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 «Правовая политика в сфере информационной безопасности»

Обучающийся А.А. Михайлова _____
(Инициалы Фамилия) (личная подпись)

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

Тольятти 2023

Аннотация

Тема выпускной квалификационной работы: «Правовая политика в сфере информационной безопасности».

Актуальность темы выпускной квалификационной работы. В настоящее время в нашей стране происходит прогрессивное развитие в информационной сфере, и создаются новейшие технологии и программы, а также усовершенствуются старые. В результате возникают опасности в способах хранения, обработки и передачи информации, в дальнейшем может быть причинен ущерб личности, обществу и государству.

Цель выпускной квалификационной работы заключается в изучении и проведении анализа теоретических и нормативных положений, которые имеют отношение к информационной безопасности Российской Федерации.

Для достижения определенной рамками написания выпускной квалификационной работы были сформированы следующие задачи:

1. определить понятие информационной безопасности;
2. установить и охарактеризовать основные угрозы;
3. изучить нормативно-правовые акты в сфере информационной безопасности в Российской Федерации и зарубежных стран;
4. изучить деятельность государства по борьбе с информационными угрозами;
5. указать ответственность за правонарушения граждан в информационной сфере.

При написании работы использовалось большое количество нормативно-правовых актов Российской Федерации и зарубежных государств, регулирующих национальную и информационную безопасность, а также специальную литературу и высказывания ученых по теме исследования.

По своей структуре работа состоит из введения, двух глав, разделенных на параграфы, заключения, а также списка используемой литературы и используемых источников.

Оглавление

Введение 4

Глава 1. Понятия и правовое регулирование информационной безопасности 8

1.1 Информационная безопасность в системе национальной безопасности 8

1.2 Правовое регулирование информационной безопасности 14

1.3 Концепции информационной безопасность в иностранных государствах 23

Глава 2. Современные информационные угрозы, пути и методы их устранения 36

2.1 Общая характеристика и виды информационных угроз 36

2.2 Деятельность государства по противодействию информационным угрозам 42

2.3 Предотвращение преступлений и ответственность граждан за правонарушения в сфере информационной безопасности 51

Заключение 64

Список литературы и используемых источников 68

Введение

Рассматривая данную тему, мы коснемся тех проблем, которые существуют в наше время и оказывают огромное влияние на все сферы нашей жизни и национальную безопасность государства.

Формирование информационного общества опирается на новейшие информационные, телекоммуникационные технологии и технологии связи. Благодаря этому новейшие технологии привели к сильному распространению глобальных информационных сетей, которые открывают новые возможности международного информационного обмена.

Именно поэтому актуальность темы исследования определена следующими положениями. Так, государство должно следить за законностью создания новейших информационных технологий и усовершенствования старых. Более того, своевременно принимать определенные законы, касающиеся информации и не допускать пробелы в законодательстве при обеспечении национальной и информационной безопасностей личности, общества и государства.

К тому же следует указать, в современном мире в основном вся информация содержится в электронном виде, поэтому ни одна программа защиты не дает стопроцентную гарантию о том, что вся информация будет защищена от взлома. Таким образом, происходит утечка информации. Кроме этого существует много информационных угроз, способные привести к утрате, изменению или незаконному распространению информации. Для их предотвращения государству необходимо разрабатывать новые законы и принимать меры ответственности за правонарушения в сфере информации.

Таким образом, данные проблемы имеют актуальность на сегодняшний день и требуют их решения.

Цель выпускной квалификационной работы заключается в изучении и проведении анализа теоретических и нормативных положений, которые имеют отношение к информационной безопасности Российской Федерации.

Для достижения определенной рамками написания выпускной квалификационной работы были сформированы следующие задачи:

1. определить понятие информационной безопасности;
2. установить и охарактеризовать основные угрозы;
3. изучить нормативно-правовые акты, которые прямо указывают на информационную безопасность;
4. проанализировать акты правового регулирования права на доступ к информации зарубежных стран;
5. изучить деятельность государства по борьбе с информационными угрозами;
6. указать ответственность за правонарушения граждан в информационной сфере.

Объектом исследования в рамках выпускной квалификационной работы являются общественные отношения, которые влияют на информационную безопасность.

Предметом исследования в рамках выпускной квалификационной работы являются теоретические положения, выраженные в виде нормативно-правовой базы Российской Федерации, а также иных действующих нормативных актов, имеющих международно–правовой характер.

Базой исследования работы являются нормативно-правовые акты, к которым можно отнести: Конституцию РФ, Трудовой кодекс РФ, Уголовный кодекс РФ, Кодекс об административных правонарушениях РФ, Гражданский кодекс РФ, Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности», Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 20.02.1995 № 24-ФЗ «Об информации, информатизации и защите информации»; Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы», Указ Президента РФ от 1 мая

2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» и другие.

Проведен анализ трудов российских и иностранных ученых: Проведен анализ трудов следующих ученых: В.И. Даль; С.Г. Трясогузова; Н.А. Косолапов; А.В. Манойло; И.Н. Панарин; С.С. Алексеев; Н.И. Матузов; М.А. Федотов; П.У. Кузнецов и других.

В ходе написания данной работы были применены следующие методы и методики:

1. анализ нормативно-правовой базы, способствующий дать понятиям точные определения и изучить нормы законодательства;

2. анализ справочной литературы;

3. сравнение;

4. синтез, используемый для суммирования выявленных сведений и данных по теме работы;

5. исторический метод, позволяющий всецело изучить исторические закономерности через конкретные исторические события и факты;

6. специально–юридический, позволяющий дать определения юридическим понятиям, выявить их признаки и классифицировать;

7. сравнительно-правовой.

Теоретическая значимость указанного исследования в рамках написания выпускной квалификационной работы определена анализом законотворчества и правоприменения в области обеспечения информационной безопасности.

Практическая значимость указанного исследования в рамках написания выпускной квалификационной работы обусловлена выявлением роли в области обеспечения информационной безопасности.

По своей структуре выпускная квалификационная работа состоит из введения, двух глав, заключения, а также списка литературы и используемых источников.

Первая глава содержит в себе теоретические основы национальной и информационной безопасности. Исследованы ключевые понятия, содержание,

виды и принципы национальной и информационной безопасности, а также правовое регулирование национальной и информационной безопасности в Российской Федерации и зарубежных государств: Соединенные Штаты Америки, Китайская Народная Республика и Республика Беларусь.

Вторая глава рассматривает информационные угрозы. Исследованы виды и общая характеристика информационных угроз, а именно их пути и методы устранения. Также данная глава содержит законодательные акты о деятельности государства по противодействию информационным угрозам и ответственность граждан за правонарушение в сфере информации. Кроме того указаны методы предотвращения преступлений в сфере информационной безопасности.

Глава 1. Понятия и правовое регулирование информационной безопасности

1.1 Информационная безопасность в системе национальной безопасности

Итак, приступая к изложению основного вопроса в рамках первой главы, именно, места информационной безопасности в системе национальной безопасности, так для начала необходимо начать исследование с определений национальной и информационной безопасностей.

Самым главным вначале необходимо отметить термин «безопасность». Так, толковый словарь под авторством русского писателя-этнографа В.И. Даля представляет вышеуказанное определение как: «отсутствие опасности; сохранность, надёжность» [2].

Также предоставляется возможным, указать понимание автора-составителя С.Г. Трясогузовой. В своем толковом словаре она представляет «безопасность» как: «состояние, при котором не угрожает опасность, есть защита от опасности» [19].

Таким образом, перед определением понятия национальной безопасности обозначим фундаментальные документы, по регулированию вопросов обеспечения национальной безопасности. Самое первое определение «национальной безопасности» содержится в Федеральном законе от 20 февраля 1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» [37]. Данный закон не раскрывает сущность и содержание национальной безопасности. 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» [15].

Далее, следует указать Концепцию национальной безопасности РФ № 1300 [30]. Данный нормативный документ был создан 17.12.1997 года,

далее Указом Президента РФ № 24 от 10.01.2000 года были внесены изменения и дополнения. Значение указанного документа можно описать как комплекс мероприятий, которые разработало государство, для обеспечения безопасности личности, общества и государства в целом от возможных внутренних и внешних угроз. В дальнейшем, данная Концепция была упразднена и переделана в Стратегию национальной безопасности РФ, которая утверждена Указом Президента РФ № 537 от 12.05.2009 года [31]. Далее, Указом Президента РФ от 31.12.2015 года № 683 «О Стратегии национальной безопасности Российской Федерации» [33] была признана утратившим силу Указ Президента Российской Федерации от 12.05.2009 года № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года». В настоящее время действующим документом является Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [28], при этом, ранее действовавший Указ Президента РФ от 31.12.2015 года № 683 «О Стратегии национальной безопасности Российской Федерации» утратил свою силу.

Существующая Стратегия национальной безопасности Российской Федерации в свою очередь имеет одну из версий, сформированную годами, о дефиниции национальной безопасности государства. Таким образом, согласно общим положениям Стратегии, под последней следует понимать: «национальная безопасность Российской Федерации (далее – национальная безопасность) – состояние защищенности национальных интересов Российской Федерации от внешних и внутренних угроз, при котором обеспечиваются реализация конституционных прав и свобод граждан, достойные качество и уровень их жизни, гражданский мир и согласие в стране, охрана суверенитета Российской Федерации, ее независимости и государственной целостности, социально-экономическое развитие страны» [28].

Исходя из определения, отмеченного в Стратегии национальной безопасности Российской Федерации, замечаем, что безопасность содержит в

себе еще ряд понятий - личности, общества, национальных ценностей, национального образа жизни, жизненно важных интересов, внешних и внутренних угроз. Данные понятие можно являются базовыми элементами в формировании национальной безопасности. Необходимо подробно описать каждое из них.

Под определением личности необходимо понимать конкретного индивида, которому присущи права и обязанности. Также обладающий совокупностью социально значимых черт, свойств и качеств, которые он реализует в общественной жизни.

Под понятием общества понимается совокупность различных форм объединения личностей и способов их взаимодействия.

Национальные ценности представляют приоритетные нравственные установки, которые существуют в социально – исторических, семейных, культурных и религиозных традициях многонационального народа государства.

