «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну».

– «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ [14]. В целях пресечения административных правонарушений в информационной сфере, законодатель выделяет главу 13 «Административные правонарушения в области связи и информации», но так же в статьях особенной части есть нормы касающиеся нарушения в данной сфере, такие как: ст. 5.4 «Нарушение порядка представления сведений об избирателях, участниках референдума», ст.5.5 «Нарушение порядка участия средств массовой информации в информационном обеспечении выборов, референдумов, общероссийского голосования», ст. 5.12 «Изготовление, распространение или размещение агитационных материалов с нарушением требований законодательства о выборах и референдумах», ст.5.25. «Непредоставление сведений об итогах голосования или о результатах выборов» ст. 5.29 «Непредоставление

информации, необходимой для проведения коллективных переговоров и осуществления контроля за соблюдением коллективного договора, соглашения», также очень важной является ст.5.39 «Отказ в предоставлении информации» в случаях, когда получение такой информации предусмотрено федеральным законодательством. Таким образом, осуществляется информационная безопасность в случае совершения правонарушений

Представлений мною перечень нормативно-правовых актов не является исчерпывающим, так как в наше время, информация имеет большой круг распространения и оказывает влияние на все сферы жизни общества, это приводит к тому, что государство призвано обеспечивать безопасность по всем направлениям, из этого следует, что каждый принятый на территории Российской Федерации законодательный акт, в какой-то степени регулирует общественные отношения с целью обеспечения информационной безопасности.

Ознакомившись с большим количеством нормативно-правовых актов, можно сказать о том что, «информационная безопасность – это 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» [36].

1.3 Место информационной безопасности в системе национальной безопасности

Для того что бы определить место информационной безопасности, нам необходимо обратиться к п.113 «Стратегии национальной безопасности» [44], в которой говориться, что «При реализации настоящей Стратегии

особое внимание уделяется обеспечению информационной безопасности с учетом стратегических национальных приоритетов». Исходя из этого, можно сделать вывод, что информационная безопасность является одним из приоритетных направлений, в том числе и для обеспечения национальной безопасности.

Так 5 декабря 2016 года Указом президента РФ была утверждена «Доктрина информационной безопасности» [36], в которой закреплены «национальные интересы в информационной сфере, законодатель относит к ним:

– 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. Выше мною уже были разобраны нормы Конституции РФ, которые как раз обеспечивают информационную безопасность, это говорит нам о том, что основной закон нашего государства обеспечивает состояние защищенности личности, общества и государства в информационной сфере, что введет к стабильности национальной безопасности.

– обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации и единой сети электросвязи Российской Федерации. Информационная инфраструктура представлена в виде совокупности 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 данном определении, особое значение уделяется «критической инфраструктуре», в ст.2 Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [56], она определяется как «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». К объектам законодатель относит «информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры».

Информационные системы представляют собой «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств» [58], в рамках национальной безопасности они существуют для реализации полномочий государственных органов и обеспечения обмена информацией между этими органами. То есть в случае нарушения работы государственной информационной системы, возможна дестабилизация государственного аппарата, что являться угрозой национальной безопасности.

Информационно-телекоммуникационные сети, являются «технологическими системами, предназначенными для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники» [58], нарушение в работе данных систем приводит к опасным, деструктурирующим, ущемляющим интересы страны информационным воздействиям, в области, как внедрения, так и получение доступа к информации.

Автоматизированные системы управления критической информационной инфраструктурой, представляют собой «комплекс

программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами» [56], осуществляется такими субъектами как: «государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах определённых законом» [56]. В пример можно привести такие сферы как: здравоохранение, науки, транспорта, энергетики, обороны и многое другое.

– 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. Все вышесказанное связанно с тем, что в наше время процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов, могут привести к угрозам безопасности личности, общества и государства, в том случае если развитие информационных технологий в нашей стране будет минимальным и оно не сможет противостоять другим государствам в данной области.

Помимо этого, развитие данной отрасли приводит к повышению эффективности государственного управления; развитию свободного, устойчивого и безопасного взаимодействия граждан и организаций, органов государственной власти Российской Федерации, органов местного самоуправления; повышение эффективности государственного управления,

развитие экономики и социальной сферы; безопасности граждан и государства в информационной сфере.

– 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. Это является очень важным аспектом, так как доведение до общественности недостоверной информации, может вызнать недопонимание со стороны населения и привести к занижению уровня легитимности или конфликтам.

– 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.

Так, рассмотрев национальные интересы, касающиеся информационной безопасности, можно сделать вывод о том, что в наше время данная сфера является ведущей для национальной безопасности, она включает в себя все объекты, на которые может быть направленна информационная угроза.

1.4 Права граждан в информационной сфере

В нашей стране данные права нашли свое отражение в первую очередь в основном законе государства, а именно в Конституции Российской Федерации [16], это говорит нам о том, что государство уделяет особое

внимание информационным правам граждан и гарантирует их исполнение и защиту для нашего многонационального народа.

В первую очередь хотелось бы уделить внимание ч. 4 ст.29 Конституции РФ, в которой говорится, что «Каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом», в данной статье также содержаться ограничение касающиеся сведений составляющих государственную тайну. Из этого следует, что законодатель наделил нас широким перечнем информационных прав, реализация которых допустима без предварительного уведомления и разрешения государства и государственных органов независимо от методов, способов и форм выражения, данное право не подлежит ограничению, за исключением сведений составляющих государственную тайну. Это означает, что данное ограничение действует для поддержания безопасности нашей страны, защиты основ конституционного строя, здоровья, нравственности и защиты прав и интересов других лиц.

Помимо этого Конституция РФ предоставляет нам такие права как:

– п.1 ст. 23 «Каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени». В подтверждение к вышесказанному наш основной закон закрепил в п.1 ст.24 что, «Сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются».

– п.2 ст.23 «Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений»;

– п.2 ст.24 обязывает органы государственной власти и местного самоуправления обеспечить возможность ознакомления документами и материалами, лиц, чьи права и свободы они затрагивают;

– в ст.28 говорится о том, что каждый имеет право распространять религиозные убеждения и действовать в соответствии с ними.

– вернувшись к ст.29 нужно еще упомянуть о том, что каждому гарантируется право на свободу слова и мысли, никто не может быть принужден к выражению своих мнений и убеждений, а также данная статья гарантирует свободу массовой информации;

– ст.33 «Право обращаться лично, а также направлять индивидуальные и коллективные обращения в государственные органы и органы местного самоуправления»;

– из ст.41 можно сделать вывод о том что, люди имеют право обладать информацией об угрозах их жизни и здоровью;

– ст.42 содержит себе право на достоверную информацию о состоянии окружающей среды;

– ст.51 дает право не свидетельствовать против себя, своего супруга и близких родственников.

Таким образом, Конституция РФ отображает основные права человека и гражданина в информационной сфере. Безусловно, перечень представленных прав довольно объемный, но государство призвано их реализовывать и контролировать законность их исполнения, именно поэтому они могут быть ограничены, но только в случаях, регламентированных федеральными законами, либо в случае, если они затрагивают права и свободы других лиц.

Если расценивать права на информацию, как систему закрепленных государством в законодательстве средств и способов реализации субъектом информационных отношений своих прав, то нормы Конституции РФ, как раз выступают постоянно развивающейся юридической гарантией в информационной сфере.

Еще одним не маловажным правовым актом в данной области выступает Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 30.12.2020) «Об информации, информационных технологиях и о защите информации» [58], действующим для реализации прав граждан на поиск, получение,

передачу, производство, распространение, защиту информации и использование информационных технологий.

На основе принципов изложенных в ст.3 данного Федерального закона:

– «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».

Обладатель информации в ст.6 наделяется такими правами как:

– «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».

Помимо этого, в п.3 ст.7 посвящённой общедоступной информации, то есть той, к которой относятся общеизвестные сведения и иная информация, доступ к которой не ограничен, говорится: «Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации» [58].

Ст.8 раскрывает нам «Право на доступ к информации». Данной статьей предоставляется право гражданам на получение от государственных органов, органов местного самоуправления, их должностных лиц информации, непосредственно затрагивающей его права и свободы. Организациям предоставляется 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.

Общим правом, как для граждан, так и для организаций является, право на поиск и получение информации из любых источников и в любых формах, с учетом соблюдения законодательства.

В п.4 данной статьи утверждает, что есть информация, доступ к которой не может быть ограничен, никаким образом, кроме случаев прямо установленных федеральным законодательством:

– «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;

– информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств

– информации, накапливаемой в открытых фондах библиотек, музеев, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан и организаций такой информацией;

– информации, содержащейся в архивных документах архивных фондов;

– иной информации, недопустимость ограничения доступа к которой установлена федеральными законами» [58].

Еще немало важным является то, что гражданам предоставляется право, на бесплатное получение информации о деятельности государственных органов и органов местного самоуправления, при условии размещения данной информации в информационно-телекоммуникационных сетях, а так же если информация затрагивает права и обязанности заинтересованного лица. Предоставленные условия являются наиболее значимыми, но их перечень не ограничен, об это нам говорит п.3 ч.8 ст.8 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» [58], в котором сказано «иная установленная законом информация», так же предоставляется бесплатно.

Таким образом, мы осветили основные права граждан, изложенные в данном законе, что наталкивает на мысль Т. А. Тимербаева который в своей работе «Право граждан на информацию», сделал выводы, что «Свободный доступ граждан к информации является необходимым атрибутом современной демократии, поэтому информация, создаваемая государственными органами во всех сферах и на уровнях, должна быть доступной для населения, а любые официальные запреты на такой доступ должны особым образом обосновываться и затрагивать как можно меньшую часть этой информации» [33].

С.Ю. Лапин, в своей статье «Понятие права граждан на информацию» приводит в пример такие нормативно-правовые как «Федеральный закон от 13 января 1995 г. № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» который касается вопросов об обеспечении распространения в государственных СМИ некоторого обязательного минимума информации в основном о текущей работе высших органов власти страны, а также непосредственного доступа к информации - посещения заседаний органов власти. Федеральный закон от 22 октября 2004 г. N 125-ФЗ «Об архивном деле в Российской Федерации», а также Федеральный закон от 29 декабря 1994 г. N 78-ФЗ «О библиотечном деле» устанавливают некоторые правовые гарантии граждан по получению информации из открытых архивов, в состав которых входит также официальная информация о деятельности органов власти» [20].

Получение информации о деятельность органов власти является важным фактором информационного общества. Н.Е. Колобаева в своей статье «право на доступ к информации о деятельности органов власти», раскрывает понятие информации о деятельности органов государственной власти, таким образом: «Это сведения (сообщения, данные) любой формы представления, созданные в пределах своих полномочий государственными

органами, их территориальными органами, органами местного самоуправления или организациями, подведомственными государственным органам, органам местного самоуправления либо поступившие в указанные органы и организации» [15]. Данное понятие указывает на большой объем информации находящейся в ведении данных органов, именно по этому урегулированию данного вопроса отведено особое внимание. Как я уже говорила, ст. 8 Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» [58], содержит в себе нормы позволяющие гражданам и организациям получение информации от государственных органов, органов местного самоуправления, и должностных лиц. Это касается как сведений затрагивающих права и свободны данных лиц, так и информации о деятельности указанных органов и использования ими бюджетных средств. Единственным ограничением данного права являются сведения, составляющие государственную или служебную тайну.

