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

Институт права
(наименование института полностью)

Кафедра «Конституционное и административное право»
(наименование)

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

Государственно-правовая
(направленность (профиль)/специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (ДИПЛОМНАЯ РАБОТА)

на тему Информационные правонарушения как угроза национальной безопасности

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

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

Тольятти 2022

Аннотация

Актуальность темы исследования. Современный этап развития характеризуется как век информационных технологий. Интернет охватывает все направления жизни. Распространение информационно-телекоммуникационных и цифровых технологий значительно упростили и ускорили процессы обмена, поиска и сбора информации, дало важность осуществлять платежи и переводы денежных средств в разные точки мира. Такие тенденции обусловили появления новых видов правонарушений – киберпреступности. В настоящее время проблемы информационных правонарушений приобрели глобальный характер, представляющие угрозы национальной безопасности. Необходимо отметить, что современная система противодействия киберпреступности и правонарушениям в информационной среде является молодой и нуждается в формировании действующих механизмов предупреждения и расследования таких преступлений. Стремительное проникновение информационных продуктов и цифровых технологий требует развития и совершенствование норм законодательного регулирования деятельности в информационной среде, обеспечивающей национальную безопасность, что подтверждает актуальность темы исследования.

Объектом исследования являются общественные отношения в сфере информационных правонарушений как угрозы национальной безопасности Российской Федерации.

Предметом исследования является совокупность правовых норм, регламентирующих правонарушения в информационной среде.

Целью выпускной квалификационной работы является исследование современного нормативно-правового регулирования информационных правонарушений для обеспечения национальной безопасности Российской Федерации.

Оглавление

Введение

Актуальность темы исследования. Современный этап развития характеризуется как век информационных технологий. Интернет охватывает все направления жизни. Распространение информационно-телекоммуникационных и цифровых технологий значительно упростили и ускорили процессы обмена, поиска и сбора информации, дало важность осуществлять платежи и переводы денежных средств в разные точки мира. Такие тенденции обусловили появления новых видов правонарушений – киберпреступности. В настоящее время проблемы информационных правонарушений приобрели глобальный характер, представляющие угрозы национальной безопасности. Необходимо отметить, что современная система противодействия киберпреступности и правонарушениям в информационной среде является молодой и нуждается в формировании действующих механизмов предупреждения и расследования таких преступлений. Стремительное проникновение информационных продуктов и цифровых технологий требует развития и совершенствование норм законодательного регулирования деятельности в информационной среде, обеспечивающей национальную безопасность, что подтверждает актуальность темы исследования.

Степень научной разработанности темы исследования. Проблемы информационных правонарушений и из влияние на национальную безопасность рассматривались в трудах ученых, таких как: М.К. Ажибеков, А.А. Аношкина, А.А. Бартош, А.В. Бойкова, К.В. Бородин, С.Б. Вепрев, С.А. Нестерович, А.А. Гребеньков, О.В. Григорьев, С.Н. Гриняев, П.Л. Мареев, Д.А. Медведев, Н.Т. Джафарова, И.Р. Дубровин, Е.Р. Дубровин, З.Т. Золоева, С.Т. Золоев, В.О. Ким, А.А. Комаров, В.А. Курбенков, А.В. Ушкань, Ю.С. Лапин, В.А. Лохбаум, К.Г. Мамцов, Н.Р. Ачилов, М.А. Мельничук, В.К. Новиков, С.В. Голубчиков, М.Ю. Троицкая, М.В. Сербин, Т.А. Овсянникова, Г.И. Пещеров, А.Н. Пименов,

А.Н. Прокопенко, И.Н. Старостенко, Е.А. Романова, О.К. Головкин, Д.Д. Савенкова, А.Г. Суханов, Е.В. Талагаева и других ученых.

Несмотря на наличие большинства научных исследований в данной области, многие проблемы остаются не проработанными, требующими дополнительных подходов и поиска направлений совершенствования правового регулирования информационных правонарушений для защиты национальной безопасности Российской Федерации.

Объектом исследования являются общественные отношения в сфере информационных правонарушений как угрозы национальной безопасности Российской Федерации.

Предметом исследования является совокупность правовых норм, регламентирующих правонарушения в информационной среде.

Цель и задачи исследования. Целью выпускной квалификационной работы является исследование современного нормативно-правового регулирования информационных правонарушений для обеспечения национальной безопасности Российской Федерации.

Для достижения указанной цели были поставлены следующие основные задачи:

- рассмотрение правовых основ национальной безопасности;
- изучение понятия информационных правонарушений;
- исследование влияния информационных правонарушений на национальную безопасность;
- раскрытие понятия и видов информационных преступлений;
- изучение административных и гражданско-правовых информационных правонарушений;
- исследование дисциплинарных информационных правонарушений;
- изучение системы законодательства об ответственности за информационные правонарушения;

– проведение анализа проблем института ответственности за информационные правонарушения, угрожающие национальной безопасности и пути их решения.

Методологическая основа исследования. В процессе проведения исследования использовались общенаучные методы познания: синтез, анализ, диалектика, дедукция, индукция, метод сравнительно-правового исследования, нормативный метод.

Теоретическая основа исследования состоит из учебной юридической литературы, раскрывающий основы информационных правонарушений как угрозы национальной безопасности Российской Федерации.

Нормативная база исследования определена системой действующих нормативно-правовых актов, в области информационных правонарушений как угрозы национальной безопасности Российской Федерации.

Структура работы. Работа состоит из введения, трех глав, включающих восемь параграфов, заключения, списка используемой литературы и используемых источников.

Глава 1 Теоретические аспекты информационных правонарушений как угрозы национальной безопасности

1.1 Правовые основы национальной безопасности

В современных условиях в основу правового обеспечения национальной безопасности входит система норм отечественного и международного права, которая регламентирует общественные отношения в данном направлении.

«Обеспечение национальной безопасности РФ выступает в качестве предмета разных отраслей национального права, конституционного, административного, уголовного, процессуального права.

Безусловно, основу правового регулирования национальной безопасности РФ составляют нормы конституционного права» [14].

По мнению Н.Р. Усмонова, «обеспечение национальной безопасности — система политических, экономических, социальных, здравоохранительных, военных и правовых мероприятий, направленных на обеспечение нормальной жизнедеятельности нации, устранение возможных угроз.

Главной целью обеспечения национальной безопасности выступает поддержание состояния защищенности всех важных интересов личности, общества, государства, которые обеспечивают благоприятные условия для жизни. Обеспечение национальной безопасности выступает в качестве одной из главных задач любого государства мира. Большинство стран мира воспринимая безопасность как одну из главных задач принимают необходимые нормативно правовые акты, которые обеспечивают правовое поле для национальной безопасности. Безопасность достигается путем осуществления единой государственной политики во всех сферах жизнедеятельности личности, да и всего общества в целом, и в политической, и в социальной, и в экономической и других жизненно важных сферах.

Для обеспечения безопасности государство не только принимает нормативно правовые акты, но и регулирует отношения в сфере безопасности,

разграничивают основные направления деятельности органов государственной власти и управления в данной области, формируют или преобразуют органы обеспечения безопасности и механизм контроля и надзора за их деятельностью. Но конечно же самое главное направление деятельности в обеспечении национальной безопасности является правовое регулирование в указанной области» [34, с. 189].

Правовую основу обеспечения безопасности составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, Федеральный закон «О безопасности», другие федеральные законы и иные нормативные правовые акты Российской Федерации, законы и иные нормативные правовые акты субъектов Российской Федерации, органов местного самоуправления, принятые в пределах их компетенции в области безопасности.

Первостепенное место в правовом обеспечении национальной безопасности отводится Конституции РФ. Данный документ имеет высшую юридическую силу.

В Конституции РФ применяется понятие «безопасность», которая в общем смысле рассматривается как национальная безопасность, так она заложена в основу других видов безопасности, охватывающих конституционно-правовые отношения. В этой связи большинство положений, раскрываемых в Конституции РФ можно отнести как к основе национальной безопасности. Именно они затрагивают ключевые общественные отношения, защита которых входит в задачи обеспечения национальной безопасности [3], [9], [11].

Международное сотрудничество Российской Федерации в области обеспечения безопасности осуществляется на основе общепризнанных принципов и норм международного права и международных договоров Российской Федерации [29].

Основными целями международного сотрудничества в области обеспечения безопасности являются [33]:

- охрана суверенитета Российской Федерации, ее независимости и государственной целостности, предотвращение внутренних и внешних угроз, пресечение действий, направленных на отчуждение части территории Российской Федерации, а также призывов к таким действиям;
- защита прав и законных интересов российских граждан за рубежом;
- укрепление отношений со стратегическими партнерами Российской Федерации;
- участие в деятельности международных организаций, занимающихся проблемами обеспечения безопасности;
- развитие двусторонних и многосторонних отношений в целях выполнения задач обеспечения безопасности;
- содействие урегулированию конфликтов, включая участие в миротворческой деятельности.