Под национальным образом жизни понимается исторически принятые в обществе формы социального и индивидуального поведения, кроме того нравственный уклон и система оценок, нарушения, приводящие к утрате самобытности или иным негативным последствиям.

Жизненно важные интересы представляют собой систему потребностей личности, общества и государства, удовлетворенность которых создает существование и возможность прогрессивного развития личности, общества и государства.

Под угрозой, в общем виде, можно понимать как намеренное причинение вреда кому-либо или чему-либо. Когда, в свою очередь, под национальной угрозой понимается «совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба национальным интересам Российской Федерации». Данное определение указано в Стратегии национальной безопасности.

Исходя из этого, можно выделить угрозы по месту зарождения:

– к внешним угрозам относятся снижение значимости РФ в мировой экономике из-за действий иностранных государств; наличие крупных группировок иностранных вооруженных сил у границ Российской Федерации; увеличение количества в мире оружия массового уничтожения; ослабление позиций России в сфере информации и телекоммуникаций; международный терроризм и другое;

– внутренние выражаются в развитии коррупции на территории России; снижении материального и духовного благосостояния населения; возникновении незаконных вооруженных группировок; ухудшении экологической ситуации; появлении национального и религиозного экстремизма и другое.

Таким образом, упомянутые выше угрозы национальной безопасности не единственные. Данный список может дополняться исходя из ситуаций в мире.

Еще одной классификацией может быть, угрозы по сферам воздействия:

– информационная сфера,

– экономическая сфера,

– научно-техническая сфера,

– социальная сфера,

– экологическая сфера,

– оборонная сфера,

– политическая сфера,

– и иные сферы.

В соответствии с указанной классификацией, можно сделать заключение о том, что внешние и внутренние угрозы обладают различным характером, сферой распространения и степенью опасности. Данные характеристики могут привести к различным последствиям, в том числе по объему и продолжительностью. Угрозы национальной безопасности вполне имеют возможность возникать и пропадать, увеличиваться и уменьшаться, а также есть возможность поменять сферу воздействия. Данные угрозы не

ограниченны в количестве, существует возможность их возникновения неопределенного количества. На основе характеристик меняется важность определенной угрозы для государства. Поэтому для обеспечения высшего уровня национальной безопасности от угроз является правильное прогнозирование и определение приоритетов, а также распределение имеющихся средств, сил и ресурсов в деятельности государственных органов.

Также необходимо упомянуть мнение российского политолога Н.А. Косолапова. По его мнению, «национальная безопасность – это стабильность, которая может поддерживаться на протяжении длительного времени, состояние достаточно разумной динамической защищенности от наиболее существенных из реально существующих угроз и опасностей, а также способности распознавать такие вызовы и своевременно принимать необходимые меры для их нейтрализации».

Так, относительно вопроса государственного обеспечения безопасности составляет один из нормативных актов Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» [43]. Указанный Федеральный закон устанавливает основные принципы и сущность деятельности по обеспечению безопасности личности, общества, государства, информационной безопасности, а также других видов безопасности, предусмотренных законодательством Российской Федерации.

Так, в соответствии со статьей 2 ФЗ «О безопасности», «основными принципами обеспечения безопасности являются: соблюдение и защита прав и свобод человека и гражданина; законность; системность и комплексность применения публичными органами власти политических, организационных, социально-экономических, информационных, правовых и иных мер обеспечения безопасности; приоритет предупредительных мер в целях обеспечения безопасности; взаимодействие органов государственной власти с общественными объединениями, международными организациями и гражданами в целях обеспечения безопасности» [43].

Для определения места информационной безопасности в системе национальной безопасности, следует упомянуть пункт 103 «Стратегии национальной безопасности РФ» [28], который содержит такую информацию «Реализация настоящей Стратегии осуществляется на плановой основе путем согласованных действий органов публичной власти, организаций и институтов гражданского общества под руководством Президента Российской Федерации за счет комплексного применения политических, организационных, социально-экономических, правовых, информационных, военных, специальных и иных мер, разработанных в рамках стратегического планирования в Российской Федерации». Таким образом, информационная безопасность считается одним из значительных направлений для обеспечения национальной безопасности.

Далее, необходимо указать «Доктрину информационной безопасности» [29], которая содержит «Национальные интересы в информационной сфере:

а) 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;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) 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;

г) 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;

д) 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» [29].

Итак, упомянув национальные интересы, касающиеся информационной безопасности, замечаем, что в современное время данная сфера считается одной из важных для национальной безопасности. Так из-за правильного составления, применения, распространения и защиты информации, осуществление деятельности в остальных сферах безопасности будет эффективнее.

Таким образом, в следующем параграфе необходимо подробно изучить правовую основу информационной безопасности, а также указать в каких нормативных актах содержатся основные направления обеспечения информационной безопасности.

1.2 Правовое регулирование информационной безопасности

Далее, следует более подробно разобрать понятие «информационная безопасность». Для того чтобы определить указанную дефиницию, нужно обратиться к пункту 2 Доктрины информационной безопасности Российской Федерации, в которой указано, 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» [29].

Таким образом, «понятие информационной безопасности в узком смысле этого слова подразумевает:

– надежность работы компьютера;

– сохранность ценных данных;

– защиту информации от внесения в нее изменений неуполномоченными лицами;

– сохранение тайны переписки в электронной связи» говорится в работе [9; с. 9].

Далее, «информационная безопасность включает:

– состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;

– состояние инфраструктуры, при котором информация используется строго по назначению и не оказывает негативного воздействия на систему при ее использовании;

– состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как конфиденциальность, целостность и доступность;

– экономическую составляющую (структуры управления в экономической сфере, включая системы сбора, накопления и обработки

информации в интересах управления производственными структурами, системы общеэкономического анализа и прогнозирования хозяйственного развития, системы управления и координации в промышленности и на транспорте, системы управления энергосистем, централизованного снабжения, системы принятия решения и координации действий в чрезвычайных ситуациях, информационные и телекоммуникационные системы);

– финансовую составляющую (информационные сети и базы данных банков и банковских объединений, системы финансового обмена и финансовых расчетов)» [9; с. 8].

Информационная безопасность государства является одним из основных приоритетов в сфере обеспечения национальной безопасности. Так, необходимо выделить активные темп информатизации и цифровизации общества. Новые информационные технологии со временем делают из информации ценнейший ресурс современности. Вышеотмеченное предопределяется присутствием ряда угроз, которые сопутствуют формированию информационных технологий. Необходимо отметить, что в последнем десятилетии XX века происходило значительное развитие правовой базы обеспечения информационной безопасности. Благодаря этому, росло количество нормативных актов, приуроченных проблеме регулированию информации в обществе и государстве. В связи с этим, из числа таких актов, посвятивших обеспечению информационной безопасности, можно отметить, на пример: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [41], Закон РФ от 21.07.1993 № 5485-1 «О государственной тайне» [8] и Доктрина информационной безопасности Российской Федерации (далее – Доктрина) [29]. Таким образом, согласно положениям Доктрины, ключевыми направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

«а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;

и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей» [29].

В Доктрине информационной безопасности Российской Федерации впервые появляется понятие системы обеспечения национальной безопасности Российской Федерации. В соответствии с п.30 указанной Доктрины обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами. Президент Российской Федерации определят состав системы обеспечения национальной безопасности. Организационную основу системы обеспечения национальной безопасности можно найти в пункте 33 Доктрины информационной безопасности Российской Федерации. В нее входят: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы,

создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности [29].

Для более полного изучения темы дипломной работы, необходимо указать, что в настоящее время существует еще один важный документ в области информационной безопасности. Таким документом является Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы [34], утвержденная указом Президента Российской Федерации от 09.05.2017 года № 203. Данная Стратегия содержит цели, задачи и меры по осуществлению внутренней и внешней политики Российской Федерации в сфере использования информационных и коммуникационных технологий, которые направлены на развитие информационного общества, создании национальной цифровой экономики, предоставлении национальных интересов и использование стратегических национальных приоритетов.

Не стоит забывать про Конституцию Российской Федерации [12], которая содержит большое количество статей, составляющих основу информационной безопасности. Закрепление основных прав в данном законе гарантируют реализацию и контроль за исполнением со стороны государства.

Также необходимо указать Федеральный закон «О безопасности» от 28.12.2010 г. № 390-ФЗ [43]. Данный нормативно-правовой акт содержит в себе важные направления деятельности, которые определяются как «состояние защищенности личности, общества и государства» от различных угроз. Информационные угрозы не являются исключением, так как имеют большое значение в национальной безопасности.

Далее, в рамках рассмотрения данной темы дипломной работы, необходимо упомянуть Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [42], в котором содержатся понятия персональных данных:

«1) персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных);

2) персональные данные, разрешенные субъектом персональных данных для распространения, – персональные данные, доступ неограниченного круга лиц к которым предоставлен субъектом персональных данных путем дачи согласия на обработку персональных данных, разрешенных субъектом персональных данных для распространения в порядке, предусмотренном настоящим Федеральным законом» [42].

Таким образом, для защиты данных в статье 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [41] предусматривается такое понятие как конфиденциальность информации. «Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя» [41]. Также Федеральный закон «Об информации, информационных технологиях и о защите информации» направлен на регулирование отношений, которые возникают при осуществлении прав на поиск, получение, передачу, производство и распространение информации. Они основываются на следующих принципах:

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

2) установление ограничений доступа к информации только федеральными законами;

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

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

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

6) достоверность информации и своевременность ее предоставления;

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

8) 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» [41].

Кроме этого на основании данного Федерального закона осуществляется применение информационных технологий и обеспечение защиты информации.

Также стоит отметить Федеральный закон «О коммерческой тайне» от 29.07.2004 г. № 98-ФЗ [40]. Данный закон регулирует отношения, которые направлены на установления, изменения и прекращения режима коммерческой тайны, в отношении информации, которая имеет ценность в связи с недоступностью ее для третьих лиц. Еще закон содержит права на отнесение информации к коммерческой тайне, права обладателя, а также охрану конфиденциальности информации и ответственность за нарушение норм указанного нормативно-правового акта.