Реализовать право на получение такой информации можно в нескольких формах:

– инициатором получения информации является гражданин;

– информация распространяется непосредственно органами власти.

Что касается права получения информации от государственных органов гражданами, то Федеральный закон «О порядке рассмотрения обращений граждан Российской Федерации» от 02.05.2006 N 59-ФЗ, дает возможность «обращаться лично, а также направлять индивидуальные и коллективные обращения, включая обращения объединений граждан, в том числе юридических лиц, в государственные органы, органы местного самоуправления и их должностным лицам, в государственные и муниципальные учреждения и иные организации, на которые возложено осуществление публично значимых функций, и их должностным лицам» [45], в том числе в виде заявлений с просьбой о содействии в реализации его

конституционных прав и свобод на получение информации. Помимо этого ст.5 уже известного нам Федерального закона «Об информации, информационных технологиях и о защите информации» говорит нам, что «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» [58]. Об этом также сказано в работе А. С. Петречука, «Правовое регулирование доступа к информации о деятельности органов государственной власти и местного самоуправления» в которой выделяет такую важную гарантию обеспечения информационного права гражданином, при обращение в государственный или муниципальный орган как электронная форма, он объясняет это так: «В целях реализации права граждан и организаций на информацию в электронной форме государственные органы и органы местного самоуправления подключают свои информационные системы к сети Интернет, открывают для неограниченного доступа свои официальные сайты, выделяют адреса электронной почты для получения запросов и передачи запрашиваемой информации» [26]. Таким образом, данные нормы дают нам возможность осуществить свое право на получение информации удобным способом. По общим правилам государственные органы должны предоставить ответ на наше обращение в течение 30 дней с момента регистрации обращения, но случае нарушения прав граждан на доступ к информации, они имеют возможность обжаловать действия или бездействие

органов власти в вышестоящий орган, вышестоящему должностному лицу или в суд.

Информация, которая распространяется непосредственно органами власти, регулируется Федеральным законом от 09.02.2009 N 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» [48]. Представленный закон обязует вышеуказанные органы активно распространять информацию, что позволяет субъектам данных правоотношений находить нужную им информацию с минимальными затратами времени на ее получение. Ст. 6 данного закона выделяет такие способы обеспечения доступа к информации, как:

– «обнародование (опубликование) государственными органами и органами местного самоуправления информации о своей деятельности в средствах массовой информации;

– размещение государственными органами и органами местного самоуправления информации о своей деятельности в сети «Интернет»;

– размещение государственными органами и органами местного самоуправления информации о своей деятельности в помещениях, занимаемых указанными органами, и в иных отведенных для этих целей местах;

– ознакомление пользователей информацией с информацией о деятельности государственных органов и органов местного самоуправления в помещениях, занимаемых указанными органами, а также через библиотечные и архивные фонды;

– присутствие граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, государственных органов и органов местного самоуправления, на заседаниях коллегиальных государственных органов и коллегиальных органов местного самоуправления, а также на заседаниях коллегиальных

органов государственных органов и коллегиальных органов, органов местного самоуправления;

– предоставление пользователям информацией по их запросу информации о деятельности государственных органов и органов местного самоуправления;

– другими способами, предусмотренными законами и (или) иными нормативными правовыми актами, а в отношении доступа к информации о деятельности органов местного самоуправления - также муниципальными правовыми актами» [48].

Данные способы обеспечения доступа к информации образуют такие права пользователя информацией как те, что изложены в ст.8 представленного Федерального закона, они включают в себя право:

– «получать достоверную информацию о деятельности государственных органов и органов местного самоуправления;

– отказаться от получения информации о деятельности государственных органов и органов местного самоуправления;

– не обосновывать необходимость получения запрашиваемой информации о деятельности государственных органов и органов местного самоуправления, доступ к которой не ограничен;

– обжаловать в установленном порядке акты и (или) действия (бездействие) государственных органов и органов местного самоуправления, их должностных лиц, нарушающие право на доступ к информации о деятельности государственных органов и органов местного самоуправления и установленный порядок его реализации;

– требовать в установленном законом порядке возмещения вреда, причиненного нарушением его права на доступ к информации о деятельности государственных органов и органов местного самоуправления» [48].

В заключение, необходимо рассмотреть судебную сферу реализации прав граждан на доступ к информации, а именно «комплекс мероприятий по

сбору и обработке, представлению информации, проводимых судами всех звеньев, а также властными органами, непосредственно взаимодействующими и осуществляющими организационное обеспечение деятельности судов» [68], именно так в своей работе «Правовая основа отношений, связанных с обеспечением доступа к информации о деятельности судов», А.В. Шемелин и Е. В. Егоров определили понятие «Обеспечение доступа к информации».

Основным правовым актом в данной области выступает Федеральный закон от 22.12.2008 N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [55]. Он раскрывает нам такие способы обеспечения доступа к информации как:

– присутствие граждан (физических лиц), в том числе представителей организаций (юридических лиц), общественных объединений, органов государственной власти и органов местного самоуправления, в открытом судебном заседании;

– обнародование (опубликование) информации о деятельности судов в средствах массовой информации;

– размещение информации о деятельности судов в сети «Интернет»;

– размещение информации о деятельности судов в занимаемых судами, Судебным департаментом, органами Судебного департамента, органами судейского сообщества помещениях;

– ознакомление пользователей информацией с информацией о деятельности судов, находящейся в архивных фондах;

– предоставление пользователям информацией по их запросу информации о деятельности судов;

– трансляция открытых судебных заседаний в сети "Интернет" в соответствии с настоящим Федеральным законом, другими федеральными законами.

Вместе с данным Федеральным законом действует «Концепция информационной политики судебной системы на 2020 - 2030 годы» [18], принятая в целях:

– гармонизация отношений судебной власти и общества;

– открытость и гласность судопроизводства;

– совершенствование способов доступа граждан, организаций, общественных объединений, органов государственной власти и органов местного самоуправления, представителей средств массовой информации к информации о деятельности судов;

– объективное освещение деятельности судов в средствах массовой информации;

– формирование благоприятного имиджа органов судебной власти;

– повышение уровня доверия к судебной системе.

В основу реализации данной концепции положено много задач способствующих реализации поставленных целей, но самой основной из них выступает «создание условий по обеспечению прав граждан на получение своевременной, объективной, полной и разносторонней информации о деятельности судебной системы». Это подтверждает, что государство уделяет особое внимание реализации прав граждан, установленных ст.8 Федерального закона от 22.12.2008 N 262-ФЗ «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» [55], к которым относит право:

– получать достоверную информацию о деятельности судов;

– не обосновывать необходимость получения запрашиваемой информации о деятельности судов, доступ к которой не ограничен;

– обжаловать в установленном законом порядке действия (бездействие) должностных лиц, нарушающие право на доступ к информации о деятельности судов и установленный порядок его реализации;

– требовать в установленном законом порядке возмещения вреда, причиненного нарушением его права на доступ к информации о деятельности судов.

Следовательно, как сказано в работе Н.Н. Федосеева «Доступ общественности к информации о деятельности судов в российской федерации» [66], что «эффективная реализация ФЗ «Об обеспечении доступа к информации о деятельности судов в РФ» позволит не только решить проблемы доступа общественности к информации о деятельности судов, но и поднять уровень эффективности самой судебной власти, сделать процедуру принятия правоприменительных решений прозрачной для общества, а также повысить социальную ответственность судей и других должностных лиц».

Следовательно, если данные права граждан будут реализованы и защищены в нашем государстве в полном объеме, то повысится доверие к деятельности судов и государственному аппарату в целом, это сыграет немаловажную роль для антикоррупционной политики, открытости, гласности и прозрачности деятельности органов власти, что окажет положительное воздействие на работу всего государства, которое в итоге приобретет статус демократического информационного общества.

С учетом всего изложенного можно сделать вывод о том, что законодательство в области информационного обеспечения граждан, постоянно совершенствуется и расширяется. Нам удалось разобрать самые важные нормативно-правовые акты, предоставляющие информационные права гражданам, это позволяет сказать о том, что обширная правовая база в нашем государстве имеется. К уже рассмотренным нормативно-правовым актам можно отнести такие акты, как: Федеральный закон от 13.01.1995 № 7-ФЗ «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» [50], Федеральный закон от 17.07.1999 № 176-ФЗ «О почтовой связи» [51], Закон Российской Федерации от 27.12.1991 г. № 2124-1 «О средствах массовой

информации» [10], Федеральный закон Российской Федерации от 29.12.2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» [64], Федеральный закон Российской Федерации от 07.07.2003 г. № 126-ФЗ «О связи» [46] и еще много законов и подзаконных актов разработано в данной области, они являются общедоступной информацией и находятся в открытом доступе для быстрого и удобного ознакомления.

Конституционное закрепление прав граждан получение, владение и распространение информации, является наивысшей гарантией соблюдения прав и свобод гражданина. Оно действует наравне с остальными нормами конституции, что делает это право не абсолютным, об этом говорится в трудах Т. Я. Хабриевой и В. Е. Чиркина: «не существует абсолютных прав и свобод, все они могут быть ограничены» [67,с.133-134], но только в той части, в которой это необходимо для «защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства» [58].

По моему мнению, ограничения можно разделить на две большие группы:

– сведения, составляющие государственную тайну;

– сведения конфиденциального характера.

Первая группа сведений регулируется Законом РФ "О государственной тайне" от 21.07.1993 N 5485-1 [9],он включает в себя:

– сведения в военной области;

– сведения в области экономики, науки и техники;

– сведения в области внешней политики и экономики;

– сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты.

Данный закон содержит в себе не только перечень сведений по указанным направлениям, но и степени секретности, порядок засекречивания и рассекречивания таких сведений, их защиту, порядок допуска, финансирование и контроль данной области, но и многое другое.

Перечень сведений второй группы строго регламентирован Указом Президента РФ от 6 марта 1997 г. N 188 «Об утверждении перечня сведений конфиденциального характера» [37] и содержит в себе:

– Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

– Сведения, составляющие тайну следствия и судопроизводства, сведения о лицах, в отношении которых в соответствии с федеральными законами от 20 апреля 1995 г. N 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов» и от 20 августа 2004 г. N 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства», другими нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты, а также сведения о мерах государственной защиты указанных лиц, если законодательством Российской Федерации такие сведения не отнесены к сведениям, составляющим государственную тайну.

– Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна).

– Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна,

тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее).

– Сведения, связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (коммерческая тайна).

– Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

– Сведения, содержащиеся в личных делах осужденных, а также сведения о принудительном исполнении судебных актов, актов других органов и должностных лиц, кроме сведений, которые являются общедоступными в соответствии с Федеральным законом от 2 октября 2007г. N 229-ФЗ «Об исполнительном производстве».

Из этого следует, что помимо названых актов, правовую базу по ограничению доступа к информации, составляют:

– акты, связанные с коммерческой тайной, такие как Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне» и ст.12 Федерального закона от 28.11.2011 N 335-ФЗ «Об инвестиционном товариществе» [60];

– акты, содержащие персональные данные, а именно Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных», ст. 13 Закона РФ от 20.07.2012 N 125-ФЗ «О донорстве крови и ее компонентов» [53], ст.98 Федерального закона от 29.12.2012 N 273-ФЗ «Об образовании в Российской Федерации» [65];

– акты, содержащие врачебную тайну, ст. 13 Федерального закона от 21.11.2011 N 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [54], п.2 ст.15 «Семейного кодекса Российской Федерации» от 29.12.1995 N 223-ФЗ [32], ст. 9 Закона РФ от 02.07.1992 N 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании» [8].