Решения межгосударственных органов, принятые на основании положений международных договоров Российской Федерации в их истолковании, противоречащем Конституции Российской Федерации, не подлежат исполнению в Российской Федерации.

К важному документу в правовых основах по обеспечению национальной безопасности относится Стратегия о национальной безопасности РФ. Вышеуказанный документ определяет основные принципы и содержание деятельности по обеспечению безопасности государства, общественной безопасности, экологической безопасности, безопасности личности, иных видов безопасности, предусмотренных законодательством РФ, полномочия и функции федеральных органов государственной власти, органов государственной власти субъектов РФ, органов местного самоуправления в области безопасности, а также статус Совета Безопасности Российской Федерации.

Систему правового обеспечения национальной безопасности входит Стратегия национальной безопасности РФ, утвержденная Указом Президента РФ от 02.07.2021 г. № 400 [33].

Стратегию можно представить базовым документом по стратегическому планированию, который определяет национальные интересы и стратегические национальные приоритеты РФ. В данном документе представлены цели и задачи государственной политики по обеспечению национальной безопасности и устойчивого развития РФ на долгосрочную перспективу.

Стратегия отражает неразрывную взаимосвязь и взаимозависимость национальной безопасности РФ и социально-экономического развития страны.

Согласно Стратегии национальной безопасности РФ «национальная безопасность Российской Федерации - состояние защищенности национальных интересов РФ 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 РФ, ее независимости и государственной целостности, социально-экономическое развитие страны. Национальные интересы РФ - объективно значимые потребности личности, общества и государства в безопасности и устойчивом развитии» [33].

«К стратегическим национальным приоритетам России относятся важнейшие направления обеспечения национальной безопасности и устойчивого развития страны.

Обеспечение национальной безопасности связано с реализацией органами публичной власти совместно с институтами гражданского общества и организациями политико-правовых, военных, социальных, экономических, информационно-организационных и иных мер» [33].

Координацию деятельности по обеспечению безопасности осуществляют Президент РФ и формируемый и возглавляемый им Совет Безопасности, а также в пределах своей компетенции Правительство РФ,

федеральные органы государственной власти, органы государственной власти субъектов РФ, органы местного самоуправления.

1.2 Понятие информационных правонарушений

Правонарушение представляет собой юридический факт, действия, противоречащие нормам права. При этом, информационным правонарушениям характерны общие и специальные признаки, имеющие существенное значение для данного класса правонарушений.

Общие признаки информационного правонарушения представлены на рисунке 1.

«На базе вышеуказанных общих и специальных признаков сформулировано определение информационных правонарушений как общественно опасных, противоправных, виновных деяний дееспособного лица, совершившего в информационной сфере или с использованием информационных средств и технологий работы с информацией независимо от ее формы в условиях информационной среды» [13].

Рисунок 1 – Общие признаки информационного правонарушения

Специальные признаки информационного правонарушения представлены на рисунке 2.

Рисунок 2 – Специальные признаки информационного правонарушения

Правонарушения относятся к юридическим фактам. Неправомерные действия в информационной области могут нести отрицательные последствия для граждан, общества и государства в целом.

М.Е. Трофимова отмечает, что «наиболее распространенными правонарушениями в информационной сфере являются проступки, имеющие следующие особенности:

– они отличаются незначительной опасностью (вред для общества);
– совершаются в различных областях информационной деятельности;
– направлены на различные объекты и имеют разные юридические последствия» [31, с. 122].

Проступки подразделяются на дисциплинарные, административные и деликты.

«Дисциплинарные проступки в информационной сфере характеризуются правонарушениями, совершаемыми субъектами информационного права в связи с неисполнением или ненадлежащим исполнением возложенных на них трудовых обязанностей, влекущих за собой применение дисциплинарного или общественного воздействия, предусмотренного ТК РФ» [22].

«К совершившему дисциплинарный проступок должностному лицу или гражданину применяются различные меры наказания: замечание, выговор, увольнение по соответствующим основаниям, а также иные взыскания в соответствии с уставами и положениями о дисциплине (ч. 5 ст. 189, ст. 192 ТК РФ) для отдельных категорий работников» [28, с. 93].

«Административным проступком в информационной сфере называется противоправное, виновное (умышленное или неосторожное) действие либо бездействие физического или юридического лица, посягающее на информационные права и свободы человека и гражданина, здоровье, общественную нравственность, установленный порядок осуществления государственной власти, общественный порядок и общественную безопасность, собственность, законные интересы других лиц, за которое законодательством предусмотрена административная ответственность» [24, с. 163].

В соответствии со ст. 3.2. КоАП РФ это:

- предупреждение;
- административный штраф;
- возмездное изъятие орудия совершения или предмета административного правонарушения;
- конфискация орудия совершения или предмета административного правонарушения; лишение специального права, предоставленного физическому лицу;
- административный арест;

– административное выдворение за пределы страны иностранного гражданина или лица без гражданства;
– дисквалификация;
– административное приостановление деятельности.

Действующий КоАП РФ включает информационные правонарушения в разные главы (например, гл. 5—8, 13—17, 19), однако в нем есть и специальная гл. 13 "Административные правонарушения в области связи и информации" (ст. 13.1— 13.26). Согласно ст. 2.1 КоАП РФ административная ответственность, в частности за нарушение информационного законодательства, может быть установлена как федеральным законодательством, так и законодательством субъектов РФ.

«Деликтами называются правонарушения, выражающиеся в нарушении норм, регулирующих информационно-имущественные отношения организаций, физических лиц, предпринимательских структур. Их называют также гражданскими правонарушениями. В суде могут быть предъявлены претензии к гражданам, организациям, ведомствам и др., и они обязаны возместить причиненный ущерб или убытки либо восстановить нарушенные информационные права» [4, с. 1159].

К более серьезным правонарушениям в информационной области относятся преступления [7]. К людям, которые совершили такие преступления суд назначает меры уголовного наказания, например, арест, лишение свободы, запрет на занятие определенных должностей и т.п.

Состав правонарушения в информационной сфере - это совокупность признаков, характерных для таких правонарушений, предусмотренных нормами информационного права [5].

«Все признаки, характеризующие состав правонарушения в исследуемой области, существуют не отдельно, а в связи друг с другом. Они группируются в нечто целое, содержащее в себе четыре основных элемента: субъект правонарушения в данной области и субъективная сторона, объект правонарушения в информационной среде и объективная сторона» [17, с. 82].

«Субъект правонарушения в информационной сфере – это конкретное лицо, которое совершило противоправное действие и способное за это нести ответственность в установленном законом порядке.

Объективная сторона правонарушения в информационной сфере проявляется во внешней стороне этого негативного явления, т.е. выражается прежде всего в том, как субъект воспринял данное проявление, что видел, слышал и т.д.» [29, с. 67].

Виды информационных правонарушений по объекту посягательств представлены на рисунке 3.

Рисунок 3 – Виды информационных правонарушений по объекту посягательств

Таким образом, проблематика информационных правонарушений остается актуальной в настоящее время, особенно в условиях цифровизации и цифровой трансформации. Следовательно, она нуждается в дополнительных глубоких исследованиях.

1.3 Влияние информационных правонарушений на национальную безопасность

Основу национальной информационной безопасности составляют определенные документы, разработанные Советом Безопасности РФ с помощью экспертного сообщества и утвержденные указами президента. Доктрины, концепции, стратегии рассматривают различные аспекты современной цифровой действительности, новые угрозы, меры противодействия им и направления активности государства, усиливающего свои геополитические позиции.

«Национальная информационная безопасность – это комплексное понятие, которое разным способом раскрывается в юридической литературе, статьях экспертов, научных изданиях. Как правило, национальную информационную безопасность связывают не только с информационной сферой, она затрагивает и иные области деятельности государства, органы власти, оборонную сферу и внутреннюю политику

В Доктрине информационной безопасности рассматриваются в качестве объекта защиты интересы личности, общества и государства. В отсутствии охраны информационных интересов личности не может восприниматься государство как субъект общественного договора и гаранта суверенитета. В содержание определения информационно безопасности также включается защита информации и информационной инфраструктуры» [9, с. 128].

Иными словами, в условиях цифровизации национальная безопасность не представляется возможной без усиленной защиты информационной безопасности гражданина, населения и государства.

«При обеспечении национальной безопасности в области информации, формируется общество, в котором прослеживается:

- абсолютная реализация конституционных прав человека;
- высокий уровень благосостояния населения;
- охрана суверенитета, территориальной целостности;

– экономическое развитие государства;

– устранение угроз безопасности государства» [1, с. 33].