Еще одним из законов, относящихся к информационной безопасности, является Закон РФ «О государственной тайне» от 21.07.1993 № 5485-1 [8]. Данный акт направлен на защиту сведений составляющих государственную тайну, а именно в области военной, экономической, научной, внешнеполитической, разведывательной, контрразведывательной и оперативно розыскной деятельности государства, распространение которых может нанести ущерб безопасности Российской Федерации. Также указанный

закон содержит перечень сведений, составляющих государственную тайну, регулирует доступ к информации, порядок засекречивания и рассекречивания, устанавливает степень секретности, ответственность и контрольно-надзорные функции за соблюдением данного закона.

Таким образом, в области обеспечения информационной безопасности существуют и другие нормативно-правовые акты, так как в современном мире информация распространяется на все сферы жизни общества.

Отталкиваясь от вышеизложенного, следует, что информация и информационные технологии играют важную роль в жизнедеятельности современного человека. Поэтому деятельность органов государственной власти в обеспечении безопасности информации основывается должным образом на разработанной нормативной базе.

1.3 Концепции информационной безопасность в иностранных государствах

Продолжая исследование по данной теме, представляется необходимым затронуть вопрос зарубежного опыта в информационной безопасности.

Таким образом, ссылаясь на вышеуказанную информацию, можно прийти к выводу о том, что вопрос обеспечения информационной безопасности наиболее активно поднимается и остается в приоритете каждого современного государства.

Одним из государств, которое стоит рассмотреть, являются Соединенные Штаты Америки. В настоящее время в законодательстве данного государства насчитывается около 500 нормативно-правовых актов, относящиеся к информационной безопасности, среди них можно выделить:

1. закон «О свободе информации (США)»;
2. закон «О секретности»;
3. закон «О праве на финансовую секретность»;
4. закон «О доступе к информации о деятельности ЦРУ»;
5. закон «О неприкосновенности частной жизни»;
6. закон «О защите частной жизни человека»;
7. закон «Закон о компьютерной безопасности»;
8. закон «О компьютерных злоупотреблениях и мошенничестве»;
9. указ Президента США «Информация по национальной безопасности» и другие.

Главным законом в правовом регулировании информационной безопасности в США является «Закон о компьютерной безопасности» № 100-235, принятый в 1987 году. Его целью является повышение безопасности и конфиденциальности секретной информации в федеральных компьютерных системах, а также формирование минимально приемлемых методов обеспечения безопасности таких систем. Данным законом был разработан Национальный институт стандарта технологий (NIST) –

конкретный исполнитель, который отвечает за выпуск стандартов и руководств, которые направлены на защиту от уничтожения и несанкционированного доступа к информации, а также от краж и подлогов, выполняемых с помощью компьютеров. Федеральный закон «Закон о компьютерной безопасности» был упразднен и в 2002 году был принят новый Федеральный закон «Закон об управлении информационной безопасностью» № 107-347. Новый акт требует, чтобы каждое федеральное агентство разработало, задокументировало и внедрило общеагентскую программу по обеспечению информационной безопасности и систем, поддерживающих операции и активы агентства, включая те, которые предоставляются или управляются другим агентством, подрядчиком или другими источниками.

Закон о свободе информации (английское название Freedom of Information Act, сокращенно FOIA) – это федеральный закон о свободе информации, который позволяет полное или частичное обнародование информации и документов правительства США. Данный закон был подписан президентом Линдоном Б. Джонсоном 4 июля 1966 года, и вступил в силу в следующем году. Закон применяется только к документам органов исполнительной власти.

Благодаря указанному закону, гражданин США имеет право запросить у любого федерального ведомства США любые документы, за исключением тех, которые относятся к правоохранительным органам, национальной обороне, финансовым и личным документам. В случае если государственное учреждение имеет запрашиваемый документ гражданином США и не предоставляет, то местный суд в принудительном порядке извлекает и передает информацию гражданину.

Следует отметить, что при сравнении законодательства США и Российской Федерации, можно увидеть, что в первом отсутствуют какие-либо нормативно-правовые акты, запрещающие разглашение государственной тайны. Так, сам Конгресс США неоднократно отказывал в принятии

соответствующих законов, считая, что раскрытие государственной тайны в данном государстве не является преступлением.

Как замечалось, представители власти США часто сами разглашали информацию, которая относится к государственной тайне, в средствах массовой информации.

Таким образом, отсутствие списка определенной информации, относимого к государственной тайне, влечет сложность для установления факта нарушения законодательства для лиц, разгласивших информацию.

Далее, говоря о правовой защиты персональных данных в Соединенных Штатах Америки, необходимо указать закон «О защите частной жизни человека», принятый в 1974 году. Данный закон указывает на право заинтересованного лица на получение данных, собранных о нем, а также на их уточнение, блокирование или устранение. В случае отказа предоставления ему таких прав, владелец вправе обжаловать даны действия в административном или судебном порядке. К данным относятся подборка информации о физическом лице, сведения об образовании, медицинские, финансовые данные, наличие или отсутствие судимости, отпечатки пальцев или запись голоса, а также любая идентификационная деталь.

Закон «О неприкосновенности частной жизни» был принят в 1974 году. Целью его создание является обеспечение достоверной обработки информации. В соответствии с указанным законом под сбор, обработку, использование и распространение попадают данные, которые находятся в системе записей федеральными агентствами. Закон «О неприкосновенности частной жизни» считается главным в США. Он включает в себя законы об Интернете, безопасности данных и конфиденциальности в США.

Следующей страной, которую необходимо упомянуть, является Китай. В указанной стране существует три важных закона в сфере информационной безопасности. Одним из главных и новых законов, можно выделить Закон КНР «О безопасности данных». Он был принят на 29-м заседании Постоянного комитета Тринадцатого Всекитайского собрания народных представителей 10

июня 2021 г. и вступил в силу 1 сентября 2021 г. Закон КНР «О безопасности данных» указывает основы правового регулирования в сфере обеспечения безопасности, управления, обработки и экспорта данных, также устанавливает юридическую ответственность за правонарушения.

Так, целью Закона КНР «О безопасности данных» является регулирование обработки данных, обеспечения безопасности данных, содействие развитию и использованию данных, защиты законных прав и интересов отдельных лиц и организаций, а также защиты суверенитета, безопасности и интересов государства в области развития. Данный закон обязателен для всех операторов данных, которые ведут деятельность на территории КНР, но есть исключения. К обработке данных не относится информация, имеющая отношение к государственной тайне, а также военные данные.

Кроме того, согласно части 2 статьи 2 Закона КНР «О безопасности данных» если обработка данных за пределами территории Китайской Народной Республики наносит ущерб национальной безопасности, общественным интересам или законным правам и интересам отдельных лиц или организаций Китайской Народной Республики, юридическая ответственность подлежит расследованию в соответствии с законом [3].

В соответствии со ст. 3 Закона КНР «О безопасности данных» «Обработка данных» включает, среди прочего, сбор, хранение, использование, обработку, передачу, предоставление и раскрытие данных. «Безопасность данных» означает обеспечение эффективной защиты и законного использования данных посредством принятия необходимых мер, а также способность гарантировать постоянную безопасность данных [3].

Основным ответственным органом, который несет ответственность за принятие решений, обсуждение и координацию работы по обеспечению национальной безопасности данных; исследование, формулирование и руководство реализацией национальной стратегии безопасности данных и соответствующих основных руководящих принципов и политик; координация

основных вопросов и важной работы в отношении национальной безопасности данных; и создание механизма координации национальной безопасности данных, в соответствии со статьей 5 Закона КНР «О безопасности данных» является Центральный орган национальной безопасности.

Также Закон КНР «О безопасности данных» содержит главу юридической ответственности, в которой говорится об ответственности физического лица и организаций, нарушивших закон. Данный закон содержит юридическую ответственность в форме предупреждения, штрафа, выдачи предписаний о приостановлении деятельности, упорядочивания деятельности, а также аннулирования ранее выданных лицензий или принудительной ликвидации.

Таким образом, в соответствии со статьей 45 Закона КНР «О безопасности данных» в случае невыполнения обязанностей по защите безопасных данных компетентный орган издает предписание об устранении нарушений, выносит предупреждение и вправе применить штраф в размере от 50 тыс. до 500 тыс. юаней (примерно от 427 тыс. до 4 млн. 270 тыс. рублей). В дополнение, указанная статья допускает издание предписаний о приостановлении деятельности, внесении исправлений, аннулировании лицензии или принудительной ликвидации.

Руководствуясь Законом КНР «О безопасности данных», вышеперечисленные меры наказания также применяются в следующих случаях нарушения: нарушение национальных правил управления основными данными физическим лицом или организацией и ставит под угрозу национальный суверенитет, безопасность или интересы развития государства; перемещения важных данных за рубеж в нарушение правил проверки безопасности; предоставление оператором данных для зарубежных судов и органов правоприменения без разрешения компетентных органов.

Далее, вторым из трех важных законов, можно выделить, Закон КНР «О сетевой безопасности» (также Закон о кибербезопасности), вступивший в силу 1 июня 2017 г. Данный нормативно-правовой акт регулирует деятельность

поставщиков сетевых продуктов и услуг. Сбор, хранение и обработка персональных данных пользователей осуществляются с целью, обозначенных поставщиком. Также указанный закон определяет порядок и специфику обеспечения безопасности информационной инфраструктуры.

Говоря об истории создания Закона КНР «О сетевой безопасности», следует упомянуть, что одной из причин создания данного нормативно-правового акта послужило создание системы электронного государственного управления в 1999 году. Так, в 2011 году положения о кибербезопасности были внесены в национальное уголовное законодательство КНР, а в 2013 году – в Закон КНР «О защите прав и интересов потребителей». Затем, в июле 2015 года Всекитайское собрание народных представителей опубликовало проект первого Закона о кибербезопасности, и уже 7 ноября 2016 года Закон КНР «О сетевой безопасности» был одобрен в третьем чтении на сессии постоянного комитета Всекитайского собрания народных представителей.

Указанный закон состоит из 7 разделов и 79 статей, содержащих информацию об обеспечении и стимулировании кибербезопасности, безопасности сетевых операций, информационной безопасности, контроле, предупреждении, чрезвычайном реагировании и мер наказания, а также юридической ответственности и дополнительный раздел.