– акты, содержащие: налоговую, адвокатскую, нотариальную, аудиторскую тайны, а также страхования, исповеди, совещания судей, связи,

следствия и многие другие, получившие закрепление в нормативно-правовых актах Российской Федерации.

Таким образом, для охраны прав, свобод и законных интересов других лиц законодателем вводятся меры, направленные на установление границ реализации информационных прав и свобод, в том числе посредством введения порядка ограничения доступа к информации определенной специфики.

1.5 Ответственность в информационной сфере

Государство, наделило нас широким перечнем прав в области информации, закрепив их в Конституции РФ и иных нормативно-правовых актах, но как известно, любое право, предоставленное государством становится его обязанностью, по обеспечению и защите данных прав, иначе законодательные нормы были бы не эффективны.

Так и появился институт юридической ответственности. Что бы определить понятие «юридической ответственности», мне пришлось обратиться к трудам ученых из разных отраслей права, так С.Н. Братусь полагал, что юридическая ответственность – ничто иное как «исполнение обязанности посредством государственного принуждения, например уплата суммы долга заемщиком на основе решения суда» [3, с. 85, 94]. Н.В. Витрук утверждает, что «юридическая ответственность как мера государственного принуждения осуществляется на основе и в рамках закона, то есть она является правовой формой государственного принуждения» [4, с. 432]. Довольно интересная точка зрения И. Л. Бачило, которая утверждает что, юридическая ответственность - это «применение компетентным государственным органом санкции правоохранительной нормы и наступление отрицательных последствий в рамках закона для правонарушителя в виде установленных вида и меры наказания, соразмерных

нанесенному ущербу (вреду)» [12, с. 373–374], но самым подходящим к тематике работы, оказалось определение юридической ответственности за нарушение информационного законодательства М.А. Федотова, который сформулировал его как «предусмотренные законодательством меры дисциплинарной, административной, гражданско-правовой, уголовной и информационной ответственности за нарушение законодательства об информации» [13, с. 471]. Однако, несмотря на то, что ученые так и не пришли к единому мнению, я полагаю, что юридическую ответственность в информационной сфере необходимо рассматривать в рамках ст. 17 Федерального закона «Об информации, информатизации и защите информации» [58], основанного на Конституции РФ, которая придает праву на информацию особую важность. В нем сказано «Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации». Стоить заметить, что представленная статья является бланкетной нормой права.

Таким образом, нам нужно проанализировать нормы законодательства по отраслям права, представленным в данном определении.

К дисциплинарной ответственности привлекаются лица, совершившие информационное правонарушение, то есть виновное, противоправное деяние совершенное работником в сфере информации, неисполнение или ненадлежащее исполнение субъектом данных правоотношений возложенных на него трудовых обязанностей.

Дисциплинарная ответственность предусмотрена ст. 192 «Трудового кодекса Российской Федерации» от 30.12.2001 N 197-Ф [34], работодатель имеет право применить такие дисциплинарные взыскания как: замечание, выговор или увольнение.

В пример можно привести п. «в» ст. 81 согласно которой, работодатель может уволить работника по собственной инициативе за «разглашения

охраняемой законом тайны (государственной, коммерческой, служебной и иной), ставшей известной работнику в связи с исполнением им трудовых обязанностей, в том числе разглашения персональных данных другого работника». Так же п. 10 ст. 81 «представления работником работодателю подложных документов при заключении трудового договора», другими словами это можно назвать данный факт как «дезинформация работодателя». Еще следует упомянуть ст.17 Федерального закона от 29.07.2004 N 98-ФЗ «О коммерческой тайне», которая подтверждает вышеуказанное мной, то есть «Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством Российской Федерации» [63].

Допускается применение дисциплинарных взысканий только прямо установленных в законе с учетом тяжести совершенного проступка и обстоятельств его совершения. Применяется не позднее месяца со дня обнаружения данного проступка, но не может быть применено: по общим правилам по истечению шести месяцем со дня совершения проступка; в ходе проверки финансово-хозяйственной деятельности или аудиторской проверки не позднее двух лет со дня его совершения; при нарушении законодательства о противодействии коррупции не позднее трех лет.

Снятие дисциплинарного взыскания происходит по истечению одного года, в случае отсутствия новых взысканий, а равно снятие взыскания возможно досрочно по инициативе работодателя, ходатайству работника или представительного органа работников.

Дисциплинарная ответственность за совершение госслужащим информационного правонарушения регулируется Федеральным законом от

27.07.2004 N 79-ФЗ «О государственной гражданской службе Российской Федерации» [57]. В нем содержится расширенный перечень дисциплинарных взысканий. К ним относят: замечание, выговор, предупреждение о неполном должностном соответствии и увольнение по основаниям ст.37. В частности это касается п. «в» ч.3 ст.37 «разглашения сведений, составляющих государственную и иную охраняемую федеральным законом тайну, и служебной информации, ставших известными гражданскому служащему в связи с исполнением им должностных обязанностей».

Возможно применение только одного дисциплинарного взыскания после получения объяснений в письменной форме от гражданского служащего или составления акта об отказе от дачи таких объяснений. Далее, по решению представителя нанимателя или гражданского служащего проводится служебная проверка, в ходе которой устанавливается:

– факт совершения гражданским служащим дисциплинарного проступка;

– вина гражданского служащего;

– причины и условия, способствовавшие совершению гражданским служащим дисциплинарного проступка;

– характер и размер вреда, причиненного гражданским служащим в результате дисциплинарного проступка;

– обстоятельства, послужившие основанием для письменного заявления гражданского служащего о проведении служебной проверки.

Таким образом, в заключении по результатам проверки должны содержаться все факты и обстоятельства, установленные в ходе проверки и предложение о применение или неприменение дисциплинарного взыскания.

Сроки применения и снятия дисциплинарного взыскания, совпадают с теми, которые установлены Трудовым кодексом РФ. Обжаловать дисциплинарное взыскание, возможно по письменному заявлению

гражданского служащего в комиссию государственного органа по служебным спорам или в суд.

Перейдем к рассмотрению гражданско-правовой ответственности, которую можно определить как, комплекс мер имущественного характера, с помощью которых производится признание или восстановление нарушенных, информационных прав субъекта. Конечно же, отправной точкой к ответственности, является совершение гражданско-правового информационного правонарушения, П.У. Кузнецов предлагает рассматривать данные правонарушения как «посягающее на нематериальные блага информационной природы общественно вредное, противоправное, виновное деяние деликтоспособного лица» [19, с. 287- 289].

В работе «Правовая природа информации как нематериального блага», Т.М. Бикташев, на анализе законодательства и трудах ученых, доказал, что информации относится к числу нематериальных благ, «которая может иметь материальное отображение, но не отождествляться с физическими объектами, служащими ее носителями» [1]. Из этого следует что, объектом гражданских правоотношений может быть любая информация способная удовлетворить потребности субъектов данных отношений.

Выделяют такие виды ответственности за совершенные правонарушения как:

– договорная;

– внедоговорная.

Договорная ответственность возникает в случае нарушения или ненадлежащего исполнения условий договора, в котором содержатся санкции, прямо не предусмотренные нормами действующего законодательства, так как законодатель разрешает вносить в договор любые условия, не противоречащие нормам права. В пример можно привести ст.783.1 Гражданского кодекса РФ, в которой говорится что, договором об оказании услуг по предоставлению информации «может быть предусмотрена

обязанность одной из сторон или обеих сторон не совершать в течение определенного периода действий, в результате которых информация может быть раскрыта третьим лицам» [6]. Также в доказательство вышесказанного можно привести ст. 495 ГК РФ, в которой продавца обязывают сообщать достоверную и необходимую информацию о товаре; ст.726 ГК РФ согласно которой, вместе с результатами работы подрядчик обязан передавать заказчику информацию касающиеся эксплуатации предмета договора; ст.727 говорит о том, что получая информацию о новых решениях или технических заданиях, в том числе не защищенную законом информацию, сторона ее получившая не имеет право на ее распространения без согласия другой стороны. Немаловажным является то, что охраняются сведения составляющие: ст. 857 ГК РФ, банковскую тайну; ст.1465 сведения, имеющие потенциальную коммерческую ценность; ст. 946 тайну страхования и многое другое.

Внедоговорную ответственность можно расценивать как, причинение вреда личности субъекта правоотношений или его имуществу, несвязанного с исполнением договорных обязательств. По аналогии с договорным видом ответственности, приведу несколько примеров. Ст. 1095 ГК РФ говорит нам, что вред, причинённый вследствие недостоверной или недостаточной информации о товаре, подлежит возмещению продавцом или изготовителем товара, лицом, выполнившим работу или оказавшим услугу, независимо от их вины и от того, состоял потерпевший с ними в договорных отношениях или нет; ст.1100 ГК РФ предоставляет возможность получения компенсации морального вреда за вред причинённый распространением сведений, порочащих честь, достоинство и деловую репутацию; ст.1253.1 говорит о том, что информационный посредник несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, за исключение случаев установленных данной статьей, а именно:

– он не является инициатором этой передачи и не определяет получателя указанного материала;

– он не изменяет указанный материал при оказании услуг связи, за исключением изменений, осуществляемых для обеспечения технологического процесса передачи материала;

– он не знал и не должен был знать о том, что использование соответствующих результатов интеллектуальной деятельности или средства индивидуализации лицом, инициировавшим передачу материала, содержащего соответствующие результат интеллектуальной деятельности или средство индивидуализации, является неправомерным.

Таким образом, гражданско-правовая ответственность имеет имущественный характер императивных мер воздействия на правонарушителя и для ее наступления необходимо установить:

– противоправность поведения;

– наличие у потерпевшего убытков или вреда, в том числе касающихся его чести, достоинства и деловой репутации;

– наличие причинно-следственной связи между действиями нарушителя и последствиями для потерпевшего;

– вину правонарушителя.