Провести оценку состояния безопасности представляется возможным по объективным параметрам. На рисунке 4 представлены ключевые параметры развитой системы информационной национальной безопасности.

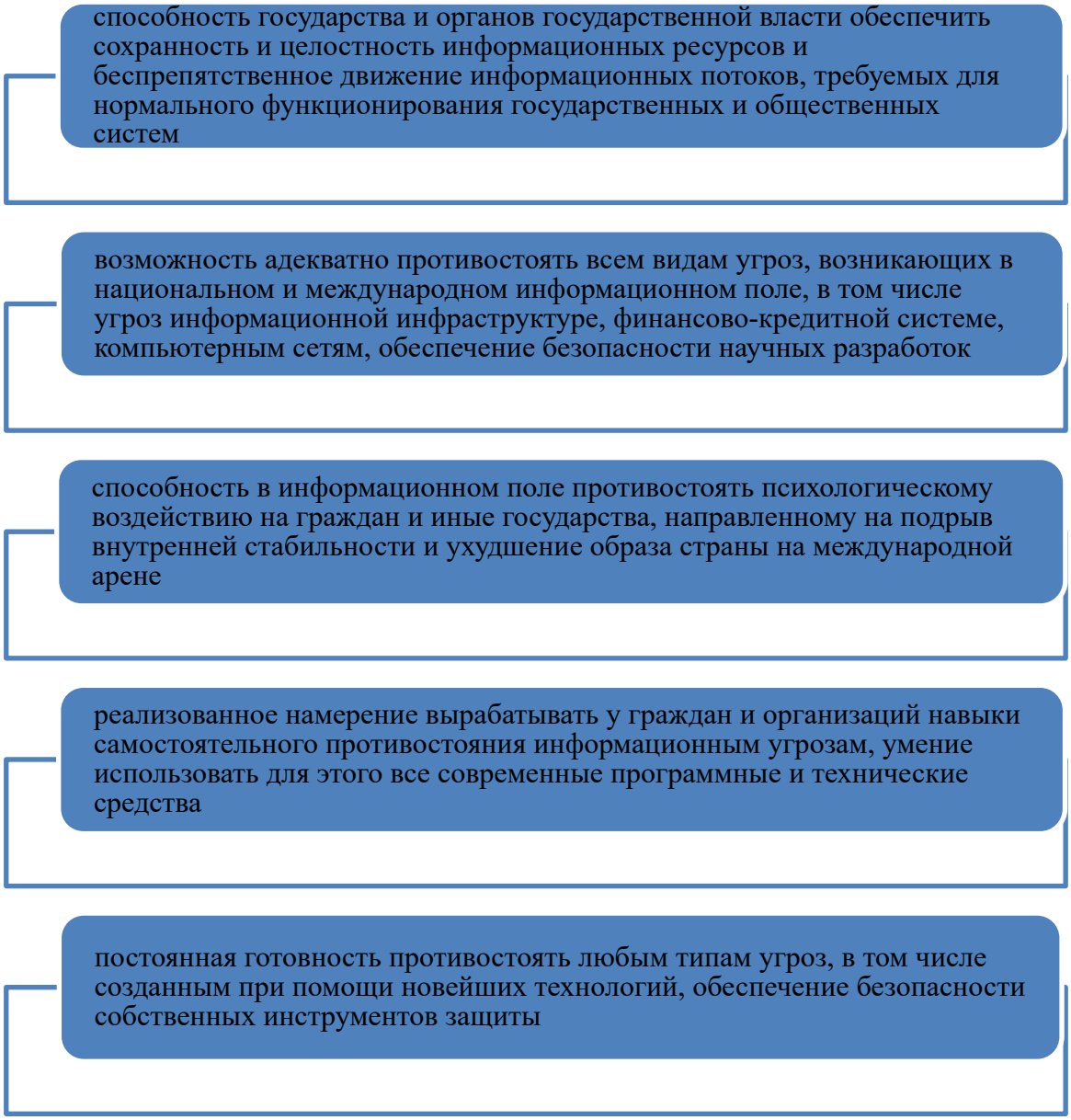

Рисунок 4 – Ключевые параметры развитой системы информационной национальной безопасности

Основу национальной информационной безопасности составляет комплекс технических, программных и научных ресурсов, являющихся объектами защиты и обеспечивающими безопасность.

За последние несколько лет произошло существенное изменение мира. Это связано с расширением цифровой трансформации, появлением новых телекоммуникационных связей, финансовых трансакций, распространение Интернета. Соответственно такие условия увеличивают доступность третьих лиц к различной личной, коммерческой информации, что вызывает определенные угрозы и риски нарушения национальной безопасности [9], [11].

«Быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

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

Активизируется деятельность специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве. Вооруженные силы таких государств отрабатывают действия по выведению из строя объектов критической информационной инфраструктуры Российской Федерации» [33].

Усиление защиты интересов личности и общества, которая выражается в сохранности информации защите от несанкционированного доступа к ней является важнейшей задачей для обеспечения национальной безопасности.

Информационное коммуникационные связи и технологии приобретают глобальный характер, что затрудняет их регулирование на национальном уровне и оперативное выявление источников рисков.

Систематический анализ возможностей и угроз в цифровом пространстве влияет на формирование приоритетных направлений

совершенствования мер защиты информационного пространства и обеспечения информационной безопасности [1], [2].

В такой ситуации можно выделить основные национальные интересы России в информационной сфере:

- обеспечение прав и свобод человека, его личных интересов в информационном пространстве;
- информационная поддержка гражданского общества;
- обеспечение безотказного информационного взаимодействия гражданина, общества и государства;
- использование информационных технологий для сохранение национальной идентичности;
- обеспечение безопасного и бесперебойного функционирования информационной инфраструктуры;
- развитие в государстве информационных технологий и электронной промышленности.

Распространение различных финансово-хозяйственных операций через сеть Интернет спровоцировало появление новых видов угроз и рисков, которые напрямую влияют на национальную безопасность. К числу таких угроз можно отнести [14]-[16], [28], [30], [31]:

- хакерские атаки;
- внедрение вирусных программ в государственные цифровые системы;
- разведывательные операции со стороны иностранных государств;
- нанесение урона путем реализации информационной войны против государства;
- блокирование программ и систем социально-значимых объектов и др.

Повышение угроз национальной безопасности вызвано:

- стремлением некоторых государств путем применения программных продуктов и технологий доминировать в информационном пространстве;

- усилением манипуляций гражданами, провоцируя их на совершение определенных действий, направленных на разбалансировку внутренней стабильности государства, нарушение суверенитета;
- давлением на российские средства массовой информации, сознательно формируя негативный образ России для иностранных государств.

Для обеспечения национальной безопасности в информационной сфере все участники данного процесса должны действовать взаимосвязано, содействовать достижению единой цели, направленной на защиту национальных интересов.

Следует подчеркнуть, что процесс защиты информационной безопасности характеризуется непрерывным взаимосвязанным применением превентивным и оперативных мер, направленных на обеспечение национальной безопасности. К таким мерам можно отнести:

- технические, а именно в области контроля над информацией в сети Интернет, импортозамещения программного обеспечения;
- организационные, в том числе направленные на разработку и принятие соответствующих нормативных документов;
- меры, производимые в сфере защиты национальных систем от хакерских атак;
- аналитические, проводимые обществом и государством;
- пропагандистские, реализуемые как на международном, так и на внутреннем уровне;
- меры, обеспечивающие информационную безопасность на международном уровне;
- кадровые, позволяющие обеспечить квалифицированных специалистов в области IT-безопасности;
- финансово-экономические, направленные на инвестирование в развитие информационных технологий и программных продуктов;
- разведывательные.

Вышеперечисленные меры не являются исчерпывающими. Они должны обеспечивать минимизацию новых вызовов и угроз в информационной сфере, своевременное прогнозирование рисков, устранение последствий в случае реализации угроз, наращение технического потенциала и усиление информационную безопасность страны.

Таким образом, в первой главе исследованы теоретические аспекты информационных правонарушений как угрозы национальной безопасности. В частности, в данной главе изучены правовые основы национальной безопасности. Раскрыт основные документы, затрагивающие вопросы обеспечения национальной безопасности РФ.

В данной главе существенное внимание уделено исследованию понятия информационных нарушений, выделению их основных видов и классификаций. Следует отметить, что на основании проведенного исследования в первой главе определено влияние информационных правонарушений на национальную безопасность страны. Существенное внимание уделено интересам России в области обеспечения информационной безопасности, раскрыты потенциальные угрозы, которые могут быть реализованы в случае реализации информационных правонарушений.

Глава 2 Классификация информационных правонарушений, угрожающих национальной безопасности

2.1 Информационные преступления

В настоящее время широкое распространение получила киберпреступность, увеличились преступления, связанные с информационными технологиями. Такая ситуация обосновывается стремительным ростом процессов цифровой трансформации, распространением информационно-телекоммуникационных каналов связи, появлением криптовалют, стремительным внедрением технологических инноваций во все отрасли экономики и человеческой жизни.