Также, стоит выделить третий немаловажный нормативно-правовой акт в сфере регулирования данных в Китае – Закон КНР «О защите персональных данных». Указанный закон принят Постоянным комитетом Тринадцатого Всекитайского собрания народных представителей 20 августа 2021 года и вступил в силу 1 ноября 2021 года.

Таким образом, Закон КНР «О защите персональных данных» создан в целях защиты прав и интересов в отношении личной информации, а также регулирования деятельности по обработке личной информации и содействия рациональному использованию личной информации в пределах границ Китая. Данный нормативно-правовой акт связан с такими законами как: Закон Китая «О кибербезопасности» и Закон Китая «О безопасности данных». Сферой

применения указанного выше закона распространяется на все организации, которые работают в Китае и обрабатывают личную информацию.

Также стоит упомянуть о содержании Закона КНР «О защите персональных данных». Указанный нормативно-правовой акт состоит из 8 глав и 73 статей, в которых указанны правила обработки личной информации, конфиденциальных данных, положения о государственных органах, обрабатывающих личную информацию, трансграничное предоставление личной информации, права физических лиц, обязанности обработчиков личной информации, а также юридическая ответственность и дополнительные положения.

Для полного анализа, в качестве третьего государства, следует указать, Республику Беларусь. В данной республике правовое регулирование информационной безопасности регулируется подзаконными актами, указами, распоряжениями, постановлениями, а также ведомственными актами. Начало правового обеспечения процессов информатизации в Республике Беларусь содержится в утратившей силу Концепции государственной политики в области информатизации, одобренной Указом Президента Республики Беларусь от 06.04.1999 г. № 195 [27].

Основным законом в целях реализации национальных интересов в Республики Беларусь является Указ Президента Республики Беларусь от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» [26]. Данный акт содержит комплекс взглядов на сущность и содержание деятельности Республики Беларусь по обеспечению интересов личности, общества, государства, а также их защите от внутренних и внешних угроз. Являясь базисом для консолидации усилий личности, общества и государства в целях реализации национальных интересов, настоящая Концепция призвана обеспечить единство подходов к формированию и реализации государственной политики обеспечения национальной безопасности, а также методологическую основу совершенствования актов законодательства в различных сферах национальной

безопасности, разработки документов стратегического планирования. Сохраняя преемственность по отношению к ранее принятым основополагающим документам в сфере национальной безопасности, настоящая Концепция исходит из основных тенденций развития Республики Беларусь, ее места и роли в современном мире [26].

В настоящее время действует Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности Республики Беларусь от 18.03.2019 № 1 [17]. Данная Концепция представляет собой «систему официальных взглядов на сущность и содержание обеспечения национальной безопасности в информационной сфере, определяет стратегические задачи и приоритеты в области обеспечения информационной безопасности. Концепция обеспечивает комплексный подход к проблеме информационной безопасности, создает методологическую основу для совершенствования деятельности по ее укреплению, служит основанием для формирования государственной политики, выработки мер по совершенствованию системы обеспечения информационной безопасности, конструктивного взаимодействия, консолидации усилий и повышения эффективности защиты национальных интересов в информационной сфере» [17].

В соответствии с Постановлением Совета Безопасности Республик Беларусь № 1 «О Концепции информационной безопасности Республики Беларусь», «Концепция информационной безопасности базируется на Концепции национальной безопасности Республики Беларусь, а именно:

– исходит из понимания основных тенденций современного мира, определенных в ней основных национальных интересов в информационной сфере, потенциальных либо реально существующих угроз национальной безопасности;

– конкретизирует цели, задачи и принципы обеспечения национальной безопасности в информационной сфере, основные направления нейтрализации

внутренних источников угроз и защиты от внешних угроз национальной безопасности в данной сфере;

– предполагает реализацию этих целей, задач и принципов как неотъемлемую часть функционирования общей системы обеспечения национальной безопасности» [17].

Далее, «Концепция информационной безопасности также исходит из геополитических интересов Республики Беларусь, ее места и роли в современном мире, основывается на соглашениях о сотрудничестве в области обеспечения информационной безопасности государств – участников Содружества Независимых Государств, государств – членов Организации Договора о коллективной безопасности, двусторонних соглашениях и иных обязательствах Республики Беларусь в области международной информационной безопасности, учитывает основные положения актов международных организаций, в том числе резолюций Генеральной Ассамблеи Организации Объединенных Наций, рекомендаций Организации по безопасности и сотрудничеству в Европе» [17].

Также в правовом регулировании информационной безопасности существует закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации» [4]. Указанным законом регламентируются общественные отношения по получению, сбору, обработке, передаче, поиску, хранении, накоплении, распространении, предоставлении и пользованию информацией. Также свою сферу действия данный закон распространяет на разработку и эксплуатацию информационных технологий, информационных систем и сетей, образование и гарантия защиты информации, создание информационных ресурсов.

Действие указанного закона не распространяется на общественные отношения, которые связанны с деятельностью средств массовой информации и охраной информации, являющейся объектом интеллектуальной собственности. Законодательством могут быть установлены особенности правового регулирования информационных отношений, связанных со

сведениями, составляющими государственные секреты, с персональными данными, рекламой, защитой детей от информации, причиняющей вред их здоровью и развитию, научно-технической, статистической, правовой, экологической и иной информацией.

Осуществление государственного регулирования и управления в области информации, информатизации и защиты информации в соответствии со статьей 8 Закона Республики Беларусь «Об информации, информатизации и защите информации» [4] «принадлежит Президенту Республики Беларусь, Совету Министров Республики Беларусь, Национальной академии наук Беларуси, Оперативно-аналитическому центру при Президенте Республики Беларусь, Министерству связи и информатизации, иным государственным органам в пределах их компетенций». Каждый из перечисленных государственных органов выполняет свои полномочия в соответствии с законодательством в области информации.

Таким образом, в соответствии с законном Республики Беларусь «Об информации, информатизации и защите информации» [4] по категории доступности информация бывает общедоступная, а также распространение и (или) предоставление информации ограничено. К общедоступной информации относятся все сведения, которые не ограничены в распространении и (или) предоставлении. Например, о деятельности государственных органах, общественных объединений, о чрезвычайных ситуациях, о состоянии преступности, здравоохранения, образования, демографии и другое. К ограниченному распространению и (или) предоставлению информации относятся сведения, составляющие государственные секреты, информацию, составляющую коммерческую, банковскую тайну, информация, содержащаяся в делах об административных правонарушениях, материалах и уголовных делах органов уголовного преследования и суда до завершения производства по делу, информация о частной жизни физического лица и персональные данные.

Далее, необходимо указать, что в Республике Беларусь существуют еще нормативно-правовые акты в области информационного обеспечения. К таким стоит отнести закон Республики Беларусь «О защите персональных данных» [5], закон Республики Беларусь «Об электронном документе и электронной цифровой печати» [6], закон Республики Беларусь «О средствах массовой информации» [7] и другие.

За преступления в сфере информации наступает уголовная ответственность по Уголовному кодексу Республики Беларусь [24]. В данном нормативном акте закреплена глава 31 Преступления против информационной безопасности.

Уголовная ответственность в соответствии с Уголовным кодексом Республики Беларусь наступает с 16 лет. Также выделяются статьи, по которым ответственность наступает с 14 лет. К ним относятся:

«1) убийство (статья 139),

2) причинение смерти по неосторожности (статья 144),

3) умышленное причинение тяжкого телесного повреждения (статья 147),

4) умышленное причинение менее тяжкого телесного повреждения (статья 149),

5) изнасилование (статья 166),

6) насильственные действия сексуального характера (статья 167),

7) похищение человека (статья 182),

8) кражу (статья 205),

9) грабеж (статья 206),

10) разбой (статья 207),

11) вымогательство (статья 208),

12) угон транспортного средства или маломерного водного судна (статья 214),

13) умышленные уничтожение либо повреждение имущества (части вторая и третья статьи 218),

14) захват заложника (статья 291),

15) хищение огнестрельного оружия, боеприпасов или взрывчатых веществ (статья 294),

16) умышленное приведение в негодность транспортного средства или путей сообщения (статья 309),

17) хищение наркотических средств, психотропных веществ, их прекурсоров и аналогов (статья 327),

18) хулиганство (статья 339),

19) заведомо ложное сообщение об опасности (статья 340),

20) осквернение сооружений и порчу имущества (статья 341),

21) побег из исправительного учреждения, исполняющего наказание в виде лишения свободы, арестного дома или из-под стражи (статья 413)» [24].

В соответствии со ст. 48 Уголовного кодекса Республики Беларусь «к лицам, совершившим преступления, применяются следующие основные наказания:

1) общественные работы,

2) штраф,

3) лишение права занимать определенные должности или заниматься определенной деятельностью,

4) исправительные работы,

5) ограничение по военной службе,

6) арест,

7) ограничение свободы,

8) исключен,

9) лишение свободы,

10) пожизненное заключение,

11) смертная казнь (до ее отмены)» [24].

Также может быть применено одно из таких наказаний как лишение воинского или специального звания, или конфискация имущества.

На основании вышеизложенного можно сделать вывод о том, что во всем мире существует большая нормативная база в области информации. Законодательство в сфере информационной безопасности регулярно развивается и увеличивается. В ходе рассмотрения правовой базы различных стран, удалось разобрать наиболее важные нормативно-правовые акты в области информационного обеспечения, которые закрепляют основные цели и задачи, направления деятельности в сфере обеспечения национальной безопасности и другие не маловажные аспекты в сфере информационной безопасности. В каждой стране существуют разные понимания о национальной и информационной безопасности.

Так, можно сделать вывод о том, что в Белоруссии очень схожее законодательство в сфере безопасности с Российской Федерацией.

Глава 2. Современные информационные угрозы, пути и методы их устранения

2.1 Общая характеристика и виды информационных угроз

Приступая к следующей главе квалификационной работы, изучим, какие информационные угрозы существуют в современном обществе.

Так, «несмотря на предпринимаемые дорогостоящие методы, функционирование компьютерных информационных систем выявило наличие слабых мест в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Однако для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным» [9].

Стоит отметить, что понятие «угрозы» рассматривается по-разному. Так, под угрозой в общем виде необходимо понимать потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам. В информационной безопасности угрозой считается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Так, угрозы информационной безопасности проявляются в нарушении конфиденциальности, достоверности, целостности, доступности информации.