Далее перейдем к рассмотрению административной ответственности в информационной сфере, которую можно понимать как, защитную меру государства от правонарушений в области информации, наступающей при нарушении законодательства об административных правонарушениях, нормы которого призваны защищать права и законные интересы личности, общества и государства. Основным и в тоже время самым динамично развивающимся нормативно-правовым актом в данной области выступает «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ [14]. Он определяет административное правонарушение как «противоправное, виновное действие (бездействие) физического или

юридического лица за которое административным законодательством предусмотрена ответственность». Так под влиянием развития информационных технологий, органам законодательной власти постоянно приходится следовать тенденциям развития в данной области и с минимальными затратами времени, в целях сокращения возможного ущерба от появляющихся опасностей и угроз, способных нанести вред личности, обществу и государству. Средствами такого следования тенденциям можно назвать: систематизацию, совершенствование, отмену и принятие новых норм административной ответственности в информационной области. С учетом вышесказанного, на данный момент «Кодексом об административных правонарушениях» выделена Гл.13 «административные правонарушения в области связи и информации» состоящая из 46 статей, содержит в себе такие составы как: использование средств связи или несертифицированных средств кодирования (шифрования), не прошедших процедуру подтверждения их соответствия установленным требованиям; нарушение законодательства Российской Федерации в области персональных данных; распространение информации о свободных рабочих местах или вакантных должностях, содержащей ограничения дискриминационного характера; нарушение правил защиты информации; разглашение информации с ограниченным доступом; злоупотребление свободой массовой информации; нарушение правил распространения обязательных сообщений; нарушение требований законодательства о хранении документов и информации, содержащейся в информационных системах; распространение владельцем аудиовизуального сервиса незарегистрированных средств массовой информации, а также остальные не менее важные составы административных правонарушений, связанные с различными сферами жизни общества, можно найти в данной главе. Административная ответственность за нарушение в информационной сфере не ограничивается нормами гл.13, ее можно встретить во многих статьях КоАП РФ, так например: ст. 6.13 пропаганда наркотических средств,

психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, новых потенциально опасных психоактивных веществ; ст. 5.61 Оскорбление, в том числе в публично демонстрирующийся произведениях, средствах массовой информации или информационно-телекоммуникационных сетях, включая сеть «Интернет»; ст. 5.1 нарушение права гражданина на ознакомление со списком избирателей, участников референдума; ст. 5.13 непредоставление возможности обнародовать опровержение или иное разъяснение в защиту чести, достоинства или деловой репутации. Не смотря на то, что административная ответственность за нарушения в области информации и так весьма широкая, нужно выделить еще одну ее особенность, она заключается в том, что использование информационно-телекоммуникационных сетей, при совершении правонарушения, может стать квалифицирующим признаком, что приведет к назначению более строгого наказания. Примером может послужить ч. 2 ст. 6.21 согласно которой «Пропаганда нетрадиционных сексуальных отношений среди несовершеннолетних, выразившаяся в распространении информации, направленной на формирование у несовершеннолетних нетрадиционных сексуальных установок совершенные с применением средств массовой информации и (или) информационно-телекоммуникационных сетей», предусматривает административный штраф, многократно превышающий сумму штрафа за неквалифицированный состав правонарушения.

Таким образом, проанализировав Административное законодательство, можно прийти к выводу, о том, что информация имеет многогранный характер и затрагивает все особо важные сферы общества.

Виды наказаний, предусмотренные по данным статьям, в большинстве случаев представляют собой такие санкции как: предупреждение,

административный штраф, конфискация орудия совершения или предмета административного правонарушения. Наиболее распространённым видом административного наказания выступает штраф, который регламентирован конкретной нормой и имеет градацию в зависимости от субъекта совершившего правонарушение. В качестве примера, приведу ст. 13.12 КоАП РФ, которая в качестве наказания за нарушение правил защиты информации, а именно за нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации, влечет наложение административного штрафа на: «граждан в размере от одной тысячи до одной тысячи пятисот рублей; на должностных лиц - от одной тысячи пятисот до двух тысяч пятисот рублей; на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей» [14].

Дела об административных правонарушениях в области связи и информации рассматривают: судьи; органы внутренних дел; органы, осуществляющие государственный надзор за связью и информатизацией; органы, осуществляющие контроль за обеспечением защиты государственной тайны; органы, осуществляю осуществляющие государственный контроль в области обращения и защиты информации; органы государственного статистического учета.

Особое внимание следует уделить тому, что включение юридических лиц в субъекты административной ответственности, тяжесть последствий и степень общественной опасности совершаемых правонарушений, возможность привлечения к ответственности во внесудебном порядке и отсутствие судимости, являются важными критериями разграничения административной ответственности от уголовной.

Что касается уголовной ответственности, она наступает за совершение преступления, то есть виновно совершенного общественно опасного деяния запрещенного уголовным кодексом, под угрозой наказания. Для привлечения к уголовной ответственности за преступление в

информационной сфере, необходимо определить: является ли лицо совершившее преступление, субъектом данных правоотношений, то есть «вменяемым физическим лицом, достигшим возраста уголовной ответственности»; наличие его вины, то есть субъективную сторону состава преступления; относятся ли общественные отношения в информационной сфере которым причинён вред, к тем, что охраняются уголовным законодательством, то есть объектом преступления; также нужно выявить, есть ли в противоправность в действиях лица совершившего тот или иной поступок, что представляет собой объективную сторону преступления.

Таким образом, нам удалось выявить такие обязательные элементы состава преступления, как:

– субъект;
– объект;
– субъективная сторона;
– объективная сторона.

При совершении деяния, совокупность данных элементов будет служить основанием для привлечения к уголовной ответственности. Следовательно, отсутствие хотя бы одного элемента, приводит к невозможности привлечения к уголовной ответственности.

Информационные преступления по своей природе являются высокотехнологичными, требующими наличия у преступника определенных знаний и опыта, специального оборудования и (или) компьютерных программ. В этом случае спецификой таких преступлений выступает, то, что они могут быть совершены только с помощью информационных технологий или информационно-телекоммуникационных сетей. В то же время, субъект противоправного деяния никогда лично не встречается с лицом, которому он причиняет ущерб.

Необходимо выделить то, что одновременно с развитием информационных технологий растет и преступность, так как, следуя за

техническим прогрессом способы совершения преступлений, постоянно усовершенствуются и обновляются. Это приводит к необходимости своевременного улучшения законодательной базы, в целях защиты абсолютно всех сфер общественной жизни. Таким образом, уголовная ответственность за преступления в информационной сфере, закреплена в разных главах и разделах уголовного кодекса РФ.

Например, законодатель выделил «Преступления в сфере компьютерной информации» [35] в Гл. 28 УК РФ, в которой закрепил:

– Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации;

– Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

– Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб;

– Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

Данной главой не ограничивается охрана информационной сферы, ведь в качестве непосредственного объекта преступления за преступления против чести и достоинства личности и нарушающие права и свободы человека и гражданина, установленного порядка управления и безопасности государства, нормы УК РФ включают в себя:

– в качестве квалифицирующего признака, при доведении лица до самоубийства или до покушения на самоубийство путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего, п. «д» ст.110 УК РФ устанавливает совершение деяния «в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»);

– п.2 ст. 128.1 УК РФ Клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации либо совершенная публично с использованием информационно-телекоммуникационных сетей, включая сеть «Интернет», либо в отношении нескольких лиц, в том числе индивидуально не определенных;

– преступления против конституционных прав и свобод человека и гражданина представленные гл.19 УК РФ, также содержат ряд статей: 137 УК РФ «нарушение неприкосновенности частной жизни», ст. 138 УК РФ «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», ст. 140 УК РФ «Отказ в предоставлении гражданину информации» и другие;

– в Гл. 20 преступления против семьи и несовершеннолетних, можно найти такие составы как: п. «в» ч.2 ст. 151.2 УК РФ «Вовлечение несовершеннолетнего в совершение действий, представляющих опасность для жизни несовершеннолетнего», ст.155 УК РФ «Разглашение тайны усыновления (удочерения)»;

– ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа», ст. 159.6. «Мошенничество в сфере компьютерной информации», ст. 163 «Вымогательство», ст. 170 «Регистрация незаконных сделок с недвижимым имуществом» и многие другие статьи содержат в себе уголовную ответственность за информационные преступления в сфере экономической деятельности;

– и иные статьи УК РФ.

К мерам уголовной ответственности за совершение преступлений в области информации, можно отнести: штраф, обязательные работы, исправительные работы, арест, лишение свободы и иные виды наказаний, предусмотренные ст. 44 УК РФ.

Представленные мною статьи Уголовного кодекса РФ, доказывают, что под охрану поставлены общественные отношения из разных областей жизни общества и государства, там самым они приобретают особую важность в обеспечении законности и правопорядка в информационной сфере.

Подводя итоги необходимо сказать, что информационная составляющая присутствует во всех проанализированных отраслях права, это в очередной раз подтверждает то, что информационные права граждан, предоставленные Конституцией РФ, охраняются нормами национального права в режиме реального времени. Кроме того, отечественному законодателю, необходимо находиться в постоянной динамике в сфере информационных правонарушений, как в России, так и за рубежом, в целях своевременного реагирования на возможные угрозы.

Глава 2 Информационная безопасность в сети «Интернет»

2.1 Обеспечение информационной безопасности в сети «Интернет»

В настоящее время сложно представить информационное общество без использования телекоммуникационных сетей, глобальных компьютерных сетей и сетей связи - радио, телевидения, фиксированных и мобильных телефонных сетей, Интернет. Так как активная разработка и внедрение во все сферы жизнедеятельности информационных технологий и средств, является характерной чертой информатизации.

По статистике на январь 2021 года, население нашей страны составляет 145,9 миллиона человек, на начало 2021 года из их числа насчитывается 124 миллиона пользователей интернета. Всемирная информационная сеть развивается большими темпами, количество участников постоянно растет. Это связанно с тем, что «Интернет» содержит в себе огромное количество социальных взаимосвязей. В виртуальном пространстве собраны все необходимые ресурсы для того, что бы облегчить жизнь любого человека. Пользователь «Интернета» может: взаимодействовать с органами государственной власти, знакомится с результатами их деятельности, и получать разъяснения на интересующие вопросы; учиться; работать; посещать развлекательные порталы; управлять своими финансами; налаживать социальные взаимосвязи; быстро и легко получать необходимую информацию и многое другое.

Безусловно, такими способами человек привык решать все свои проблемы с минимальными затратами усилий и времени. Несмотря на свою общедоступность и позитивные аспекты, которые предоставляет нам «Интернет», он может быть использован для нанесения вреда пользователю и его близким, так и имуществу. Именно поэтому к сетям предъявляются не только требований по обеспечению надёжности передачи данных,

стабильности работы, качества и масштабов охвата, но и информационной безопасности.

Таким образом, информационная безопасность в сети интернет, ничто иное как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [36].

Другими словами, информационная безопасность – это состояние защищенности информационной среды, защита конфиденциальности, доступности и целостности информации.

Три составляющие данного понятия, можно определить как:

– конфиденциальность, то есть обязательное требование не передавать такую информацию третьим лицам, без согласия ее обладателя;

– доступность, рассматривают как возможность получения информации и ее использование, обладателем;

– целостность, как неизменность информации в процессе ее передачи или хранения.

Необходимость информационной безопасности в сети «Интернет» обусловлена появлением и значительным ростом различных видов мошенников, вирусов, разнообразных «групп смерти», воздействующих на психическое состояние человека и иных угроз и опасностей, которые могут причинить ущерб жизненно-важным потребностям личности, общества и государства.

Основными целями несанкционированного доступа являются: повреждение, изменение или уничтожение сведений; кража персональных данных или иной конфиденциальной информации, в том числе сведений составляющих государственную, военную, коммерческую, врачебную,

банковскую и иных видов тайн; кража денежных средств со счетов, электронных кошельков и банковских карт; фишинг, то есть кража идентификационных данных пользователя и многое другое.

Исходя из вышесказанного, нужно понимать, что размещая какую либо информацию в «Интернете», она становится доступной для большого круга лиц, что может привести к неблагоприятным последствиям, даже в том случае если она размещена на закрытых разделах сайта.

Именно поэтому, порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет», утвержден Указом Президента РФ от 22 мая 2015 г. N 260 «О некоторых вопросах информационной безопасности Российской Федерации» [42]. Согласно которому, подключение информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет», осуществляется по каналам передачи данных, защищенным с использованием шифровальных (криптографических) средств, а их защита обеспечивается в соответствии с законодательством Российской Федерации.