Безустанное распространение информационных технологий, формирование единого мирового информационного пространства сформировали возможность делового сотрудничества, общения людей по всему миру.

При этом, возникает острая проблема в том, что в настоящее время отсутствует законодательное регулирование информационного пространства как в пределах отдельно взятой страны, так и на мировом уровне. Это породило множество разных видов преступлений в информационной среде. Примерами таких преступлений могут быть следующие виды [16, с. 244]:

- преступления, связанные с интернетом. В частности, мошенничество в социальных сетях, при предоставлении дистанционных услуг;
- преступления, с использованием роботов, чат-ботов;
- преступления, связанные кибератакой и распространением вредоносных компьютерных программ;
- преступления, связанные с несанкционированным доступом к конфиденциальной информации;

– преступления, связанные с распространением «фэйковой» информации и др.

Необходимо отметить, что преступления в информационной сфере могут наносить огромный ущерб не только отдельным гражданам, но и организациям, государственным структурам. Тем самым, такие преступления могут оказывать негативное влияние на развитие отдельных отраслей, в целом экономику страны, национальную безопасность государства.

Как показывает практика, преступления, которые совершаются в информационно-телекоммуникационной сфере очень сложно раскрыть и доказать при судебном рассмотрении. Примерами могут выступать факты звонков мошенников, которые представляются сотрудниками правоохранительных органов и требуют раскрыть персональные данные, данные об открытых счетах в банках, затем добиваются перевода денежных средств путем обмана на их счета. Бывают инциденты, когда злоумышленники направляют сообщения своим жертвам о необходимости срочно перечислить денежные средства за родственника, попавшего в беду.

При этом практический опыт показывает, что при проверке сотрудниками внутренних дел таких сообщений, отмечается, что ущерб нанесен не был, так как злой умысел был своевременно раскрыт, их требования не выполнены, соответственно и нет состава преступления. В то время как действия неустановленных лиц, должны расцениваться как покушение на мошенничество. Такие действия являются преступлением, которое нарушитель собирался совершить с применением информационно-телекоммуникационных технологий.

В.А. Курбенков, А.В. Ушкань отмечают, что «низкой раскрываемости преступлений, совершаемых с использованием информационно-телекоммуникационных технологий способствуют также неудовлетворительное качество проводимых оперативно-розыскных мероприятий и доследственных процессуальных проверок, несвоевременное выполнение неотложных следственных действий, которые приводят к утрате

вещественных доказательств, затрате времени на поиски очевидцев, назначению дополнительных судебных экспертиз, что негативным образом сказывается на сроках предварительного расследования» [17, с. 81].

Необходимо отметить, что преступления в информационной среде имеют определенные особенности. Это связано со спецификой работы в компьютерных программах через телекоммуникационные каналы связи.

В современном законодательстве дается определение термина «информационные (виртуальные) следы преступлений. Они представляют различные изменения состояния автоматизированной информационной системы, которое связано с событием преступления и является зафиксированным в виде компьютерной информации.

Эта информация может отражать время, которое потратил преступник на совершение преступления [23, с. 89].

Однако, на практике для раскрытия преступлений в информационной среде такие сведения являются недостаточными.

Так сложились современные обстоятельства и тенденции, что сеть интернет выступает основным средством коммуникации между людьми. С ее помощью осуществляется не просто общение, а производятся финансовые операции, представляется возможность людям для самостоятельного перевода денежным средств в различные точки мира, приобретаются товары и услуги, осуществляется обмен информацией.

Таким образом, интернет распространился на все сферы жизни. Сейчас немыслимо как можно вести бизнес без помощи сети Интернет.

Для предпринимателей он также предоставляет широкие возможности, сокращая трудозатраты и время осуществления отдельных хозяйственных операций.

Именно посредством сети интернет и разных компьютерных программ предприниматели могут осуществлять переводы, отчитываться перед налоговыми органами [35, с. 155].

Следует отметить, что такая новая сфера информационного пространства не могла обойтись без преступлений. В этой связи стали появляться новые виды преступлений, такие как:

– IT-преступления;
– киберпреступность.

За последние годы большая часть финансовых преступлений совершается с использованием электронных платежных систем в информационном пространстве. Это порядка 10000 преступлений в год. [37, с. 14].

Кроме вышеуказанных, большое распространение получают преступления, связанные с неправомерным доступом к информации, а также разработкой и распространением вредоносных компьютерных программ.

По мнению Т.А. Овсянниковой и Г.И. Пещерова «парадокс цивилизации заключается в том, что криминальный мир более заинтересован в научно-техническом прогрессе и раньше, чем государства осваивает и использует новые достижения человеческого общества.

Широкое внедрение информационных технологий в научной, промышленной, образовательной, банковской, торговой и других сферах человеческой деятельности, закономерно расширяет границы преступной деятельности в этих сферах, создавая угрозу, как отдельному человеку, так и обществу в целом.

За последние десятилетия, интернет стал главным средством преступников экстремистско-террористической направленности, которые не только получают доступ к объектам особой важности, но и нарушают их нормальное функционирование» [23, с. 89].

Следует заметить, что дестабилизация работы информационной структуры негативно влияет на функционирование государственных систем управления, что напрямую нарушает национальную безопасность страны и общества.

Консервативные взгляды нормотворческих органов формируют позитивную основу для последующего распространения преступлений с информационной среде.

Т.А. Овсянникова и Г.И. Пещеров справедливо отмечают «несмотря на то, что термин преступления в сфере высоких технологий давно изучаются учеными и специалистами в области права, законодательный механизм, к сожалению, действует со значительным опозданием. При этом, в настоящее время в правовой системе существуют противоречия относительно того, что входит в понятие «преступления в сфере высоких технологий».

Причина тому стремительное развитие новых технологий, когда сформировавшееся, например, сегодня понятие, завтра уже становится устаревшим и не соответствует действительности реальной жизни» [23, с. 89].

К основным причинам повышения количества киберпреступлений следует отнести [6, с. 56-57]:

- высокий доход, получаемый от данных преступлений;
- прост количества электронных платежей населения, что способствует к активному применения интернет-банкинга и увеличению числа сетевых преступников;
- неграмотность пользователей, которые доверяют интернет мошенникам;
- слабая защита от современных телефонов от проникновения вредоносных программ, посредством которых преступники похищают денежные средства с банковских счетов;
- возможность использования для преступлений информации из социальных сетей, которую люди размечают о себе;
- трудная доказуемость преступлений, совершенных в информационной среде;
- не проработанность правовых норм, регулирующих отношения в информационной среде;

- отсутствие достаточной практики расследования киберпреступлений;
- слабые системы защиты информационного пространства от несанкционированного доступа к личной информации.

В настоящее время различаю следующие основные группы мер, направленных на предупреждение преступлений в информационной среде [30, с. 235].

К первой группе относятся правовые меры - представляют собой нормотворческую деятельность по разработке норм законодательства, направленных на регулирование отношений в обществе и обеспечивающие информационную безопасность.

Ко второй группе относятся организационные меры, предполагающие разработку программ защиты компьютерных программ, баз данных.

К основным норм уголовного права, закрепляющим ответственность за преступления в информационной среде относятся:

- ст. 159.3 УК РФ – мошенничество с использованием электронных средств платежа;
- ст. 273 УК РФ – создание, использование и распространение вредоносных компьютерных программ;
- ст. 272 УК РФ – неправомерный доступ к компьютерной информации.

В завершении необходимо отметить, что профилактические меры по предотвращению преступлений в информационной среде должны состоять из:

- комплекса законодательных норма, отвечающим современным требованиям,
- постоянного совершенствования средств защиты информации и доступа к сетям, программам, базам данных;
- совершенствования технических средств и методов работы правоохранительной системы, специальных служб и судебной системы.

Считаем, что сократить преступления в информационной среде можно только с помощью комплексного механизма, учитывающего интересы всех стран и охватывающего информационное пространство.

2.2 Административные и гражданско-правовые информационные правонарушения

Эффективное функционирование области информационных правоотношений реализуется посредством разных правовых средств, важную роль среди которых играют административно-юрисдикционные средства.

В настоящее время для борьбы с правонарушениями в информационной среде отводится административному законодательству. В главе 13 КоАП РФ закреплены нормы административной ответственности за совершение правонарушений в информационной среде.

В этой связи, исследование вопросов института административной ответственности за деяния в информационном пространстве, что предопределяет актуальность и потребность в исследовании проблем в данной сфере.

Именно использование административного наказания направлено на соблюдение принципа восстановления социальной справедливости, относящего к ключевым конституционным принципам [19, с. 104].