Для полного понимая, стоит разобрать каждое нарушение. Так, под нарушением конфиденциальности необходимо понимать разглашение или утечку информации. К нарушению достоверности информации относятся подделка, фальсификация или мошенничество. Нарушение целостности информации представляет собой потерю, искажение или допущение ошибок в данные информации. Под нарушением доступности информации стоит понимать нарушение связи или воспрещение получения информации.

В связи с этим, у правонарушителей существует возможность завладеть информацией, изменить данные или уничтожить ее. Также правонарушитель, после доступа к информации, может ограничить или заблокировать доступ легального пользователя к данным. Правонарушителем может стать любой человек, как сотрудник организации, так и посторонний субъект. Помимо этого, значимость данных может снизиться из-за неумышленных погрешностей сотрудников, а также по естественным природным причинам.

Далее, следующим необходимо разобрать классификацию информационных угроз.

а) по объектам воздействия:

1) для государства являются:

- информационные противодействия,
- информационная война,
- распространение секретной служебной информации,
- кибершпионаж;

2) для организации считаются:

- утечка,
- разглашение,
- несанкционированный доступ;

3) для личности являются:

- онлайновое мошенничество (поддельные письма),
- раскрытие персональных данных, логина, пароля, номера банковской карты,
- киберслежка.

б) по природе возникновения:

1) естественные – угрозы, связанные с возникновением и воздействием физических процессов или стихийными природными явлениями, не зависящие от воли человека;

2) искусственные – угрозы, которые создаются деятельностью человека:

- случайные – ошибки, созданные по вине персонала, сбоя системы, отказ вычислительной и коммуникационной техники,

- умышленные – угрозы созданные действиями людей с прямым умыслом для распространения вирусных программ, неправомерного доступа к информации и т.д.;

в) по размерам нанесенного ущерба:

1) общие – причинение ущерба объекту безопасности в целом,

2) локальные – причинение вреда отдельным частям объекта безопасности,

3) частные – причинение вреда отдельным свойствам элементов объекта безопасности;

г) по степени воздействия на информационную систему выделяют следующие угрозы:

1) пассивные – несанкционированное использование информационных ресурсов, влияние на их функционирование отсутствует. Например, попытка получения информации, посредством прослушивания,

2) активные – нарушение процесса функционирования путем целенаправленного воздействия на программные и информационные ресурсы. Например, изменение сведений в базе данных.

Далее, носителями угроз безопасности информации считаются источники угроз. Источниками могут быть субъекты, т.е. сотрудники организации, совершающие своими действиями умышленные нарушения в сфере информации, а также объективные факторы. Источники угроз информационной безопасности делятся на три вида:

– из-за действий субъекта – приведение к нарушению безопасности информации. Действия квалифицируются как умышленные или случайные преступления;

– из-за технических средств – зависящие от свойств техники;

– из-за стихийных явлений – данные источники не могут быть спрогнозированы. Они носят объективный и абсолютный характер, который распространяется на всех.

Так как в настоящее время очень актуальна тема информационной борьбы между государствами, необходимо изучить понятие информационная война. Российский политолог А.В. Манойло определяет эту дефиницию как «процесс противоборства человеческих общностей, направленный на достижение политических, экономических, военных или иных целей стратегического уровня, путём воздействия на гражданское население, власти и (или) вооружённые силы противостоящей стороны, посредством распространения специально отобранной и подготовленной информации, информационных материалов, и, противодействия таким воздействиям на собственную сторону».

Далее, «определяя термин «информационное противоборство» как форму борьбы сторон, представляющую собой использование специальных (например, политических, экономических, дипломатических, военных) методов, способов и средств для воздействия на информационную среду противостоящей стороны и защиты собственной в интересах достижения поставленной цели. И.Н. Панарин также выделяет наиболее актуальные и часто встречающиеся сферы ведения информационного противоборства:

– Политическая сфера;

– Дипломатическая сфера;

– Финансово-экономическая сфера;

– Инновационная сфера;

– Военная сфера» [20; с. 46].

Также стоит указать понятие геополитическое информационное противоборство, обозначающее как одну из современных форм борьбы между государствами, а также систему мер, проводимых одним государством с целью нарушения информационной безопасности другого государства, при

одновременной защите от аналогичных действий со стороны противостоящего государства.

Таким образом, процессами управления геополитического информационного противоборства являются прогнозирование и планирование; организация и стимулирование; обратная связь; регулирование; контроль исполнения.

Этапами формирования решения в процессе данного противоборства следует выделять:

– оценка ситуации;

– постановка целей;

– установление смысла решения;

– создание вариантов решения.

Для полного понимания стоит указать, чем пользуются представители государства для достижения своих целей в информационном противоборстве. Так, «информационным оружием считаются средства уничтожения, искажения или хищения информационных массивов, добывания из них необходимой информации после преодоления систем защиты, ограничения или воспрещения доступа к ним законных пользователей, дезорганизации работы технических средств, вывода из строя телекоммуникационных сетей, компьютерных систем, всего высокотехнологического обеспечения жизни общества и функционирования государства» [20; с. 72].

Главными отличительными признаками информационного оружия являются:

– масштабность (способность нанести ущерб без ограничения пространства на все сферы жизнедеятельности человека);

– скрытность (достижение цели без специальной подготовки);

– универсальность (допустимость использования, как в гражданских, так и в военных структурах страны для нападения против гражданских и военных объектов страны поражения).

Информационная безопасность в сети «Интернет» возникла с появлением различных видов мошенников, вирусов, которые воздействуют на психическое состояние человека, а также на систему компьютера или телефона. Такие опасности могут причинить вред не только личности, но и обществу или государству в целом.

При размещении какой-либо информации в «Интернете», необходимо понимать, что данная информация становится доступной большому кругу лиц и может причинить вред не только лицу, который размещает данную информацию, но и вред окружающим.

Так, порядок подключения информационных систем и информационно-телекоммуникационных сетей к информационно-телекоммуникационной сети «Интернет» и размещения (публикации) в ней информации через российский государственный сегмент информационно-телекоммуникационной сети «Интернет», утвержден Указом Президента РФ от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации» [32].

Таким образом, можно отметить, что информационные угрозы считаются очень опасным явлением для информационной безопасности. В случае неправильной или не своевременной организации слежения за работой сотрудников организаций или техникой, может произойти утечка, фальсификация, искажение информации. В связи с такими проблемами наносится ущерб каким-либо интересам человека.

Исходя из вышесказанного, в следующем параграфе необходимо изучить деятельность государства в сфере информации для предотвращения образования информационных угроз.

2.2 Деятельность государства по противодействию информационным угрозам

Далее, следует более подробно изучить деятельность государства в противодействии информационным угрозам, какими нормативно-правовыми актами руководствуются при противодействии таким угрозам.

Прежде всего, необходимо сказать, что государственная политика в области обеспечения безопасности должна создаваться за счет развития нормативной базы, кроме того применения мер административного предупреждения.

Итак, приступая к подробному рассмотрению и изучению деятельности государства в информационной сфере, стоит отметить, что одним из основных законодательных актов является Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности». В нем существует глава 2, посвященная полномочиям федеральных органов государственной власти, функции органов государственной власти субъектов Российской Федерации и органов местного самоуправления в области обеспечения безопасности.

Далее, следующим необходимо указать Доктрину информационной безопасности Российской Федерации от 5 декабря 2016 г. № 646. «Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации» [29; п. 4]. «Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности» [29; п. 6].

Еще одним законодательным актом можно указать Указ Президента Российской Федерации от 22.05.2015 г. № 260 «О некоторых вопросах информационной безопасности Российской Федерации». Данный указ создан «в целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации» [32]. Также Указ содержит 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».

«Подключение государственных информационных систем и информационно-телекоммуникационных сетей, предусмотренных перечнем, к сети «Интернет» через российский сегмент осуществляется:

а) по защищенным каналам, создание, содержание и развитие которых обеспечивается ФСО России;

б) за счет и в пределах бюджетных ассигнований, предусмотренных в федеральном бюджете ФСО России» [32].

В соответствии с Федеральным законом от 27.05.1996 № 57-ФЗ «О государственной охране» [38] необходимо указать основные обязанности Федеральной службы безопасности в сфере информационной безопасности:

– организовывают и проводят мероприятия по развитию и совершенствованию связи для нужд органов государственной власти, обеспечению ее надежности, информационной безопасности и оперативности при предоставлении Президенту Российской Федерации, Правительству Российской Федерации, иным государственным органам, а при необходимости органам местного самоуправления и организациям;

– осуществляют разработку, создание и развитие федеральных информационных систем для информационно-технологического и информационно-аналитического обеспечения деятельности Президента

Российской Федерации, Правительства Российской Федерации, иных государственных органов;

– организовывают шифровальные работы;

– взаимодействуют с органами федеральной службы безопасности по противодействию утечке информации;

– и другие.

При изучении деятельности государства в информационной сфере, следует упомянуть слова Президента Российской Федерации. Так, В.В. Путиным было предложено создать в России государственную систему защиты информации, сказав следующие слова: «Нужно укреплять оборону отечественного цифрового пространства – здесь не должно быть слабых мест. Принципиально важно свести на нет риски утечек конфиденциальной информации и персональных данных граждан, в том числе за счет более строгого контроля правил использования служебной техники, коммуникаций, связи» [18].