Таким образом, подключение государственных и находящихся в ведении государственных органов информационных систем и информационно-телекоммуникационных сетей, к сети «Интернет» через российский сегмент осуществляется:

– по защищенным каналам, создание, содержание и развитие которых обеспечивается ФСО России и государственными органами за счет и в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете этим органам;

– за счет и в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете ФСО России.

Помимо этого, в целях обеспечения информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей, позволяющих осуществлять передачу информации через государственную границу Российской Федерации, в том числе при использовании международной компьютерной сети «Интернет», Указ Президента РФ от 17 марта 2008 г. N 351 [40], устанавливает, что:

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

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

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

Ученые в своих трудах выделяют такие средства защиты информации как: технические, организационные и правовые.

К техническим относят:

– антивирусные программы, обнаруживающие вредоносное программное обеспечение, шпионские программы, сайты на которых возможен несанкционированный доступ к конфиденциальной информации о пользователе;

– сети VPN обеспечивающие анонимность, оберегают от кражи личной информации, но нужно быть осторожнее, потому что, данные программы могут быть использованы правонарушителем и это осложнит поиск его местонахождения и идентификацию;

– системы аутентификации и шифрования;

– регламентирование доступа к информационным объектам, в этом случае у каждого пользователя имеется определенный набор прав, исходя из которых, они могут работать с информацией;

– применение DLP- и SIEM-систем. Это внутренняя защита от недобросовестных сотрудников. В первом случае программа не даёт копировать информацию на сторонние носители, например, флэшку; вторая отслеживает, запросы к базе данных и сообщает, если считает ситуацию подозрительной;

Это только основные технические средства, на самом деле их гораздо больше и они пополняются довольно часто, так же как и возникают новые угрозы.

К организационным мерам относят:

– инструктаж работников по поводу обращения с информацией;

– запрет на использование личного компьютера и информационных носителей;

– подписание документа о неразглашение информации, ставшей доступной сотруднику в ходе исполнения его обязанностей;

– создание идентифицированных аккаунтов и определенных уровней доступа к информации, это поможет узнать, с какого компьютера произошла утечка информации.

Правовые средства, действуют в целях предупреждения и сдерживания потенциальных правонарушителей, а также привлечения к юридической ответственности лиц нарушивших нормы информационного законодательства. Анализ нормативно–правовых актов показал, что в нашем государстве обширная законодательная база в данной области, нарушение норм которой, влечет за собой привлечение к уголовной, административной, гражданско-правовой или дисциплинарной ответственности.

Все это говорит о том, что информационной безопасности отводится особое внимание при работе в «Интернете». Но, не смотря на большое количество средств и методов, проблема обеспечения информационной безопасности в сети «Интернет» является актуальной и на сегодняшний день. Развитие информационных технологий побуждает к постоянному приложению совместных усилий по совершенствованию методов и средств, позволяющих достоверно оценивать угрозы безопасности информационной сферы. Решением данной проблемы должно заниматься не только государство, в лице его уполномоченных органов, но и каждый человек в частности. Поэтому при использовании глобальной сети необходимо быть внимательным и осторожным и не пренебрегать уже существующими средствами обеспечения информационной безопасности.

2.2 Блокировка информации в сети «Интернет»

Как было указанно ранее, п.4 ст.29 Конституции РФ закрепляет право граждан, на поиск, получение, передачу, производство и распространение информации любым законным способом. Хоть данное право и является неотъемлемым, всё же существует ряд ограничений, обоснованных

«необходимостью защиты основ конституционного строя, обеспечения безопасности государства и государственного суверенитета, охраны прав интеллектуальной собственности, защиты нравственности, жизни и здоровья населения, обеспечения права на неприкосновенность частной жизни, защиты конфиденциальной информации, в том числе персональных данных» [7]. Из этого следует что, блокирование информации должно быть обоснованно и осуществляться только на законодательном уровне с точным указанием критериев, которые свидетельствуют о том, что данный вид сведений отнесен к перечню запрещенной информации, с соблюдением «порядка установления правового режима и применения ограничительных мер, а также перечня субъектов государственного управления, уполномоченных на принятие решений в данной сфере» [2].

Согласно ст. 15.1 Федерального закона от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» [58]. В Российской Федерации действует автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено»

Создание, формирование и ведение реестра возложено на Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций, так как данная служба «осуществляет функции по контролю и надзору в сфере средств массовой информации, в том числе электронных, и массовых коммуникаций, информационных технологий и связи, функции по контролю и надзору за соответствием обработки персональных данных требованиям законодательства Российской Федерации в области персональных данных» [28], которая в свою очередь наделена правом, привлекать к формированию и ведению реестра – организацию, зарегистрированную на территории РФ.

Проанализировав нормы законодательства выявлено, что существуют разные критерии блокировки доступа к сайтам в сети «Интернет», их можно разделить по основаниям, перечень которых строго определен; по порядку применений решений о блокировке; по субъектам, уполномоченным выносить решения о блокировке; по сфере применения; по порядку ограничения и процессуальным срокам и срокам действия ограничений.

Основания внесения сведений в «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» четко регламентирован ч.5 ст. 15.1 Федеральным законом «Об информации, информационных технологиях и о защите информации» [58], туда входят:

– решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, таких как Роскомнадзор, МВД РФ, Роспотребнадзор, Росздравнадзор, ФНС, Росалкогольрегулирование, Росмолодежь, принятые в соответствии с их компетенцией в отношении распространяемых посредством сети «Интернет»:

– материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

– информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

– информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

– информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

– информации о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети «Интернет»;

– информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

– информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

– информации, содержащей предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, розничная торговля которыми ограничена или запрещена в соответствии с законодательством об обращении лекарственных средств, и (или) информации, содержащей предложение о розничной торговле лекарственными препаратами, в том числе дистанционным способом, лицами, не имеющими лицензии и разрешения на осуществление такой деятельности, если получение лицензии и разрешения предусмотрено законодательством об обращении лекарственных средств.

Категории вышеизложенной информации предполагают блокирование сведений в сети «Интернет», уполномоченными Правительством РФ органами исполнительной власти, во внесудебном порядке.

На сайте Роскомнадзора можно найти процедуру направления информации по вопросу ограничения доступа. В ней четко расписано, что в случае обнаружения материалов с признаками запрещенной информации, необходимо сформировать электронное Сообщение на сайте в разделе «прием сообщений», там нужно выбрать тип информации, добавить ссылку на данный «Интернет» ресурс, приложить скриншот экрана, определить вид информации, режим доступа к ней и предоставить запрашиваемую информацию о заявителе. В данном сообщении, нужно указывать именно конкретную страницу интернет-сайта, содержащую признаки наличия запрещенной информации, потому что, закон не может быть применим к поисковым сервисам, так как они не являются владельцами сайтов содержащих запрещенную информацию.

Таким образом, обязательный порядок блокировки информации осуществляется в определенной последовательности:

– подача правильно сформированного сообщения;

– принятие Роскомнадзором данного сообщения и направление его в уполномоченный орган ответственный за запрет информации данного типа;

– в суточный срок, а при необходимости проведения экспертизы в семидневный срок, уполномоченный орган должен принять решение о признании информации запрещенной или отказать в признании. По факту принятия решения, информация направляется в Роскомнадзор;

– при выявленном нарушении, в течение суток, Роскомнадзор вносит данные реестр и уведомляет об этом владельца «Интернет» ресурса и оператора хостинга;

– по истечении суток с момента направления уведомления, сотрудник Роскомнадзора проверяет, приняты ли меры для удаления запрещенной информации с сайта. Если меры приняты и информация больше недоступна то, Роскомнадзор убирает веб-страницу из реестра, если

требование проигнорировано, информация об этом передается оператору связи, который обязан в течение суток ограничить доступ к сайту.

В то время как, судебный порядок предусматривает ограничение доступа к сайтам в сети «Интернет» за информацию порочащую честь, достоинство или деловую репутацию гражданина или юридического лица, на основании постановления судебного пристава-исполнителя или вступившего в законную силу решения суда о признании информации, содержащейся «Интернете», запрещенной к распространению на территории Российской Федерации. Таким образом, на основании административного искового заявления, поданного прокуратурой или физическими лицами. По итогам судебного заседания и получения положительного судебного решения, заявители направляют его в Роскомнадзор, который вносит запись в реестр, уведомляет владельца, а затем блокирует «Интернет» ресурс, в случае неисполнения требований по удалению запрещенной информации.

По итогам изучения судебной практики выявлено, что в Центральном районном суде г. Тольятти и Автозаводском районном суде г. Тольятти, по заявлению Прокурора о признании информации, содержащейся в информационно-коммуникационной сети «Интернет», запрещенной к распространению на территории РФ, принимается много удовлетворительных решений, с последующим занесение информации в реестр. Можно сделать вывод, что прокуратура, которая не относится к числу органов ответственных за блокировку сайтов, играет немаловажную роль, проводя мониторинг для выявления ресурсов содержащих или распространяющих запрещенную информацию и подавая иски в суд, в целях защиты прав неопределенного круга лиц.

Помимо этого, в ст.15.1 -15.9 Федерального закона «Об информации, информационных технологиях и о защите информации» регламентирован порядок ограничения доступа разного рода информации. Например, ограничение доступа к информации, распространяемой с нарушением

авторских и (или) смежных прав, осуществляется таким образом: Правообладатель в случае обнаружения в сети «Интернет», объектов авторских и (или) смежных прав которые распространяются без его разрешения, обращается в Роскомнадзор с заявлением о принятии мер по ограничению доступа к информационным ресурсам, на основании вступившего в силу судебного акта. Далее в течение трех рабочих дней Роскомнадзор определяет провайдера хостинга и направляет уведомление на русском и английском языках о нарушении исключительных прав, указав наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», с требованием принять меры по ограничению доступа к такой информации. Фиксируется дату и время направления такого уведомления. Потом, в течение одного рабочего для после получения уведомления провайдер хостинга информирует об этом владельца информационного ресурса, которому дается еще один рабочий день на удаление незаконно размещенной информации или принятия мер по ограничению доступа к ней. В случае отказа или бездействия провайдер в течение трех рабочих дней самостоятельно ограничивает доступ к такому информационному ресурсу. Если никто из вышеуказанных лиц, не ограничивает доступ к информации, то в течение трех суток, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа.