Анализ санкций правовых норм КоАП РФ позволяет выделить административные наказания, применяемые за правонарушения, совершаемые в сети. К ним можно причислить [19, с. 104]:

- предупреждение;
- административный штраф;
- конфискация орудия совершения или предмета административного правонарушения;
- административный арест;

- административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства;
- дисквалификация;
- административное приостановление деятельности;
- обязательные работы.

«Административное наказание характеризуется эффективным и достаточным средством, ограниченной необходимостью адекватной реакции государства именно на правонарушение и позволяющее, исходя из принципов справедливости, соразмерности и правовой безопасности, гарантировать защиту конституционных ценностей» [31, с. 122].

«Общими признаками административного наказания за правонарушения, совершаемыми в глобальной информационной сети являются:

- административное наказание представляет собой меру ответственности, которая установлена государством и применяется от его имени;
- административное наказание применяется только в случае совершения административного правонарушения;
- административное наказание применяется только тогда, когда установлена и доказана вина лица, которое совершило административное правонарушение;
- при назначении административного наказания учитывается личность правонарушителя;
- административное наказание должно соответствовать (быть пропорциональным, адекватным) тяжести совершенного правонарушения;
- административное наказание обусловливает формирование состояния наказанности лица,
- которое совершило правонарушение» [19, с. 105].

«Административные правонарушения в глобальной сети относятся к явлению достаточно новому для российской административно правовой науки, в связи с чем административное наказание в виде конфискации технических средств, с помощью которых осуществлялось распространение информации через интернет, предусмотрено не во всех правовых нормах КоАП РФ, устанавливающих ответственность за подобные правонарушения» [29, с. 66].

Так, за изготовление и (или) распространение теле-, видео-, кинопрограмм, документальных и художественных фильмов, а также относящихся к специальным средствам массовой информации информационных компьютерных файлов и программ обработки информационных текстов, содержащих скрытые вставки, воздействующие на подсознание людей и (или) оказывающие вредное влияние на их здоровье часть 1 статьи 13.15 КоАП РФ предусматривает наложение административного штрафа на граждан, должностных и юридических лиц с конфискацией предмета административного правонарушения [19, с. 107].

Положения статьи 20.29 КоАП РФ «Производство и распространение экстремистских материалов» предусматривают конфискацию лишь материалов и оборудования, использованных для производства экстремистских материалов.

За некоторые правонарушения, совершаемые в сети, применяется административное наказание в виде административного ареста.

Данный вид административного наказания может применяться только в случае наличия обстоятельств, отягчающих административную ответственность, исчерпывающий перечень которых приведен в части 1 статьи 4.3 КоАП РФ. Если такие обстоятельства отсутствуют, то должны применяться другие, менее суровые административные наказания.

Часть 2 статьи 6.13 КоАП РФ «за пропаганду либо незаконную рекламу наркотических средств, психотропных веществ или их прекурсоров, растений, содержащих наркотические средства или психотропные вещества либо их

прекурсоры, и их частей, содержащих наркотические средства или психотропные вещества либо их прекурсоры, а также новых потенциально опасных психоактивных веществ, если правонарушение совершено иностранным гражданином либо лицом без гражданства, предусматривает наложение административного штрафа с административным выдворением за пределы Российской Федерации либо административный арест на срок до пятнадцати суток» [15].

КоАП РФ за незаконные действия по получению и (или) распространению информации, например, составляющей кредитную историю, если такие действия не содержат уголовно наказуемого деяния, предусмотрено применение административного наказания в виде административного штрафа, налагаемого на должностных лиц, или дисквалификацию на срок до трех лет.

Часть 2 статьи 5.26 КоАП РФ предусматривает за умышленное публичное осквернение религиозной или богослужебной литературы, а также предметов религиозного почитания, знаков или эмблем мировоззренческой символики и атрибутики либо за их порчу или уничтожение применение в отношении граждан административного штрафа либо обязательных работ на срок до ста двадцати часов [19, с. 109].

«К основным признакам административной ответственности за правонарушения в информационном праве можно отнести совокупность противоправных, виновных, общественно опасных деяний организаций и физических лиц, в отношении которых предусмотрено установление мер административной ответственности» [29, с. 66].

«Проанализировав административные правонарушения, посягающие на общественные отношения в информационной сфере, предусмотренные главой 13 КоАП РФ, можно разделить их на три основные группы:

- административные правонарушения в области средств массовой информации (ст. ст. 13.1-13.18, 13.21-13.23 КоАП РФ);

- кроме того, существует определенный вид административных правонарушений, которые посягают на установленный на территории Российской Федерации порядок сбора, хранения и распространения информации ограниченного доступа. Этот порядок рассматривается в статьях 13.11, 13.11.1, 13.12-13.14, 13.19, 13.19.1, 13.20, 13.25, 13.27, 13.28 КоАП РФ;
- административные правонарушения, связанные с нарушением использования и распространения информации в сети Интернет (ст.ст. 13.31, ст.13.32, 13.35, 13.36, 13.37, ст.13.39 КоАП РФ).

На современном этапе существует определенный перечень проблем, связанных с привлечением к административной ответственности за правонарушения юридических и физических лиц в информационном праве.

К важнейшим из них можно отнести:

- наличие взаимных пересечений норм административной и уголовной ответственности к нарушителям информационной безопасности;
- низкий уровень эффективности расследования дел в информационной сфере и, соответственно, установления соответствующего наказания» [8, с. 40].

«Естественно, по состоянию на 2021 год в Российской Федерации уровень эффективности мер административной ответственности за противоправные деяния в информационной сфере вышел на новые рубежи, однако до полного охвата всей сферы информационного права ещё далеко. Можно отметить, что данный аспект связан с особым менталитетом российского народа, привыкшего к безнаказанности за деяния в интернете» [10, с. 74].

«К основным мероприятиям по совершенствованию мер административной ответственности в информационном праве следует отнести модернизацию ответственности за незаконную деятельность по разглашению информации с ограниченным доступом по статье 13.14 КоАП РФ.

Считаем важным ограничить круг должностных лиц, которые уполномочены составлять протоколы по данной категории дел. Кроме того, следует ужесточить меры административной ответственности в области оскорблений в сети интернет» [8, с. 40].

Таким образом, административным наказанием за правонарушения, совершаемые в информационном пространстве, является мера ответственности, установленная государством и применяемая к лицу, признанному виновным в совершении данного правонарушения, в целях предупреждения совершения новых правонарушений как самим правонарушителем, так и другими лицами и заключающаяся в применении таких административных наказаний в зависимости от характера административного правонарушения в киберпространстве, как предупреждение, административный штраф, конфискация орудия совершения или предмета административного правонарушения, административный арест, административное выдворение за пределы Российской Федерации иностранного гражданина или лица без гражданства, дисквалификация, административное приостановление деятельности, обязательные работы.

2.3 Дисциплинарные информационные правонарушения

Дисциплина труда является обязательной для всех сотрудников и направлена на подчинение правилам поведения, установленным ТК РФ [32].

Дисциплинарная ответственность наступает за нарушение работником своих трудовых обязанностей. За совершение дисциплинарного проступка, т.е. за неисполнение или ненадлежащее исполнение лицом, состоящим в трудовых отношениях или гражданским служащим по его вине возложенных на него должностных обязанностей, наниматель или представитель нанимателя имеет право применить одно из следующих дисциплинарных взысканий:

– замечание;
– выговор;
– предупреждение о неполном должностном соответствии;
– освобождение от замещаемой должности гражданской службы;
– увольнение с гражданской службы.

Дисциплинарная ответственность применяется на основании норм Трудового кодекса Российской Федерации.

Увольнение с гражданской службы осуществляется по основаниям, установленным пунктом 2, подпунктами «а» — «г» пункта 3, пунктами 5 и 6 части 1 статьи 37 Федерального закона от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации».

«Дисциплинарным информационным правонарушением (проступком) является виновное, противоправное деяние (действия или бездействие), т.е. неисполнение или ненадлежащее исполнение работником возложенных на него трудовых обязанностей, совершенное в сфере информации.

Необходимо отметить, что дисциплинарные информационные правонарушения имеют отличительные признаки. К ним можно отнести:

– сферу информации (информационную сферу) — пространственно-временную область деятельности, связанную с поиском, хранением, обработкой, передачей и использованием информации;
– наличие факта неисполнения или ненадлежащего исполнения трудовых обязанностей, связанных с информацией» [22, с. 163].

Дисциплинарные информационные правонарушения имеют ряд особенностей.

Во-первых, нормы права, которые регулируют обязанности согласно трудовым контрактам, связанные с использованием информации носят как правило локальный характер.

Иными словами, организация может самостоятельно утвердить специфические трудовые обязанности, которые непосредственно связаны с работой в информационной среде.