Для более устойчивой и безопасной работы информационных ресурсов Российской Федерации Президентом Российской Федерации был принят Указ Президента РФ от 01.05.2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации». Так п. 1 говорит о том, что «руководителям федеральных органов исполнительной власти, высших исполнительных органов государственной власти субъектов Российской Федерации, государственных фондов, государственных корпораций (компаний) и иных организаций, созданных на основании федеральных законов, стратегических предприятий, стратегических акционерных обществ и системообразующих организаций российской экономики, юридических лиц, являющихся субъектами критической информационной инфраструктуры Российской Федерации (далее – органы (организации):

а) возложить на заместителя руководителя органа (организации) полномочия по обеспечению информационной безопасности органа

(организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты;

б) создать в органе (организации) структурное подразделение, осуществляющее функции по обеспечению информационной безопасности органа (организации), в том числе по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты, либо возложить данные функции на существующее структурное подразделение;

в) принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обеспечению информационной безопасности органа (организации). При этом могут привлекаться исключительно организации, имеющие лицензии на осуществление деятельности по технической защите конфиденциальной информации;

г) принимать в случае необходимости решения о привлечении организаций к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты. При этом могут привлекаться исключительно организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за исключением случая, предусмотренного подпунктом «б» пункта 5 настоящего Указа;

д) обеспечивать должностным лицам органов федеральной службы безопасности беспрепятственный доступ (в том числе удаленный) к принадлежащим органам (организациям) либо используемым ими информационным ресурсам, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет», в целях осуществления мониторинга, предусмотренного подпунктом «в» пункта

5 настоящего Указа, а также обеспечивать исполнение указаний, данных органами федеральной службы безопасности по результатам такого мониторинга;

е) обеспечивать незамедлительную реализацию организационных и технических мер, решения о необходимости осуществления которых принимаются Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю в пределах их компетенции и направляются на регулярной основе в органы (организации) с учетом меняющихся угроз в информационной сфере» [36].

Далее, пункт 5 указывает «Федеральной службе безопасности Российской Федерации:

а) организовать аккредитацию центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

б) определить переходный период, в течение которого допускается осуществлять мероприятия по обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты в интересах органов (организаций) на основании заключенных с Федеральной службой безопасности Российской Федерации (Национальным координационным центром по компьютерным инцидентам) соглашений о сотрудничестве (взаимодействии) в области обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

в) определить порядок осуществления мониторинга защищенности информационных ресурсов, принадлежащих органам (организациям) либо используемых ими, и осуществлять такой мониторинг» [36].

Данный Указ также содержит информацию о том, что с 1 января 2025 года субъекты критической информационной инфраструктуры Российской Федерации не имеют права пользоваться средствами защиты информации, созданные иностранными государствами, которые также

совершают в отношении Российской Федерации, российских юридических и физических лиц недружественные действия, либо производители которых выступают организации, которые находятся под юрисдикцией таких иностранных государств.

В соответствии с частью 3 статьи 5 Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» «средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения, предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации» [44].

Далее, часть 1 статьи 13 Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» говорит о том, что «государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры проводится в целях проверки соблюдения субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, требований, установленных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Указанный государственный контроль проводится путем осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, плановых или внеплановых проверок» [44].

Так, в целях совершенствования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и в соответствии со статьей 6 Федерального закона от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» был издан Указ Президента Российской Федерации от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».

В данном указе содержатся сведения о возложении обязанностей на Федеральную службу безопасности Российской Федерации в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Кроме того, указ устанавливает задачи государственной системы обнаружения, предупреждения и ликвидации компьютерных атак на информационные ресурсы Российской Федерации:

«а) прогнозирование ситуации в области обеспечения информационной безопасности Российской Федерации;

б) обеспечение взаимодействия владельцев информационных ресурсов Российской Федерации, операторов связи, иных субъектов, осуществляющих лицензируемую деятельность в области защиты информации, при решении задач, касающихся обнаружения, предупреждения и ликвидации последствий компьютерных атак;

в) осуществление контроля степени защищенности информационных ресурсов Российской Федерации от компьютерных атак;

г) установление причин компьютерных инцидентов, связанных с функционированием информационных ресурсов Российской Федерации» [35].

Далее, можно выделить Федеральную службу по надзору в сфере связи, информационных технологий и массовых коммуникаций – Роскомнадзор. Данная служба является федеральным органом исполнительной власти, которая 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 и защите данных, а также функции по организации деятельности радиочастотной службы.

В соответствии с Постановлением Правительства РФ от 16.03.2009 № 228 «О Федеральной службе по надзору в сфере связи, информационных технологий и массовых коммуникаций» «Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций осуществляет следующие полномочия:

а) федеральный государственный контроль (надзор):

1) за соблюдением законодательства Российской Федерации о средствах массовой информации;

2) в области связи:

– за соблюдением требований к построению сетей электросвязи и почтовой связи, требований к проектированию, строительству, реконструкции и эксплуатации сетей и сооружений связи;

– за соблюдением операторами связи и владельцами сетей связи специального назначения требований к пропуску трафика и его маршрутизации;

– за соблюдением пользователями радиочастотного спектра порядка, требований и условий, относящихся к использованию радиоэлектронных средств или высокочастотных устройств, включая надзор с учетом сообщений (данных), полученных в процессе проведения радиочастотной службой радиоконтроля;

– за выполнением правил присоединения сетей электросвязи к сети связи общего пользования, в том числе условий присоединения;

3) за представлением обязательного федерального экземпляра документов в установленной сфере деятельности Службы;

4) за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию (за исключением федерального государственного контроля (надзора) за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, осуществление которого в соответствии с Положением о Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека, утвержденным постановлением Правительства Российской Федерации от 30 июня 2004 г. № 322 «Об утверждении Положения о Федеральной службе по надзору в сфере защиты прав потребителей и благополучия человека», отнесено к полномочиям Федеральной службы по надзору в сфере защиты прав потребителей и благополучия человека, а также федерального государственного контроля (надзора) за соблюдением законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию, осуществление которого в соответствии с Положением о Федеральной службе по надзору в сфере образования и науки, утвержденным постановлением Правительства Российской Федерации от 28 июля 2018 г. № 885 «Об утверждении Положения о Федеральной службе по надзору в сфере образования и науки и признании утратившими силу некоторых актов Правительства Российской Федерации», отнесено к полномочиям Федеральной службы по надзору в сфере образования и науки);

5) за обработкой персональных данных;

6) за соблюдением требований в связи с распространением информации в информационно-телекоммуникационных сетях, в том числе в сети Интернет» [16].

Таким образом, на сегодняшний день государственная политика в сфере обеспечения безопасности базируется на правовом регулировании жизнедеятельности общества.

2.3 Предотвращение преступлений и ответственность граждан за правонарушения в сфере информационной безопасности

В данном параграфе следует рассмотреть, какая ответственность может быть установлена к лицам, совершившим правонарушения в информационной безопасности, а также необходимо указать какие меры необходимо принимать, чтобы не допускать наступления правонарушений в сфере информации.

В современном мире для комфортной жизни человека создаются новые технологические разработки. В связи с этим информация стала одним из распространенных предметов посягательства. Через новейшие информационные технологии появилась сложность в выявлении правонарушений. Тем самым технологические приспособления позволяют правонарушителям избегать ответственности.

Итак, приступая к рассмотрению видов ответственности за правонарушения в информационной безопасности, необходимо обозначить дефиницию фразе «юридическая ответственность». Под юридической ответственностью С.С. Алексеев понимает «применение к правонарушителю предусмотренных санкцией юридической нормы мер государственного принуждения, выражающихся в форме лишений личного, организационного либо имущественного характера» [21]. Н.И. Матузов считает, что «юридическая ответственность – один из видов социальной ответственности индивида. Ее главная особенность в том, что юридическая ответственность связана с нарушением юридических норм, законов, за которыми стоит принудительный аппарат государства. Это – властно-императивная форма ответственности, опирающаяся на силовое начало. Здесь всегда присутствуют

карательный, воспитательный и превентивный моменты. Иными словами, перед нами извечная проблема деяния и воздаяния» [22; с. 215]. Самым близким к теме дипломной работы, было определение юридической ответственности за нарушение информационного законодательства М.А. Федотова, сформулированное как «предусмотренные законодательством меры дисциплинарной, административной, гражданско-правовой, уголовной и информационной ответственности за нарушение законодательства об информации» [10; с. 471]. Несмотря на то, что нет единого мнения при трактовке юридической ответственности в информационной сфере, все-таки необходимо пользоваться статьей 17 Федерального закона «Об информации, информационных технологиях и о защите информации» [41], который основывается на Конституции Российской Федерации, придающая праву на информацию особую важность. Так указанный закон указывает на то, что «нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации» [41].

Таким образом, исходя из вышеуказанного определения, необходимо проанализировать нормы законодательства по отраслям права.

Дисциплинарная ответственность лица наступает после совершения противоправного, виновного деяния в информационной сфере в виде неисполнения или ненадлежащего исполнения субъектом данных правоотношений возложенных на него трудовых обязанностей.

В соответствии со статьей 192 «Трудового кодекса Российской Федерации" от 30.12.2001 № 197-ФЗ [23] дисциплинарная ответственность работника наступает в виде дисциплинарного взыскания. Работодатель вправе применить такие дисциплинарные взыскания как: замечание, выговор, увольнение.

Так, согласно пункту «в» статьи 81 Трудового кодекса Российской Федерации работодатель может расторгнуть трудовой договор с работником

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» [23]. Также необходимо упомянуть пункт 2 статьи 14 Федерального закона от 29.07.2004 № 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» [40].

Кроме этого, за каждый проступок может быть применено только одно дисциплинарное взыскание с учетом тяжести совершенного проступка и обстоятельств, при которых он был совершен. Применение его должно быть не позднее одного месяца со дня обнаружения проступка. Также применение должно быть не позднее шести месяцев со дня совершения проступка, по результатам ревизии, проверки финансово-хозяйственной деятельности или аудиторской проверки не позднее двух лет со дня совершения, а за несоблюдение законодательства о противодействии коррупции не позднее трех лет.

Снятие дисциплинарного взыскания возможно по истечению одного года, если работником не было совершено еще одно правонарушение, которое могло бы привести к дисциплинарному взысканию. Также имеет место быть такой случай, до истечения года, дисциплинарное взыскание отменяется в следующих случаях: по инициативе работодателя; по просьбе работника; по ходатайству непосредственного руководителя.

Далее, дисциплинарная ответственность также может применяться к государственным служащим за совершения информационного

правонарушения. Данный вид ответственности регулируется Федеральным законом от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации» [39]. В соответствии с указанным законом дисциплинарные взыскания могут быть в виде: замечания; выговора; предупреждения о неполном должностном соответствии; увольнение с гражданской службы по основаниям статьи 37. Таким образом, пункт «в» части 3 статьи 37 Федерального закона № 79-ФЗ «О государственной гражданской службе Российской Федерации» содержит следующее «служебный контракт может быть расторгнут в случае однократного грубого нарушения гражданским служащим должностных обязанностей, а именно разглашения сведений, составляющих государственную и иную охраняемую федеральным законом тайну, и служебной информации, ставших известными гражданскому служащему в связи с исполнением им должностных обязанностей» [39].