В качестве второго примера можно привести «Порядок ограничения доступа к информации, распространяемой с нарушением закона», к такой относят информацию содержащую «призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых мероприятиях, проводимых с нарушением установленного порядка, недостоверную общественно значимую информацию, распространяемую под

видом достоверных сообщений, которая создает угрозу причинения вреда жизни и здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и общественной безопасности, либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, информационных материалов иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28 декабря 2012 года N 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации», сведений, позволяющих получить доступ к указанным информации или материалам» [58]. Так, при поступлении уведомлений в отношении недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений от органов государственной власти или граждан в Роскомнадзор, в случае если информация размещена на информационном ресурсе, зарегистрированном в соответствии с Законом Российской Федерации от 27 декабря 1991 года N 2124-1 «О средствах массовой информации» [10] в качестве сетевого издания, незамедлительно уведомляет редакцию сетевого издания о необходимости удаления указанной информации. Если информация не удалена, она направляется операторам связи, которые незамедлительно должны ограничить доступ к сетевому изданию, за исключением случая, если «доступ к такой информации в сети связи оператора связи ограничивается с помощью технических средств противодействия угрозам в порядке централизованного управления сетью связи общего пользования» [46]. При обращениях, не относящихся к деятельности сетевых изданий, Роскомнадзор по системе взаимодействия направляет операторам требование об ограничении доступа, определяет лицо

обеспечивающее размещение информационного ресурса и направляет уведомление о нарушении порядка распространения информации с требованием принять меры по удалению такой информации. Фиксируется дата и время уведомления. После его получения, оператор связи обязан незамедлительно ограничить доступ к информационному ресурсу и уведомить владельца данного ресурса о незамедлительном удалении данной информации. В течение суток информация должна быть удалена, если владелец бездействует или отказывает в требовании, то по истечению суток провайдер хостинга ограничивает доступ к соответствующему информационному ресурсу.

Следовательно, любое ограничение доступа должно быть регламентировано в законе, преследовать одну из конституционно значимых целей, осуществляться только уполномоченным органом и произведено в определенном порядке.

Безусловно, ограничение доступа к информации определенного характера благоприятно влияет на поддержание правопорядка в обществе. Ярким примером распространения недостоверной информации, послужила ситуация сложившиеся в связи с распространением COVID-19 и вакцинацией от данного вируса, в сеть «Интернет», начала поступать неподтвержденная информация, которая создала волнения в обществе, но по требованию Генеральной прокуратуры были заблокированы около тысячи сайтов с ложными сведениями, что благоприятно повлияло отношение общественности к данному вопросу.

Тем не менее, проблематика состоит в том, что в открытом доступе существует много способов обхода блокировки сайтов, создаются копии заблокированных сайтов и информация, в том числе недостоверная, распространяется с огромной скоростью, потому что, находится в открытом доступе и направленна на потребление большого количества людей, она

скачивается, пересылается и копируется на разные информационные ресурсы, что существенно осложняет работу Роскомнадзора.

2.3 Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы

Для решения задач по прогнозированию ситуации в области обеспечения информационной безопасности, осуществлению контроля степени защищенности, установлению причин компьютерных инцидентов и обеспечению взаимодействия субъектов осуществляющих лицензируемую деятельность в области защиты информации был издан Указ Президента РФ от 15 января 2013 г. N 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [39]. Далее, 12.12.2014 года, Президентом РФ была утверждена «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (далее по тексту – ГосСОПКА) [5], в которой определяется назначение, функции и принципы создания данной системы. Таким образом, ГосСОПКА создана для обеспечения защищённости информационных ресурсов Российской Федерации от компьютерных атак и штатного функционирования данных ресурсов в условиях возникновения компьютерных инцидентов, вызванных компьютерными атаками. С ее помощью реализуются такие функции как:

– выявление признаков компьютерных атак, их источников, способов и средств осуществления, а равно разработка методов их предупреждения и при необходимости ликвидации последствий;

– формирование и постоянное пополнение информации о состоянии информационных ресурсов;

– прогнозирование ситуации в области обеспечения информационной безопасности;

– осуществление взаимодействия со всем заинтересованным организациями в области обнаружения сетевых атак и их источников, включая обмен опытом, для выявления и устранения уязвимостей;

– сбор и анализ информации о компьютерных атаках;

– мониторинг степени защищенности информационных систем и телекоммуникационных сетей.

Мною названы только основные функции данной системы, полный перечень составляет около двенадцати позиций закрепленных в Концепции ГосСОПКА Российской Федерации.

К субъектам Системы можно отнести Федеральную службу безопасности, владельцев информационных ресурсов, Национальный координационный центр, операторов связи и иные организации, осуществляющие лицензионную деятельность в области защиты информации.

Основной организационно - технической составляющей являются центры обнаружения, предупреждения и ликвидации последствий. Которые подразделяются на главный центр Системы, региональные и территориальные центры, центры органов государственной власти и органы власти субъектов РФ, их называют ведомственными центрами, также выделяют ещё корпоративные центры.

Главный, региональные и территориальные центры создаются федеральными органами исполнительной власти, организовывают и проводят мероприятия по оценке степени защищенности информационной инфраструктуры РФ от компьютерных атак.

Корпоративные центры создаются государственными корпорациями, операторами связи, а также организациями, осуществляющими лицензионную деятельность в области защиты информации. Функционирование такого центра осуществляется организацией создавшей его.

Так выстраивается иерархическая система, где на нижнем уровне находятся компании, ведомства, корпорации и организации, которые силами собственной службы безопасности выявляют любые инциденты или подозрительную активность и направляют об этом отчет в региональные или территориальные центры субъекта РФ, оттуда информация направляется в главный центр ГосСОПКА, в котором и аккумулируется вся информация о компьютерных атаках и инцидентах.

Подключение любого центра к ГосСОПКА осуществляется на основании соглашения государственного органа, корпорации или организации с Федеральной службой безопасности.

В Федеральном законе от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [56]. Говорится, что «Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты». В ст.2 вышеуказанного федерального закона раскрыты понятия компьютерной атаки и компьютерного инцидента.

Компьютерную атаку необходимо понимать как «целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях

нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации». В то время как, компьютерный инцидент не что иное, как «факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки» [56].

Принятый Указ Президента РФ от 22 декабря 2017 г. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [43], наделил Федеральную службу безопасности Российской Федерации функциями в данной области. ФСБ выполняет функции по обеспечению и контролю Системы, формированию и реализации научно-технической политики и разрабатывает методические рекомендации по обнаружению, предупреждению и ликвидации компьютерных атак и инцидентов.

В свою очередь, ФСБ России создан Национальный координационный центр по компьютерным инцидентам, который является составной частью сил, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. Помимо НКЦКИ к силам относятся подразделения и должностные лица ФСБ и субъекты критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты уполномоченный осуществлять внутрироссийское и международное взаимодействие по вопросам реагирования на компьютерные инциденты, в которые вовлечены российские информационные ресурсы. Он выполняет функции связанные с:

– координацией мероприятий по реагированию на компьютерные инциденты;

– организацией и осуществлением обмена информации между субъектами;

– осуществлением методического обеспечения деятельности субъектов критической информационной инфраструктуры;

– участием в обнаружении, предупреждении и ликвидации последствий компьютерных атак; сбором, хранением и анализом информации о компьютерных инцидентах и компьютерных атаках;

– передачей информации в ГосСОПКА;

– и многое другое.

Помимо НКЦКИ к силам относятся подразделения и должностные лица ФСБ и субъекты критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

В качестве средств предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, можно назвать технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов), а также криптографические средства защиты.

Таким образом, при таких событиях как:

– заражение вредоносным программным обеспечением;

– распространение вредоносного программного обеспечения;

– нарушение или замедление работы контролируемого информационного ресурса;

– несанкционированный доступ в систему;

– попытки несанкционированного доступа в систему или к информации;

– сбор сведений с использованием информационно-коммуникационных технологий;

– нарушение безопасности информации;

– распространение информации с неприемлемым содержимым;

– наличие уязвимости или недостатка в контролируемом ГосСОПКА субъекте.

В срочном порядке должно быть инициировано взаимодействие с Национальным координационным центром по компьютерным инцидентам, для получения рекомендаций по реагированию.

Ознакомившись с результатами работы НКЦКИ за апрель 2021 года, можно сделать вывод, что за месяц работы, пресекается деятельность тысяч вредоносных ресурсов и принимается огромное количество мер для поддержания информационной безопасности.

Безусловно, создание данной системы благоприятно влияет на информационную безопасность, так как компьютерные атаки становятся все опаснее и сложнее, они могут провоцировать техногенные аварии, экологические катастрофы, военные конфликты, транспортные катастрофы и многое другое. Другими словами, может быть нанесен колоссальный ущерб личности, обществу и государству в целом. Из этого следует, что справится в одиночку с таким явлением практически невозможно, но используя все силы и средства Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, можно на основе собранной информации о контролируемом объекте повысить уровень безопасности и свести уязвимости, угрозы и недостатки к минимуму, а при необходимости, своевременно отреагировать на компьютерные атаки и предотвратить компьютерный инцидент.

Однако, несмотря на то, что вопросам обеспечения информационной безопасности объектов критической инфраструктуры в последнее время уделяют пристальное внимание, остается ряд пробелов в действующем законодательстве. Так, в Приказе ФСБ России от 24 июля 2018 года № 368 «Об утверждении Порядка обмена информацией» [31], отсутствует точная форма для предоставления информации, что приводит к предоставлению лишних сведений и возникновению сложностей при ее анализе и не определены сроки, в которые должен быть произведен обмен информацией о компьютерных инцидентах.

Кроме того, в Российской Федерации до сих пор не введена Административная ответственность, за нарушения требований к созданию систем безопасности, за несвоевременное предоставление или отказ от предоставления информации о компьютерных инцидентах, а также в случае нарушения порядка категорирования или обмена информацией о компьютерных атаках и инцидентах в области критической информационной инфраструктуры. Аналогично, отсутствует ответственность за нарушение Приказов ФСБ утверждающих требования к средствам ГосСОПКА, их условий установки и эксплуатации.

Однако если восполнить законодательные пробелы, собрать команду высококвалифицированных специалистов и наладить эффективное взаимодействие с НКЦКИ, своевременно реагировать на инциденты, проводить мероприятия для превентивной защиты, а также организовать оперативный обмен данными, то работа Системы будет налажена и существенно повысится устойчивость подконтрольных объектов перед компьютерными атаками, что приведет к повышению уровня информационной безопасности и стабильной работе объектов критической информационной инфраструктуры.

«Право граждан на информацию, как и право на доступ к государственной информации, законодательно определены в конституциях

многих стран и представляют собой основу демократического общества как гарант возможности эффективного взаимодействия граждан и государства» [25]. Доступ к информации - это гарантированное законом беспрепятственное предоставление гражданину необходимой общественно-значимой информации. Так, «к началу XXI века во всем мире стали стремительно распространяться идеи транспарентности и открытости. Эти процессы привели к тому, что в настоящее время имеет место глобальная тенденция популяризации доступа к информации» [25].

В качестве первого примера будет представлен анализ законодательных актов и конституционных положений Канады.

В Канаде право на доступ к информации не закреплено на конституционном уровне, Важной особенностью правовой системы Канады является отсутствие единого основного закона страны. Конституцией в настоящее время являются «Конституционный акт» вступивший в силу 17 апреля 1982г. [30], первую часть которого составляет «Хартия прав и свобод», гарантирующая «свобода мысли, убеждений, мнения и выражения включая свободу печати и других средств коммуникации» [30]. В 2010 г. Верховный суд Канады постановил, что данная свобода выражения мнений, включает в себя право требовать предоставление доступа к правительственным документам для предметного обсуждения и дискуссий по вопросам, представляющим общественный интерес. Но все же, основным законодательным актом в данной сфере выступает «Закон о доступе к информации, принятый парламентом в 1982 г. и вступивший в силу 01.07.1983», в связи с актуальной для того времени тенденцией распространения идей о свободе информации и открытого правительства.