Такие условия закрепляются в особых инструкциях и положениях по работе с цифровыми устройствами, информационными программами, а также по регламенту работы с конфиденциальной информацией.

Во-вторых, информация, используемая работником в пределах организации в связи с исполнением функциональных обязанностей, носит служебный характер.

«К наиболее распространенному виду дисциплинарного информационного правонарушения относятся нарушения работниками режима информации, а именно разглашение сведений, составляющих коммерческую, банковскую или государственную тайну, персональные данные другого работника или клиентов» [18]. Такие действия работника могут стать основанием привлечения к дисциплинарной ответственности в виде увольнения (подл, «в» и. 6 ст. 81 ТК РФ).

Увольнение работника за информационные дисциплинарные правонарушения могут быть в случаях, если:

- информация является коммерческой тайной;
- работник ознакомлен с информацией. составляющей коммерческую тайну;
- работник распространил конфиденциальную информацию или ее утратил.

Деяниями (действием или бездействием), которые могут быть основаниями для увольнения в информационной сфере, являются:

- нарушение требований по распространению информации и сведений, содержащих охраняемую федеральным законом тайну, и служебную информацию, ставших известными гражданскому служащему в связи с исполнением им должностных обязанностей;
- предоставления гражданским служащим представителю нанимателя подложных документов или заведомо ложных сведений при заключении служебного контракта;

– прекращения допуска гражданского служащего к сведениям, составляющим государственную тайну, если исполнение должностных обязанностей требует допуска к таким сведениям.

За каждый дисциплинарный проступок может быть применено только одно дисциплинарное взыскание.

В ст. 90 ТК РФ установлено, что «за нарушение норм, регулирующих получение, обработку и защиту персональных данных, лицо несет дисциплинарную, административную, гражданско-правовую или уголовную ответственность в соответствии с федеральными законами» [32].

«Режим конфиденциальности работы с данными включает в себя следующие условия:

– правила сбора, обработки, передачи и использования персональных данных закреплены локальным нормативным актом организации;
– руководителем организации определены специально уполномоченные работники, обладающие доступом к персональным данным;
– права, обязанности и ответственность работников, имеющих допуск к персональным данным, регулируются должностными инструкциями и трудовым договором (контрактом)» [38, с. 159].

Дисциплинарная ответственность работника может наступить за совершение действий или бездействие при обработке персональных данных с учетом названных условий режима конфиденциальности.

До применения дисциплинарного взыскания представитель нанимателя должен затребовать от гражданского служащего объяснение в письменной форме. В случае отказа гражданского служащего дать такое объяснение составляется соответствующий акт.

Отказ гражданского служащего от дачи объяснения в письменной форме не является препятствием для применения дисциплинарного взыскания.

Перед применением дисциплинарного взыскания проводится служебная проверка.

При применении дисциплинарного взыскания учитываются тяжесть совершенного гражданским служащим дисциплинарного проступка, степень его вины, обстоятельства, при которых совершен дисциплинарный проступок, и предшествующие результаты исполнения гражданским служащим своих должностных обязанностей.

Дисциплинарное взыскание применяется непосредственно после обнаружения дисциплинарного проступка, но не позднее одного месяца со дня его обнаружения, не считая периода временной нетрудоспособности гражданского служащего, пребывания его в отпуске, других случаев отсутствия его на службе по уважительным причинам, а также времени проведения служебной проверки.

Дисциплинарное взыскание не может быть применено позднее шести месяцев со дня совершения дисциплинарного проступка, а по результатам проверки финансово-хозяйственной деятельности или аудиторской проверки — позднее двух лет со дня совершения дисциплинарного проступка. В указанные сроки не включается время производства по уголовному делу.

«Копия акта о применении к гражданскому служащему дисциплинарного взыскания с указанием оснований его применения вручается гражданскому служащему под расписку в течение пяти дней со дня издания соответствующего акта.

Гражданский служащий вправе обжаловать дисциплинарное взыскание в письменной форме в комиссию государственного органа по служебным спорам или в суд» [39, с. 479].

Если в течение одного года со дня применения дисциплинарного взыскания гражданский служащий не подвергнут новому дисциплинарному взысканию, он считается не имеющим дисциплинарного взыскания.

Представитель нанимателя вправе снять с гражданского служащего дисциплинарное взыскание до истечения одного года со дня применения дисциплинарного взыскания по собственной инициативе, по письменному

заявлению гражданского служащего или по ходатайству его непосредственного руководителя.

Таким образом, во второй главе рассмотрена классификация информационных правонарушений, угрожающих национальной безопасности. В данной главе исследованы информационные преступления, представлены основные статьи, устанавливающие уголовную ответственность за такие преступления.

Особое внимание уделено изучению административных и гражданско-правовых информационных правонарушений. Указаны меры административных наказаний правонарушения в информационном пространстве.

Во второй главе раскрыты дисциплинарные информационные правонарушения, изучены видны дисциплинарных наказаний за такие правонарушения.

Глава 3 Проблемы ответственности за информационные правонарушения, угрожающие национальной безопасности

3.1 Система законодательства об ответственности за информационные правонарушения

В настоящее время информация представляет собой один из важных ресурсов мирового общества. Информация приобретаем большое значение во всех сферах экономики, политики и права. Современное развитие научно-технического прогресса выводит информацию на новый уровень, поскольку она ложится в основу развития современного общества, экономики, государства.

Быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства.

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

Увеличивается количество компьютерных атак на российские информационные ресурсы. Большая часть таких атак осуществляется с территорий иностранных государств.

Инициативы Российской Федерации в области обеспечения международной информационной безопасности встречают противодействие со стороны иностранных государств, стремящихся доминировать в глобальном информационном пространстве.

Активизируется деятельность специальных служб иностранных государств по проведению разведывательных и иных операций в российском информационном пространстве. Вооруженные силы таких государств

отрабатывают действия по выведению из строя объектов критической информационной инфраструктуры Российской Федерации» [33].

В целях дестабилизации общественно-политической ситуации в Российской Федерации распространяется недостоверная информация, в том числе заведомо ложные сообщения об угрозе совершения террористических актов.

«В информационно-телекоммуникационной сети интернет размещаются материалы террористических и экстремистских организаций, призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, совершению самоубийства, осуществляется пропаганда криминального образа жизни, потребления наркотических средств и психотропных веществ, размещается иная противоправная информация. Основным объектом такого деструктивного воздействия является молодежь.

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

Использование в Российской Федерации иностранных информационных технологий и телекоммуникационного оборудования повышает уязвимость российских информационных ресурсов, включая объекты критической информационной инфраструктуры Российской Федерации, к воздействию из-за рубежа» [33].

В этой связи, повышается необходимость в поиске эффективных направлений защиты информации, предотвращения преступлений в информационной среде посредством совершенствования системы законодательства.

«В механизме правового обеспечения в информационной сфере значимое место занимают борьба с нарушениями информационного законодательства и их предупреждение. Для этого действует так называемый институт юридической ответственности, закрепленный в российском законодательстве.

Основополагающие положения законодательства в информационной сфере содержатся в Конституции РФ. В ней закреплено право каждого на неприкосновенность частной жизни, личную и семейную тайну, указано, что сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются и т.д. Федеральным законом «О персональных данных» сведения о гражданах (персональные данные), т.е. о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, отнесены к конфиденциальной информации. Законодательством также определены сведения, право свободного доступа, к которым не может быть ограничено» [21].

Российское государство усиливает свое внимание к проблеме укрепления информационного правопорядка.

В Стратегии национальной безопасности Российской Федерации отмечено, что «целью обеспечения информационной безопасности является укрепление суверенитета Российской Федерации в информационном пространстве» [33]

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

- формирование безопасной среды оборота достоверной информации;
- развитие системы прогнозирования, выявления и предупреждения угроз информационной безопасности Российской Федерации;
- предотвращение деструктивного информационно-технического воздействия на российские информационные ресурсы;

- создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных правонарушений, совершаемых с использованием информационно-коммуникационных технологий;
- повышение защищенности и устойчивости функционирования единой сети электросвязи Российской Федерации, российского сегмента сети "Интернет";
- снижение до минимально возможного уровня количества утечек информации ограниченного доступа и персональных данных;
- предотвращение и (или) минимизация ущерба национальной безопасности, связанного с осуществлением иностранными государствами технической разведки;
- обеспечение защиты конституционных прав и свобод человека и гражданина при обработке персональных данных, в том числе с использованием информационных технологий;
- укрепление информационной безопасности Вооруженных Сил, других войск, воинских формирований и органов, а также разработчиков и изготовителей вооружения, военной и специальной техники;
- совершенствование средств и методов обеспечения информационной безопасности на основе применения передовых технологий, включая технологии искусственного интеллекта и квантовые вычисления;
- укрепление сотрудничества Российской Федерации с иностранными партнерами в области обеспечения информационной безопасности;
- развитие взаимодействия органов публичной власти, институтов гражданского общества и организаций при осуществлении деятельности в области обеспечения информационной безопасности Российской Федерации;
- иные задачи, связанные с обеспечением информационной безопасности Российской Федерации» [33].