На основании объяснения в письменно форме гражданского служащего или отказа дачи показаний, составляется соответствующий акт. В соответствии, с которым к гражданскому служащему может применяться только одно дисциплинарное взыскание. Для того чтобы применить дисциплинарное взыскание необходимо провести проверку и установить следующее:

- тяжесть совершенного проступка;
- степень вины гражданского служащего;
- обстоятельства совершения правонарушения;
- предшествующие результаты исполнения гражданским служащим своих должностных обязанностей.

В ходе проверки должны быть учтены все факты и обстоятельства совершенного правонарушения для определения применения или неприменения дисциплинарного взыскания. В случае применения, по результатам данной проверки составляется соответствующий акт, копия

которого должна быть вручена гражданскому служащему под расписку не позднее пяти дней со дня издания данного акта.

При анализе Трудового кодекса РФ и Федерального закона № 79-ФЗ «О государственной гражданской службе Российской Федерации» установлено, что сроки применения и снятия дисциплинарного взыскания совпадают. Дисциплинарное взыскание можно обжаловать гражданским служащим в письменной форме в комиссию государственного органа или в суд.

Далее, гражданско-правовая ответственность представляет собой восстановление нарушенных прав, заглаживание нанесенного ущерба в результате неправомерных действий и возмещается в натуре или в виде компенсации.

Необходимо указать мнение П.У. Кузнецова. Он рассматривает гражданско-правовое информационное правонарушение (деликт) как «посягающее на нематериальные блага информационной природы общественно-вредное, противоправное, виновное деяние деликтоспособного лица» [13; с. 287- 289].

«Правонарушитель может осуществить восстановление прежнего состояния, возмещение нанесенного ущерба добровольно, на основе соглашения с потерпевшей стороной. Если возникающие в результате правонарушения обязанности не осуществляются добровольно, потерпевший использует мер правовой защиты, в результате чего правонарушитель принуждается государством в лице его компетентных органов и должностных лиц в специально предусмотренных законом процедурах к соблюдению своих невыполненных обязанностей» [14; с. 140].

За правонарушения в информационной сфере гражданско-правовая ответственность делится на:

– договорную,

– внедоговорную (деликтную).

Таким образом, договорная ответственность наступает за нарушения условий договора, в котором содержатся санкции. При таком виде

ответственности деяние лица будет регулироваться в соответствии с условиями договора и закона. Так, статья 495 ГК РФ содержит информацию об обязанностях продавца представлять необходимую и достоверную информацию о товаре для покупателя; статья 505 ГК РФ говорит о том, что «в случае неисполнения продавцом обязательства по договору розничной купли-продажи возмещение убытков и уплата неустойки не освобождают продавца от исполнения обязательства в натуре» [1]; в соответствии со статьей 726 ГК РФ подрядчик вместе с результатом работы передает заказчику информацию, касающуюся использования договора подряда; статья 732 ГК РФ говорит о том, что подрядчик обязан предоставить необходимую и достоверную информацию о предлагаемой работе до заключения договора и другие статьи.

Внедоговорная ответственность возникает при причинении вреда личности или его имуществу, не связанного договорными обязательствами. В данном случае деяние регулируется законом, а не договором. Чтобы привлечь лицо к внедоговорной ответственности, нужно доказать факт понесенного ущерба. Для полного понимания указанного вида ответственности стоит привести примеры. Так, статья 1095 ГК РФ говорит, что вред причиненный лицу из-за недостоверной или недостаточной информации о товаре, подлежит возмещению продавцом или изготовителем товара, а также лицом, выполнившим работу или оказавшим услугу, независимо от их вины и от того, состоял потерпевший с ними в договорных отношениях или нет; статья 1100 ГК РФ свидетельствует о том, что возможна компенсация морального вреда за вред, причиненный путем распространения сведений, порочащих часть, достоинство и деловую репутацию; статья 1101 ГК РФ содержит информацию о способе и размере компенсации морального вреда; статья 1301 ГК РФ предусматривает ответственность за нарушение исключительного права на произведение; статья 1253.1 ГК РФ сообщает, что информационный посредник несет ответственность за нарушение интеллектуальных прав в информационно-телекоммуникационной сети на общих основаниях, за исключением случаев, предусмотренных в части 2 данной статьи:

– 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 результата интеллектуальной деятельности или средства индивидуализации лицом, инициировавшим передачу материала, содержащего соответствующие результат интеллектуальной деятельности или средство индивидуализации, является неправомерным.

Следующим видом необходимо указать административную ответственность за информационные правонарушения. Такая ответственность представляет собой противоправное, виновное деяние, выраженное в виде действия или бездействия физического или юридического лица, за которое наступает ответственность в соответствии с Кодексом Российской Федерации об административных правонарушениях [11]. Указанный нормативно-правовой акт является основным в регулировании административных правоотношений.

Также, Кодекс Российской Федерации об административных правонарушениях содержит отдельную главу 13 «Административные правонарушения в области связи и информации». В данной главе содержатся следующие статьи, касающиеся защиты информации: статья 13.11 Нарушение законодательства Российской Федерации в области персональных данных; статья 13.12 Нарушение правил защиты информации; статья 13.13 Незаконная деятельность в области защиты информации; статья 13.14 Разглашение информации с ограниченным доступом; статья 13.15 Злоупотребление свободой массовой информации и другие.

Стоит отметить, что существуют другие статьи, за которые может применяться административное наказание за правонарушение в информационной сфере. К таким статьям могут относиться:

– статья 5.14 КоАП РФ Умышленное уничтожение или повреждение агитационного материала либо информационного материала, относящегося к выборам, референдуму, общероссийскому голосованию;

– статья 5.39 КоАП РФ Отказ в предоставлении информации;

– статья 5.61 КоАП РФ Оскорбление;

– статья 6.17 КоАП РФ Нарушение законодательства Российской Федерации о защите детей от информации, причиняющей вред их здоровью и (или) развитию;

– статья 8.32.1 КоАП РФ Ненаправление, несвоевременное направление, направление недостоверной информации в федеральный орган исполнительной власти, уполномоченный на ведение реестра недобросовестных арендаторов лесных участков и покупателей лесных насаждений;

– статья 17.6 КоАП РФ Непредставление информации для составления списков присяжных заседателей;

– статья 19.7.2 КоАП РФ Непредставление информации и документов или представление заведомо недостоверных информации и документов в орган, уполномоченный на осуществление контроля в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд, в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере государственного оборонного заказа, орган внутреннего государственного (муниципального) финансового контроля;

– и другие.

В соответствии со статьей 3.2 Кодекса Российской Федерации об административных правонарушениях за правонарушения в информационной сфере могут применяться такие административные наказания:

«– административный штраф;

– дисквалификация;

– административное приостановление деятельности;

– конфискация орудия совершения или предмета административного правонарушения;

– административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства;

– и другие» [11].

В качестве примера можно привести статью 13.11 КоАП РФ, которая за нарушение законодательства РФ в области персональных данных, а именно обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных «влечет наложение административного штрафа на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от шестидесяти тысяч до ста тысяч рублей» [11].

Уголовная ответственность считается значимым элементом в системе мер правового обеспечения информационной безопасности, защиты прав граждан, общества и государства в информационной сфере. Информационное преступление – это виновное общественно опасное деяние, которое запрещено Уголовным кодексом Российской Федерации под угрозой наказания.

Далее, необходимо указать основные элементы состава преступления:

– субъект,

– объект,

– субъективная сторона,

– объективная сторона.

Таким образом, при привлечении лица к уголовной ответственности, должны присутствовать все указанные элементы состава преступления. При отсутствии хотя бы одного из них, влечет отказ в возбуждении уголовного дела.

Уголовный кодекс РФ содержит отдельную главу 28 «преступления в сфере компьютерной информации» [25], которая включает в себя такие статьи как:

– неправомерный доступ к компьютерной информации;

– создание, использование и распространение вредоносных компьютерных программ;

– нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;

– неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации;

– нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования.

Также стоит отметить, что это не исчерпывающий список статей уголовного кодекса, по которым можно привлечь лицо к уголовной ответственности за правонарушения в информационной сфере. В качестве примера необходимо привести несколько таких статей за отдельные преступления против чести и достоинства личности и нарушающие права и свободы человека и гражданина, установленного порядка управления и безопасности государства:

– так пункт «д» части 2 статьи 110 УК РФ конкретно указывает на то, что доведение лица до самоубийства или до покушения на самоубийство путем угроз, жестокого обращения или систематического унижения человеческого достоинства потерпевшего может быть «в публичном выступлении, публично демонстрирующемся произведении, средствах массовой информации или информационно-телекоммуникационных сетях (включая сеть «Интернет»)»;

– часть 2 статьи 128.1 УК РФ указывает на то, что «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»;

– статья 140 УК РФ содержит информацию о том, что «неправомерный отказ должностного лица в предоставлении собранных в установленном порядке документов и материалов, непосредственно затрагивающих права и свободы гражданина, либо предоставление гражданину неполной или заведомо ложной информации»;

– статья 159.6 УК РФ отмечает, что «мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей»;

– статья 276 УК РФ устанавливает, что «передача, собирание, похищение или хранение в целях передачи иностранному государству, международной либо иностранной организации или их представителям сведений, составляющих государственную тайну, а также передача или собирание по заданию иностранной разведки или лица, действующего в ее интересах, иных сведений для использования их против безопасности Российской Федерации либо передача, собирание, похищение или хранение в целях передачи противнику сведений, которые могут быть использованы против Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов Российской Федерации, совершенные в условиях вооруженного конфликта, военных действий или иных действий с применением вооружения и военной техники с участием Российской Федерации, то есть шпионаж, если эти деяния совершены иностранным гражданином или лицом без гражданства»;

– и иные статьи УК РФ.