«Закон был принят в целях обеспечения права на доступ к информации, содержащейся в документах правительственных учреждений. В его основе лежат три принципа:

– правительственная информация должна быть доступна для общественности;

– необходимые исключения из права на доступ должны быть ограничены и точно определены;

– решения о раскрытии правительственной информации должны приниматься автономно и проходить независимую экспертизу» [23].

Правом на доступ обладает любой гражданин либо лицо, обладающее статусом постоянного жителя Канады. В Законе четко регламентирован процесс направления запроса, его форма и также установлен тридцатидневный срок на получение ответа на запрос. Немаловажно то, что все запросы на получение информации обрабатываются единообразно и без учета личности заявителя, его должности или целей, для которых он обращается за информацией.

В 1983 г. было создано специализированное Управление Уполномоченного по вопросам информации для оказания помощи физическим лицам и организациям, которые считают, что правительственные учреждения нарушают их право на доступ к информации. Уполномоченный по вопросам информации, имеет право проходить в любое правительственное учреждение, изучать все документы и информацию, кроме защищенных грифом «тайны Кабинета» и давать рекомендации по предоставлению информации, либо отказе в предоставлении.

В обязанности данного Управления входит:

– проведение расследований по поступившим жалобам и принятие мер по разрешению споров;

– представление Уполномоченного в судебных делах;

– оказание правовой помощи в расследованиях;

– проведение консультаций по вопросам законодательства.

Таким образом, данный подход к предоставлению доступа к информации являлся многообещающим и «Канаду долгое время

воспринимали как возможного лидера в данной области, обладающего не только специализированным законодательством, подробно регламентирующим правила осуществления доступа и предоставления информации, но и необходимой институциональной основой» [25].

Правовое регулирование доступа к информации в Республике Беларусь закреплено в ст. 34 Конституции Республики Беларусь и осуществляется на основании общиной правовой базы, но ведущим актом, а данной области, выступает Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [11]. Он закрепляет в себе необходимые положения о «поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, а также пользовании информацией; создании и использовании информационных технологий, информационных систем и информационных сетей, формировании информационных ресурсов; организации и обеспечении защиты информации». Проанализировав данный законодательный акт, можно сделать выводы, что он хорошо детализирован, но его положения схожи с Федеральным законом Российской Федерации «Об информации, информационных технологиях и о защите информации» [58], и особой спецификой не наделены.

Изучив законодательные акты иностранных государств, можно сделать вывод, что в некоторых из них, таких как: Германии, Армении, Бразилия, Албания, США, Франция, Болгария, Южная Африка, Израиль, Чехия, Великобритания, право на доступ к информации выделено в качестве самостоятельного права, по аналогии с Россией. Также присутствует регламентация в качестве свободы выражения мнений в Финляндии, Новой Зеландии, Венгрии, Южной Корее. Каждый рассмотренный законодательный акт содержит четкую процедуру, форму, сроки и порядок обращения граждан для реализации права на доступ к информации. Также выявлено, что не одним государством данное право не признано абсолютным, ограничения в

целях защиты прав лиц, которым может быть причинен вред при реализации права на доступ к информации; безопасности государства, суверенитета и т.д.

Помимо этого в конституционных положениях закреплено не только право на доступ к информации, но и другие нормы, непосредственно связанные с правом человека на информацию, к ним можно отнести нормы, регулирующие свободу слова, обеспечение личной, семейной тайны, тайны телефонных, телеграфных и иных сообщений.

В статье Максимовой О.И., сказано, что «некоторые государства Перу, Ирландия и др. в конституционных положениях предусматривают возможность взимания платы за предоставление информации. Чрезвычайно высокая плата за предоставление ответа на запрос часто устанавливается специально для того, чтобы предотвратить наплыв запросов» [21]. Это выступает особенностью правового регулирования доступа к информации, но в тоже время, высокая плата может стать препятствием для социально незащищенных слоев общества, что явно дискриминирует их конституционные права.

Подводя итоги, необходимо обратить внимание на то, что тенденция по включению права на информацию в законодательство каждого государства развивается динамично, закрепление права на информацию в основополагающих международных документах, а также в Конституции, подчеркивает его огромное значение для демократизации и становления информационного общества. При том основное внимание следует уделить именно реализации данного права, обеспечение свободного доступа к информации, имеющей общественное значение, информационная открытость органов власти являются важнейшими условиями и критериями функционирования правового государства.

Заключение

Подведем итоги. В первой главе данного исследования были рассмотрены основные законодательные акты в области национальной безопасности, раскрыто понятие национальной безопасности, выделены ее основные объекты, национальные интересы в данной области и основные виды безопасности, а также представлена классификация угроз по различным основаниям. На основе нормативно-правовой базы, выявлено, что информационная безопасность представляет собой «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» [36] и является одним из важнейших направлений в обеспечении национальной безопасности. Рассмотрены Конституционные права граждан в информационной сфере, способы их реализации и правовые ограничения. Также проанализированы нормативно-правовые акты, устанавливающие дисциплинарную, административную, гражданско-правовую и уголовную ответственность в случае нарушения информационных прав.

Во второй главе, обоснована необходимость обеспечения информационной безопасности в сети «Интернет», описаны технические, организационные и правовые средства защиты информации, определён перечень информации распространение которой запрещено в Российской Федерации и основания внесения данных сведений в «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», а также порядок и процедура ограничения доступа к данному виду информации.

Помимо этого, были рассмотрены задачи, функции, средства, субъекты и организационно-техническая составляющая Государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы. В заключении данной главы представлен опыт иностранных государств по правовому регулированию в информационной сфере.

В результате проведенного исследования можно сделать выводы о том, информационная сфера затрагивает все сферы жизни общества, поэтому в Российской Федерации имеется обширная и динамично развивающаяся правовая база, регулирующая общественные отношения, возникающие в информационной области.

Но с появлением новых технологий, способов хранения, обработки и передачи информации, возникает все больше потенциальных уязвимостей, то есть одновременно с развитием информационных технологий растет количество правонарушений, так как, следуя за техническим прогрессом способы совершения правонарушений, постоянно усовершенствуются и обновляются.

На данный момент, в сети «Интернет» происходит значительный рост различных видов мошенников, вирусов, разнообразных «групп смерти», воздействующих на психическое состояние человека и иных угроз и опасностей, которые могут причинить ущерб жизненно-важным потребностям личности, общества и государства. В основном их целями является: повреждение, изменение или уничтожение сведений; кража персональных данных или иной конфиденциальной информации, в том числе сведений составляющих государственную, военную, коммерческую, врачебную, банковскую и иных видов тайн; кража денежных средств со счетов, электронных кошельков и банковских карт; кража идентификационных данных пользователя.

Государство борется с информационными правонарушениями различными способами, такими как: привлечение к юридической ответственности, блокировка запрещенной информации и созданием системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы.

Проблематика состоит в том, что в открытом доступе существует много способов обхода блокировки сайтов, создаются копии заблокированных сайтов и информация, в том числе недостоверная, распространяется с огромной скоростью, а привлечение к юридической ответственности осложняется тем, что в большинстве случаев информационные правонарушения являются высокотехнологичными, требующими наличия определенных знаний и опыта, специального оборудования и (или) компьютерных программ. В то же время, субъект противоправного деяния почти никогда лично не встречается с лицом, которому он причиняет ущерб и к тому же правонарушитель может находиться вне юрисдикции нашего государства.

Список используемой литературы и используемых источников

1. Бикташев Т.М. Правовая природа информации как нематериального блага [Электронный ресурс] / Т.М. Бикташев. – Режим доступа: URL: https://cyberleninka.ru/article/n/pravovaya-priroda-informatsii-kak-nematerialnogo-blaga/viewer (дата обращения: 10.01.2021)

2. Бородин К.В. Объекты и субъекты правового регулирования борьбы с распространением вредной информации в сети Интернет // Информационное право. 2016. № 2. С. 13–17.

3. Братусь, С. Н. Юридическая ответственность и законность / С. Н. Братусь. – М.,1978. – 208 с.

4. Витрук, Н. В. Общая теория юридической ответственности / Н. В. Витрук. – М., 2009. – 432 с.

5. «Выписка из Концепции государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» (утв. Президентом РФ 12.12.2014 № К 1274) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1162202293054267013 35959618&cacheid=2354A7A903C5F2B1D87B187106CBDCB1&mode=splus&base=LAW&n=181661&rnd=4889E3608FEC3B45F6F4CA33172F5CD1#v7z4dfs2lp (дата обращения: 13.03.2021)

6. «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996. № 14-ФЗ (ред. от 09.03.2021) // СЗ РФ. – 29.01.1996. –№ 5. ст. 410

7. Ельчанинова Н.Б. Проблемы совершенствования законодательства в сфере ограничения доступа к противоправной информации в сети интернет [Электронный ресурс] / Н.Б. Ельчанинова. - Режим доступа: URL: https://cyberleninka.ru/article/n/problemy-

sovershenstvovaniya-zakonodatelstva-v-sfere-ogranicheniya-dostupa-k-protivopravnoy-informatsii-v-seti-internet/viewer (дата обращения: 4.02.2021)

8. Закон РФ от 02.07.1992. № 3185-1 (ред. от 08.12.2020) «О психиатрической помощи и гарантиях прав граждан при ее оказании» // «Ведомости СНД и ВС РФ». – 20.08.1992. – № 33. ст. 1913.

9. Закон РФ от 21.07.1993. № 5485-1 (ред. от 09.03.2021) «О государственной тайне» // СЗ РФ. – 13.10.1997. –№ 41. стр. 8220-8235(2)

10. Закон РФ от 27.12.1991. № 2124-1 (ред. от 30.12.2020) «О средствах массовой информации» (с изм. и доп., вступ. в силу с 01.01.2021) // СЗ РФ. – № 32. 08.02.1992

11. Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» [Электронный ресурс] / Национальный правовой Интернет-портал Республики Беларусь. - Режим доступа: URL: https://pravo.by/document/?guid=3871&p0=h10800455 (дата обращения: 12.04.2021)

12. Информационное право: учебник / под ред. И. Л. Бачило. – М.: Издательство Юрайт, 2016. – 419 с.

13. Информационное право: учебник для вузов / М. А. Федотов [и др.]; под редакцией М. А. Федотова. — Москва : Издательство Юрайт, 2020. — 497 с.

14. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001. № 195-ФЗ (ред. от 30.04.2021) // СЗ РФ. – 07.01.2002. №1 (ч. 1). ст. 1

15. Колобаева Н.Е. Право на доступ к информации о деятельности органов власти [Электронный ресурс] / Н.Е. Колобаева. - Режим доступа: URL: https://cyberleninka.ru/article/n/pravo-na-dostup-k-informatsii-o-deyatelnosti-organov-vlasti/viewer (дата обращения 15.05.2021)

16. «Конституция Российской Федерации» (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе

общероссийского голосования 01.07.2020) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 04.07.2020

17. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.) [Электронный ресурс] / Национальный правовой Интернет-портал Республики Беларусь. - Режим доступа: URL: https://pravo.by/pravovaya-informatsiya/normativnye-dokumenty/konstitutsiya-respubliki-belarus/ (дата обращения: 11.03.2021)

18. «Концепция информационной политики судебной системы на 2020 - 2030 годы» (одобрена Советом судей РФ 05.12.2019) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа:URL:http://www.consultant.ru/cons/cgi/online.cgi?req=doc&ts=1162202930542670133595961 8&cacheid=5BC85DC14579509F3C51635082834635&mode=splus&base=LAW&n=339776&rnd=4889E3608FEC3B45F6F4CA33172F5CD1#1y9fyg9n0eh (дата обращения: 17.01.2021)

19. Кузнецов П. У. Основы информационного права: учебник для бакалавров. - Москва: Проспект, 2015. - 312 с.