При этом особо отмечается, что национальные интересы России в информационной сфере заключаются в соблюдении конституционных прав и свобод граждан в области получения информации и пользования ею, в развитии современных телекоммуникационных технологий, в защите государственных информационных ресурсов от несанкционированного доступа.

Проведенное исследование показало, что за правонарушения в информационной среде может наступать:

- уголовная ответственность;
- административная ответственность;
- дисциплинарная ответственность.

Меры наказания за преступления в информационной среде закреплены в УК РФ.

В зависимости от видов информационных преступлений меры наказаний могут отличаться.

Однако проведенное исследование показало, что в настоящее время возникаю значительные сложности в расследовании информационных преступлений.

Кроме этого, ответственность за многие преступления в информационной среде не раскрываются в нормах законодательства. Это связано с тем, что неустанно развиваются цифровые технологии, создавая не только возможности для совершения различных финансово-хозяйственных операций, но провоцирующих появление новых видов преступлений.

Как было отмечено ранее за административные информационные правонарушения наступает административная ответственность, которая регулируется КоАП РФ.

За административные информационные нарушения КоАП РФ предусмотрены такие меры наказания, как:

- предупреждение;
- административный штраф;

– конфискация орудия совершения или предмета административного правонарушения;
– административный арест и др.

В Уголовном кодексе РФ к преступлениям в информационной сфере можно отнести более 50 статей, причем отдельная глава УК РФ (глава 28) посвящена составам преступлений в сфере компьютерной информации. В ней содержатся три статьи преступлений (ст. 272-274).

В Кодексе РФ об административных правонарушениях, существенным новшеством которого является возможность привлечения за правонарушения к административной ответственности юридических лиц, также имеется глава 13 и отдельные статьи в ряде глав, посвященные административным правонарушениям в информационной сфере.

«Отдельные правонарушения, связанные с информацией, которые могут допустить работники влекут дисциплинарную ответственность. Необходимо отметить, что меры дисциплинарной ответственности могут устанавливаться в локальных документах и быть различными на разных предприятиях.

Основанием для возникновения юридической ответственности является совершенное субъектом (участником) информационных правоотношений правонарушение в информационной сфере.

Правонарушением в информационной сфере принято считать виновное, противоправное деяние (действие, бездействие) конкретного субъекта, посягающее на установленный информационный правопорядок и причиняющее вред информационной сфере либо создающее реальную угрозу такого причинения» [24, с. 165].

Для реализации юридической ответственности важно установить причинно-следственные связи между негативными последствиями, наступившими в результате правового предписания, и действиями (бездействием) предполагаемого правонарушителя.

«Основной целью применения юридической ответственности к правонарушителям является поддержание информационного правопорядка,

основанного на соблюдении большинства субъектов информационных правоотношений установленным материальным нормам информационного права, а не только наказание виновного субъекта.

К сожалению, не все субъекты правоотношений соблюдают информационный правопорядок.

Многие из них нарушают этот правопорядок и подвергаются воздействию норм информационного права, устанавливающих юридическую ответственность.

Однако на часть субъектов сам факт наличия таких норм права, которые устанавливают юридическую ответственность, действует как сдерживающий фактор, предупреждающий их неправомерные действия в информационной сфере.

Отсюда вытекает, что установление юридической ответственности носит еще и некое нравственно-воспитательное значение» [29, с.67].

Таким образом, юридическая ответственность за правонарушения в информационной сфере - это применение к виновному лицу, совершившему правонарушение, мер воздействия, предусмотренных санкцией нарушенной нормы информационного права в определенном регламентированном порядке.

«Юридическим основанием привлечения к ответственности является наличие в деянии (действии, бездействии) правонарушителя состава правонарушения в информационной сфере, предусмотренного нормами права.

Состав правонарушения, в том числе и информационного, включает в себя четыре обязательных элемента (признака):

- объект,
- объективную сторону,
- субъект;
- субъективную сторону.

Объектом правонарушения является совокупность общественных отношений в информационной сфере.

Субъектами правонарушения в информационной сфере могут быть физические и юридические лица в зависимости от вида юридической ответственности» [31, с. 122].

«Отнесение правонарушения к тем или иным видам зависит в основном от степени причиненного природе и обществу вреда, личности правонарушителя, иных обстоятельств дела, влияющих на уровень ответственности» [37, с. 15].

Важно понимать, что стремительное развитие сети интернет, широкое применение информационно-телекоммуникационных технологий не только в повседневной жизни, бизнес-среде, но и в управлении государством создает новые угрозы национальной безопасности.

В настоящее время практически сформирована основная нормативная база по предупреждению и пресечению правонарушений в информационной сфере, предусматривается как:

- гражданско-правовая,
- дисциплинарная (включая материальную),
- административная ответственность,
- уголовная ответственность за совершение правонарушений и преступлений в информационной сфере.

В современных условиях разработаны и действуют многочисленные законы и подзаконные акты в информационной сфере. Существенное внимание уделяется вопросам снижения информационной безопасности в различных отраслях экономики, системе государственного управления.

Но их практическое применение довольно слабое, отсутствуют конкретные механизмы применения и соблюдения законодательства на практике, существуют трудности по наложению взысканий за его нарушения, отсутствует систематизация действий правоохранительных органов по осуществлению своих обязанностей и прав и информационной сфере.

3.2 Анализ проблем института ответственности за информационные правонарушения, угрожающие национальной безопасности и пути их решения

В настоящее время процессы, происходящие внутри государства тесно взаимосвязаны с глобальной интеграцией в общемировую информационную сферу. Влияние факторов мирового информационного пространства происходит ежедневно.

Следствием такого влияние является распространение информации, которая не всегда может отражать реальную действительность.

Кроме этого возрастают факты распространения информации, имеющей агрессивную, противоречивую направленность, носящую скрытый негативный подтекст.

Все эти обстоятельства отрицательно влияют на стабильность в обществе, создавая определенный дисбаланс, что создает угрозу национальной безопасности страны.

Следует осознавать, что в современных условиях создается противоречивая обстановка, при которой происходят процессы трансформации информационного общества.

В настоящее время особую угрозу может вызывать информационная война, которая не только дестабилизирует государственную систему, но и может запустить волну общественного протеста. Все это может быть спровоцировано злоумышленниками, имеющими цель нарушить национальную безопасность отдельно взятой страны.

В этой связи остаются нерешенными вопросы обеспечения действенной правовой охраны информационной среды, установления разных мер юридической ответственности за совершение преступлений в информационном пространстве и с использованием цифровых и информационно-телекоммуникационных технологий.

Следует подчеркнуть, что современная правовая система в области защиты от информационных правонарушений является не до конца развитой. Она не учитывает скорость совершенствования цифровых технологий и быстроту появления новых мошеннических схем в области информационного пространства.

При этом возникают существенные проблемы привлечения к ответственности за совершенные преступниками информационные правонарушения.

Отсутствуют адекватные реальным условиям меры защиты граждан и государства от несанкционированного доступа к конфиденциальной личной и государственной информации.

К основной проблеме привлечения к административной ответственности за правонарушения в информационной сфере относится скорость развития интернет-пространства [20], [25], [26], [27], [40].

Общепризнанным сегодня является утверждение, что XXI в. представляет собой прежде всего век информации.

«Органы государственной власти, организации различных форм собственности, а также граждане в повседневной деятельности могут получить путем использования различных технических устройств мгновенный доступ практически к любой информации.

Неслучайно, что именно в современных условиях развития государства, общества и личности Интернет расположился в числе главнейших информационных средств передачи и хранения информации, наряду с такими классическими СМИ, как радио и телевидение, журналы, газеты. И именно СМИ принадлежит одна из главнейших ролей в создании политической и государственной пропаганды, в оказании влияния на сознание общества и граждан» [38, с. 160].

Взаимоотношения, образующиеся в информационном пространстве с использованием сети интернет, имеют ряд особенностей в их правовом регулировании.

Первая особенность состоит в том, что в интернет пространстве местонахождение участников отношений определить достаточно трудно. «Так, сообщения в сети Интернет могут передаваться лицами, которые физически находятся в разных государствах, соответственно, может возникать коллизия в применении норм права соответствующей страны, в том числе в установлении местоположения лиц, совершающих противоправные деяния с использованием глобальной сети.

В данном контексте виновные лица (организатор) могут быть привлечены к административной ответственности за неисполнение обязанностей по распространению информации в сети Интернет (ст. 13.31 КоАП РФ)» [36].