В соответствии со статьей 44 УК РФ можно выделить виды наказания за совершения преступлений в области информации:

«– штраф;

– исправительные работы;

– принудительные работы;

– ограничение свободы;

– лишение свободы на определенный срок;

– лишение права занимать определенные должности или заниматься определенной деятельностью;

– и другие виды» [25].

Таким образом, отсылки на информацию содержатся во всех отраслях права. Вышесказанное подтверждает, что информационные права граждан, закрепленные в Конституции Российской Федерации, охраняются нормами права.

Необходимо указать, что в современном мире существует множество правонарушений связанных с информацией и информационными технологиями. Данные проблемы возникли с появлением сети Интернет.

В качестве примера преступности в Интернете можно привести следующее:

– открытый доступ к ресурсам сети Интернет;

– низкий уровень охраны программного обеспечения;

– несовершенство парольных систем;

– информационная «безграмотность» пользователей;

– и другое.

Для своевременного предотвращения совершения правонарушений, законодателю необходимо постоянно контролировать противоправные действия в сфере информации. Также, важно проводить массовые мероприятия, беседы на темы «Безопасность в сети Интернет» с различными слоями населения, которые больше всего подвергаются опасности. К таким можно отнести пенсионеров, подростков и других граждан. Немаловажным

является рассылка актуальных правил безопасности пользователям сети Интернет.

Для того чтобы защитить себя и свои личные данные необходимо пользоваться такими способами:

– установка антивирусных программ на компьютеры или телефоны;

– создание сложных паролей для входа в личный кабинет;

– своевременное обновление программного обеспечения;

– не переходить на сомнительные сайты;

– создать пароль для разблокировки экрана на компьютере или телефоне.

Исходя из вышесказанного, в целях своевременного реагирования на возможные угрозы, необходимо постоянно анализировать информационные правонарушения. Для охраны прав, свобод и законных интересов граждан законодателем создаются меры, которые ограничивают доступ к определенной информации.

Заключение

Подводя итоги вышесказанного, стоит указать, что основной целью обеспечения национальной безопасности Российской Федерации является создание и поддержание необходимого уровня защищенности жизненно важных интересов всех объектов безопасности, который бы создавал благоприятные условия для развития личности, общества и государства. И исключал опасность ослабления роли и значения Российской Федерации, как субъекта международного права, подрыва способности государства реализовывать национальные интересы Российской Федерации.

Также следует еще раз упомянуть, что в первой главе данной работы были рассмотрены законодательные акты, на которых базируется национальная безопасность. Исходя из этого, было выделено основное понятие национальной безопасности, принципы обеспечения безопасности, а также входящие в нее виды безопасности. Одним из видов является информационная безопасность, который 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» [29].

Также первая глава содержит сведения о правовом регулировании информационной безопасности в различных странах. В ходе написания дипломной работы были изучены и проанализированы законодательные основные законодательные акты Соединенных Штатов Америки, Китая и Республики Беларусь, которые содержат к национальную и информационную безопасность.

Вторая глава основывается на рассмотрении понятия информационных угроз, а также ее общей характеристики и различных классификаций. Таким образом, в соответствии с Доктриной информационной безопасности

Российской Федерации, расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы [29]. Также данная глава содержит понятия и основные сведения об информационной войне, информационном противоборстве, геополитическом информационном противоборстве.

Кроме этого, во второй главе рассмотрена деятельность государства по противодействию информационным угрозам. Таким образом, следует указать, в каких законодательных актах содержатся основные полномочии и функции федеральных органов исполнительной власти:

– Указ Президента РФ от 22.05.2015. № 260 «О некоторых вопросах информационной безопасности Российской Федерации»;

– Указ Президента РФ от 5.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;

– Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

– Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»;

– Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 09.03.2021) «Об информации, информационных технологиях и о защите информации»;

– Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности»;

– Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

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.

Выше было рассмотрена дефиниция юридической ответственности. Так, С.С. Алексеев понимает «применение к правонарушителю предусмотренных санкцией юридической нормы мер государственного принуждения, выражающихся в форме лишений личного, организационного либо имущественного характера» [21]. В соответствии со статьей 17 Федерального закона № 149-ФЗ «Об информации, информационных технологиях и о защите информации» «нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации» [41]. Далее были рассмотрены и проанализированы нормативно-правовые акты, которые устанавливают ответственность за противоправные деяния в сфере информации.

В результате написания выпускной квалификационной работы, были выделены множество проблем, связанных с информационной безопасностью, с которыми сталкивается население нашей страны ежедневно. Таким образом, информация и все что связано с ней, касается всех сфер жизни общества. В связи с этим, в Российской Федерации существует значительная правовая база, которая регулирует общественные отношения в информационной сфере.

В связи с появлением новейших технологий, а также методов обработки, передачи и хранения данных, появляется более возможный шанс совершить то или иное правонарушение. Это объясняется тем, что с развитием информационных технологий способы совершения правонарушений улучшаются в большую сторону.

Цель выпускной квалификационной работы достигнута – был изучен вопрос правовой политики в сфере информационной безопасности. Таким образом, в рамках исследования были подробно изучена правовая база национальной и информационной безопасности в Российской Федерации, а

также в зарубежных странах. Также подробно разобрана ответственность за правонарушения в информационной сфере.

Список литературы и используемых источников

1. «Гражданский кодекс Российской Федерации (часть вторая)» от 26.01.1996 № 14-ФЗ (ред. от 01.07.2021, с изм. от 08.07.2021) (с изм. и доп., вступ. в силу с 01.01.2022);

2. Даль В.И. Толковый словарь живого великорусского языка: избр. ст. / В.И. Даль; совмещ. ред. изд. В.И. Даля и И.А. Бодуэна де Куртенэ; [науч. ред. Л.В. Беловинский]. - М.: ОЛМА Медиа Групп, 2009 - С. 573;

3. Закона Китайской Народной Республики «О безопасности данных» от 10.06.2021 г. (вступ. в силу 01.09.2021 г.);

4. Закон Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации»;

5. Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»;

6. Закон Республики Беларусь от 28.12.2009 № 113-З «Об электронном документе и электронной цифровой печати»;

7. Закон Республики Беларусь от 17.07.2008 № 427-З «О средствах массовой информации»;

8. 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);

9. Информационная безопасность: Учебное пособие. Авторы: Ясенев В.Н., Дорожкин А.В., Сочков А.Л., Ясенев О.В. Под общей редакцией проф. Ясенева В.Н. – Нижний Новгород: Нижегородский госуниверситет им.Н.И. Лобачевского, 2017 – 198 с.;

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

11. «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 № 195-ФЗ (ред. от 29.12.2022) (с изм. и доп., вступ. в силу с 11.01.2023);

12. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства РФ, 01.07.2020, № 31, ст. 4398;

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

14. Общая теория юридической ответственности: Монография / Н.В. Витрук. – М.: Изд-во РАП, 2008 – 304 с.;

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

16. Постановление Правительства РФ от 16.03.2009 N 228 (ред. от 30.03.2023) "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");

17. Постановление Совета Безопасности Республики Беларусь от 18.03.2019 № 1 «О Концепции информационной безопасности Республики Беларусь»;

18. Сайт Ведомости: https://www.vedomosti.ru/technology/articles/2022/05/20/922998-gosudarstvennuyu-sistemu-zaschiti ;

19. С.Г. Трясогузова Толковый словарь русского языка для школьников/ [авт.-сост. С.Г. Трясогузова]. – М.: РИПОЛ классик, 2009. – 704 с. – (Школьные словари);

20. Сулейманова Ш.С., Назарова Е.А., Информационные войны: история и современность: Учебное пособие. – М.: Международный издательский центр «Этносоциум», 2017 124 с.;

21. Теория государства и права: Учеб. для студентов вузов, обучающихся по специальности "Юриспруденция" / [Алексеев С.С.,

Архипов С.И., Игнатенко Г.В. и др.; Авт. предисл. С.С. Алексеев; Отв. ред.: В.М. Корельский, В.Д. Перевалов]. - 2-е изд., изм. и доп. - М.: НОРМА: НОРМА-ИНФРА-М, 2000. - XX, 595 с.; 22 см.; ISBN 5-89123-388-6 (НОРМА);

22. Теория государства и права: учебник для студентов высших учебных заведений, обучающихся по направлению и специальности «Юриспруденция» / Н.И. Матузов, А.В. Малько; Саратовский филиал ин-та государства и права Российской акад. наук. - Изд. 2-е, перераб. и доп. - Москва : Юристъ, 2007. - 540, [1] с. : ил.; 22 см. - (Institutiones).; ISBN 978-5-7975-0778-9 (В пер.);

23. «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);

24. «Уголовный кодекс Республики Беларусь» от 09.07.1999г. № 275-З (с изменениями и дополнениями по состоянию на 09.03.2023 г.);

25. «Уголовный кодекс Российской Федерации» от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022);

26. Указ Президента Республики Беларусь от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь»;

27. Указ Президента Республики Беларусь от 06.04.1999 № 195 «О некоторых вопросах информатизации» (утратил силу);

28. Указ Президента РФ от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации»;

29. Указ Президента РФ от 5.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Собрание законодательства Российской Федерации от 12.12.2016 г. № 50 ст. 7074;

30. Указ Президента РФ от 17.12.1997 № 1300 (ред. от 10.01.2000) «Об утверждении Концепции национальной безопасности Российской Федерации» (утратил силу);

31. Указ Президента РФ от 12.05.2009 № 537 (ред. от 01.07.2014) «О Стратегии национальной безопасности Российской Федерации до 2020 года» (утратил силу);

32. 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;

33. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» (утратил силу);

34. Указ Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы»;

35. Указ Президента РФ от 22.12.2017 № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»;

36. Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

37. 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);

38. Федеральный закон от 27.05.1996 № 57-ФЗ (ред. от 04.08.2022) «О государственной охране»;

39. Федеральный закон от 27.07.2004 № 79-ФЗ (ред. от 28.12.2022) «О государственной гражданской службе Российской Федерации»;

40. Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 14.07.2022) «О коммерческой тайне»;

41. 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;

42. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 14.07.2022) «О персональных данных»;

43. Федеральный закон от 28.12.2010 № 390-ФЗ (ред. от 09.11.2020) «О безопасности»// Собрание законодательства Российской Федерации от 3 января 2011 г. № 1;

44. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».