20. Лапин Ю.С. Понятие права граждан на информацию [Электронный ресурс] / Ю.С. Лапин. – Режим доступа: URL: https://cyberleninka.ru/article/n/ponyatie-prava-grazhdan-na-informatsiyu/viewer (дата обращения: 15.05.2021)

21. Максимова О.И. Право человека на информацию в конституционном законодательстве РФ и зарубежных государств [Электронный ресурс] / О.И. Максимова. - Режим доступа: URL: file:///C:/Users/Влад/Downloads/pravo-cheloveka-na-informatsiyu-v-konstitutsionnom-zakonodatelstve-rf-i-zarubezhnyh-gosudarstv-sravnitelno-pravovoy-analiz.pdf (дата обращения: 28.03.2021)

22. Мельников В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2017. - 336 с.

23. Мельничук М.А. Опыт Канады в правовом регулировании доступа к информации [Электронный ресурс] / М.А. Мельничук. - Режим доступа:URL:file:///C:/Users/%D0%92%D0%BB%D0%B0%D0%B4/Downloads/opyt-kanady-v-pravovom-regulirovanii-dostupa-k-informatsii.pdf (дата обращения: 26.02.2021)

24. Мельничук М.А. Актуальные тенденции правового регулирования доступа к информации в России и за рубежом [Электронный ресурс] / М.А. Мельничук. - Режим доступа: URL: file:///C:/Users/%D0%92%D0%BB%D0%B0%D0%B4/Downloads/aktualnye-tendentsii-pravovogo-regulirovaniya-dostupa-k-informatsii-v-rossii-i-za-rubezhom%20(3).pdf (дата обращения: 02.04.2021)

25. Олейник С.А., Мельничук М.А. Правовое регулирование доступа к информации на примере Канады (сравнительно-правовая характеристика) [Электронный ресурс] / С.А. Олейник, М.А. Мельничук. - Режим доступа: URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-dostupa-k-informatsii-na-primere-kanady-sravnitelno-pravovaya-harakteristika/viewer (дата обращения: 09.04.2021)

26. Петречук А.С. Правовое регулирование доступа к информации о деятельности органов государственной власти и местного самоуправления [Электронный ресурс] / А.С. Петречук. - Режим доступа: URL: https://cyberleninka.ru/article/n/pravovoe-regulirovanie-dostupa-k-informatsii-o-deyatelnosti-organov-gosudarstvennoy-vlasti-i-mestnogo-samoupravleniya/viewer (дата обращения: 16.05.2021)

27. Послание Президента РФ Федеральному Собранию от 23.02.1996. // СЗ РФ. – № 39. 27.02.1996

28. Постановление Правительства РФ от 16.03.2009. № 228 (ред. от 28.12.2020) «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» (вместе с «Положением о Федеральной службе по надзору в сфере связи,

информационных технологий и массовых коммуникаций») // СЗ РФ. – 23.03.2009. – № 12. ст. 1431

29. Постановление Правительства РФ от 22.12.2018. № 1636 «Об утверждении перечня объектов инфраструктуры внеуличного транспорта (в части метрополитенов), являющихся объектами транспортной инфраструктуры» // СЗ РФ. – 31.12.2018. – № 53 (часть II). ст. 8676

30. Прокламация о Конституционном акте 1982 г. [Электронный ресурс] / Прокламация о Конституционном акте 1982 г.- Режим доступа: URL:https://www.concourt.am/armenian/legal_resources/world_constitutions/constit/canada/canada-r.htm (дата обращения: 15.04.2021)

31. Приказ ФСБ России от 24.07.2018. № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» (Зарегистрировано в Минюсте России 06.09.2018 № 52107) // Официальный интернет-портал правовой информации http://www.pravo.gov.ru, 10.09.2018

32. «Семейный кодекс Российской Федерации» от 29.12.1995. № 223-ФЗ (ред. от 04.02.2021, с изм. от 02.03.2021) // СЗ РФ. – 01.01.1996. № 1. ст.16

33. Тимербаев Т.А. Право граждан на информацию [Электронный ресурс] / Т.А. Тимербаев. – Режим доступа: URL:

https://cyberleninka.ru/article/n/pravo-grazhdan-na-informatsiyu/viewer (дата обращения 12.05.2021)

34. «Трудовой кодекс Российской Федерации» от 30.12.2001. № 197-ФЗ (ред. от 30.04.2021) (с изм. и доп., вступ. в силу с 01.05.2021) // СЗ РФ. – 07.01.2002. – №1 (ч. 1). ст. 3

35. «Уголовный кодекс Российской Федерации» от 13.06.1996. № 63-ФЗ (ред. от 05.04.2021, с изм. от 08.04.2021) // СЗ РФ. – 17.06.1996. –№ 25. ст. 2954

36. Указ Президента РФ от 05.12.2016. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. – 12.12.2016. – № 50. ст. 7074

37. Указ Президента РФ от 06.03.1997. № 188 (ред. от 13.07.2015) «Об утверждении Перечня сведений конфиденциального характера» // СЗ РФ. – 10.03.1997. – № 10. ст. 1127

38. Указ Президента РФ от 13.05.2017. № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» // СЗ РФ. – 15.05.2017. – № 20. ст. 2902

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

40. Указ Президента РФ от 17.03.2008. № 351 (ред. от 22.05.2015) «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» // СЗ РФ. – 24.03.2008. – № 12. ст. 1110

41. Указ Президента РФ от 17.12.1997. № 1300 (ред. от 10.01.2000) «Об утверждении Концепции национальной безопасности Российской Федерации» // СЗ РФ. – № 247. 26.12.1997. (утратил силу)

42. Указ Президента РФ от 22.05.2015. № 260 «О некоторых вопросах информационной безопасности Российской Федерации» (вместе с «Порядком подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет») // СЗ РФ. – 25.05.2015. – № 21. ст. 3092

43. Указ Президента РФ от 22.12.2017. № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» // СЗ РФ. – 25.12.2017. – № 52 (Часть I). ст. 8112 (58)

44. Указ Президента РФ от 31.12.2015. № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. – 04.01.2016. – № 1 (часть II). ст. 212

45. Федеральный закон от 02.05.2006. № 59-ФЗ (ред. от 27.12.2018) «О порядке рассмотрения обращений граждан Российской Федерации» // СЗ РФ. – 08.05.2006. – № 19. ст. 2060

46. Федеральный закон от 07.07.2003. № 126-ФЗ (ред. от 30.04.2021) «О связи» // СЗ РФ. – 14.07.2003. – № 28. ст. 2895

47. Федеральный закон от 09.02.2007. № 16-ФЗ (ред. от 02.12.2019) «О транспортной безопасности» // СЗ РФ. – 12.02.2007. – № 7. ст. 837

48. Федеральный закон от 09.02.2009. № 8-ФЗ (ред. от 30.04.2021) «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» // СЗ РФ. – 16.02.2009. – № 7. ст. 776

49. Федеральный закон от 10.01.2002. № 7-ФЗ (ред. от 09.03.2021) «Об охране окружающей среды» // СЗ РФ. – 14.01.2002. – № 2. ст. 133

50. Федеральный закон от 13.01.1995. № 7-ФЗ (ред. от 12.03.2014) «О порядке освещения деятельности органов государственной власти в государственных средствах массовой информации» // СЗ РФ. – 16.01.1995. – № 3. ст. 170

51. Федеральный закон от 17.07.1999. № 176-ФЗ (ред. от 27.12.2019) «О почтовой связи» // СЗ РФ. – 19.07.1999. – № 29. ст. 3697

52. Федеральный закон от 20.02.1995. № 24-ФЗ (ред. от 10.01.2003) «Об информации, информатизации и защите информации» // СЗ РФ. – 20.02.1995. – № 8. ст. 609 (Утратил силу)

53. Федеральный закон от 20.07.2012. № 125-ФЗ (ред. от 08.12.2020) «О донорстве крови и ее компонентов» // СЗ РФ. – 23.07.2012. – № 30. ст. 4176

54. Федеральный закон от 21.11.2011. № 323-ФЗ (ред. от 30.04.2021) «Об основах охраны здоровья граждан в Российской Федерации» // СЗ РФ. – 28.11.2011. – № 48. ст. 6724

55. Федеральный закон от 22.12.2008. № 262-ФЗ (ред. от 08.12.2020) «Об обеспечении доступа к информации о деятельности судов в Российской Федерации» // СЗ РФ. – 29.12.2008. – № 52 (ч. 1). ст. 6217

56. Федеральный закон от 26.07.2017. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. – 31.07.2017. – № 31 (Часть I). ст. 4736

57. Федеральный закон от 27.07.2004. № 79-ФЗ (ред. от 24.03.2021) «О государственной гражданской службе Российской Федерации» СЗ РФ. – 02.08.2004. – № 31. ст. 3215

58. Федеральный закон от 27.07.2006. № 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 20.03.2021) // СЗ РФ. – 31.07.2006. – № 31 (1 ч.). ст. 3448

59. Федеральный закон от 27.07.2006. № 152-ФЗ (ред. от 30.12.2020) «О персональных данных» (с изм. и доп., вступ. в силу с 01.03.2021) // СЗ РФ. – 31.07.2006. – № 31 (1 ч.). ст. 3451

60. Федеральный закон от 28.11.2011. №335-ФЗ (ред. от 27.12.2018) «Об инвестиционном товариществе» // СЗ РФ. – 05.12.2011. – № 49 (ч. 1). ст. 7013

61. Федеральный закон от 28.12.2010. № 390-ФЗ (ред. от 09.11.2020) «О безопасности» // СЗ РФ. – 03.01.2011. – № 1. ст. 2

62. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 20.03.2021) // СЗ РФ. - 31.07.2006.- № 31 (1 ч.). ст. 3448

63. Федеральный закон от 29.07.2004. № 98-ФЗ (ред. от 09.03.2021) «О коммерческой тайне» // СЗ РФ. – 09.08.2004. – № 32. ст. 3283

64. Федеральный закон от 29.12.2010. № 436-ФЗ (ред. от 05.04.2021) «О защите детей от информации, причиняющей вред их здоровью и развитию» // СЗ РФ. – 03.01.2011. – N 1, ст. 48

65. Федеральный закон от 29.12.2012. № 273-ФЗ (ред. от 30.04.2021) «Об образовании в Российской Федерации» // СЗ РФ. –31.12.2012. – № 53 (ч. 1). ст. 7598

66. Федосеева Н.Н. Доступ общественности к информации о деятельности судов в Российской Федерации [Электронный ресурс] / Н.Н. Федосеева. - Режим доступа: URL: https://cyberleninka.ru/article/n/dostup-obschestvennosti-k-informatsii-o-deyatelnosti-sudov-v-rossiyskoy-federatsii/viewer (дата обращения: 27.03.2021)

67. Хабриева Т. Я., Чиркин В. Е. Теория современной конституции. М.: Норма, 2005.320 с.