Вторая особенность заключается в сложности идентификации сторон взаимоотношений. «Всемирная паутина Интернет предоставляет пользователю возможность оставаться, как правило, максимально анонимным, что создает благоприятную атмосферу для совершения действий противоправного характера» [36].

Третья особенность состоит в специфике сети интернет, которая создавая большие технические возможности для пользователей позволяет им совершать различные электронные действия – переписку, распространение фото-, видео информации, осуществлять платежи, переводы денежных средств, быть участниками фондовых бирж, проводить онлайн-голосования и анкетирования и т.д.

Такая возможность предоставляется и органам государственной власти. Например, органы государственной власти и местного самоуправления, которые размещают в сети интернет информацию о своей деятельности в случаях, установленных федеральным законом. При этом, за нарушение установленной обязанности виновные лица привлекаются к ответственности по ст. 13.27 КоАП РФ.

Принимая во внимание вышеуказанные особенности необходимо понимать, что регулирование интернет-взаимоотношений посредством

различных механизмов и законодательных мер является проблематичным и не всегда возможным в практике. В первую очередь, это связано с отсутствием проработанной законодательной базы, затрагивающую информационную среду.

В этой связи представляется необходимым системно провести изменения в соответствующих нормах законодательства с учетом специфики отношений и возможностей информационного пространства.

Следующей проблемой, в частности привлечения к административной ответственности за правонарушения в информационной сфере является конкуренция норм законодательства об административных правонарушениях и уголовного законодательства в сфере информации.

В частности, в процессе квалификации административных правонарушений и преступлений в информационной сфере могут возникать сложности в определении оценки категории "существенный вред".

«Присутствие критерия "существенный ущерб" лежит в основе разграничения ст. 5.39 КоАП РФ и ст. 140 УК РФ.

Так, административная ответственность по ст. 5.39 КоАП РФ наступает за неправомерный отказ в предоставлении гражданину и (или) организации информации, предоставление которой закреплено в нормах законодательства, либо несвоевременное получение или предоставление заведомо недостоверной информации, за исключением случаев, установленных в ст. 7.23.1 КоАП РФ.

При наличии существенного вреда при совершении данного правонарушения ответственность наступает по ст. 140 УК РФ.

Заметим, что понятие "существенный вред" является оценочной категорией. Как правило, существенным вредом признается вред, причиненный имущественным отношениям.

Вместе с тем отметим, что в литературе существует и иная точка зрения, согласно которой вред, причиненный правам и законным интересам гражданина, может быть и моральным, т.е. выражаться в нравственных

страданиях потерпевшего, например, в результате неполучения, неполного или несвоевременного получения пенсии или заработной платы.

В случае отсутствия конкретизации последствий нанесенного вреда в результате совершения административного правонарушения можно презюмировать наличие как морального, так и имущественного вреда, причиненного правам и законным интересам гражданина.

В подобных случаях отграничение состава административного правонарушения в информационной сфере от уголовно-наказуемых деяний, посягающих на информационные отношения, представляется достаточно сложным» [36].

В этой связи, на наш взгляд, законодателю необходимо отказаться от использования оценочных категорий, что, в свою очередь, может позитивно повлиять на преодоление сложностей в их квалификации.

Возможное решение указанной проблемы видится в дополнении соответствующих норм административного и уголовного права, содержащих оценочные категории, их легальным определением в соответствующих примечаниях, в которых будет даваться исчерпывающая характеристика соответствующих понятий.

Считаем также целесообразным вышестоящей судебной инстанции нашей страны принять соответствующее разъяснение Пленума Верховного Суда Российской Федерации, посвященное информационным правонарушениям, положения которого могли бы поспособствовать единообразному применению норм отраслевых актов в информационной сфере.

Третьей проблемой привлечения к административной ответственности за правонарушения в информационной сфере выступает низкая эффективность расследования рассматриваемой категории правонарушений и судебного разбирательства.

«Определенные проблемы в борьбе с административными правонарушениями в информационной сфере вызывают следующие обстоятельства.

В первую очередь это высокий уровень латентности указанной группы правонарушений.

Здесь основной причиной, на наш взгляд, является отсутствие видимых материальных следов приготовления и совершения данного правонарушения» [31, с. 123].

«Следующее обстоятельство — это, конечно, разнообразие способов совершения данных административных правонарушений. Вызывает также определенные трудности определение самого события правонарушения, включающего в себя место и время его совершения. Также вызывает затруднение определение времени совершения административных правонарушений в информационной сфере. Например, разглашение информации с ограниченным доступом (ст. 13.14 КоАП РФ) может иметь место не с момента получения такой информации, а с момента наступления определенного события» [8, с. 40].

Как правило, дела об административных правонарушениях в информационной сфере в основном возбуждаются либо по сведениям, полученным в ходе осуществления административных мероприятий, либо по факту уже совершенного правонарушения.

«Вместе с тем заметим, что расследование совершенного административного правонарушения в информационной сфере имеет ретроспективный характер и проводится, как правило, не сразу, а спустя определенное время после его совершения, тем самым понижается возможность установления лиц, причастных к совершению данного правонарушения, и получения необходимых доказательств по делу ввиду несохранения провайдером соответствующей информации в течение длительного периода времени.

Тем самым процесс получения "виртуальных" следов, имеющих значение для восстановления механизма совершенного административного правонарушения, является достаточно затруднительным, что, соответственно, прямым образом отражается на судебном разбирательстве информационных правонарушений» [10, с. 76].

К четвертой проблеме привлечения к административной ответственности является назначение и исполнение меры административного наказания для правонарушения в информационном пространстве.

«Санкции административно-правовых норм, устанавливающих ответственность за правонарушения в информационной сфере, вызывают определенные сомнения в их эффективности.

Несмотря на все нововведения, которые периодически вносятся в содержание норм главы 13 КоАП РФ, размеры административных штрафов, назначаемых за совершение административных правонарушений в информационной сфере, несмотря на их увеличение, в целом не соответствуют достижению целей административного наказания и превенции подобных правонарушений.

Правовые последствия совершенных административных правонарушений в информационной сфере порою могут в разы превышать реальный ущерб, причиненный охраняемым законом общественным отношениям» [15].

Представляется, что для решения указанной проблемы назначения справедливого административного наказания за правонарушения в информационной сфере законодателю необходимо кардинально пересмотреть принципы и правила его назначения. Фиксированный вид и размер административного наказания за совершение того или иного вида административного правонарушения должны быть конкретизированы в законодательстве.

Кроме того, считаем, что при назначении административного наказания за правонарушения в информационной сфере соответствующим

уполномоченным лицам, рассматривающим дела об административных правонарушениях, необходимо отказаться от субъективного усмотрения в вопросе выбора вида и размера наказания — необходимо прежде всего исходить из совокупности смягчающих и отягчающих обстоятельств, имеющихся по административному делу.

Таким образом, мы приходим к выводу, что нормы административного законодательства, устанавливающие ответственность за правонарушения в информационной сфере, характеризуются присутствием в них определенных проблем.

«В этой связи представляется необходимым проводить их дальнейшее усовершенствование с учетом практики их применения. Обязательным условием при этом является необходимость достижения гармонизации в применении норм различных отраслей права в регулировании информационных отношений, максимальное уменьшение их несбалансированности.

Решение указанных проблем — насущная потребность безопасного существования российского государства, общества и личности» [12, с. 306].

Полагаем, что для устранение выявленных проблем необходимо совершенствование системы законодательства об ответственности за информационные правонарушения должно стать создание четкого механизма регулирования информационно-коммуникационных технологий, которые выступают в качестве правовых основ для широкого использования информационных технологий в современном гражданском обществе, а также во взаимоотношениях государства с отдельно взятыми организациями и гражданами.

В настоящее время при широком использовании и повсеместном внедрении новейших информационно-коммуникационных технологий соответствующая нормативная база должна быть создана таким образом, чтобы она не только не препятствовала, но и в большей мере способствовала

усовершенствованию информационно-коммуникационных технологий в Российской Федерации.

«В части борьбы с компьютерными преступлениями, ответственность за которые установлена в УК РФ, необходимым видится создание эффективных мер по вопросам хакерства и мошенничества в компьютерных сетях.

Здесь считаем необходимым:

- обеспечить гласность и открытость разработки норм права с привлечением общественности при подготовке проектов нормативных документов и их обсуждении в информационно-телекоммуникационной сети Интернет;
- организовать системный подход, направленный на совершенствование действующего законодательства в сфере создания и последующего использования информационных ресурсов и инфраструктуры» [13, с. 325].

Реализация указанных мер и принципов, по нашему мнению, позволит создать механизм четкого и интенсивного развития информационного общества в Российской Федерации и будет способствовать развитию системы законодательства об ответственности за информационные правонарушения. Полагаем, что модернизация современного законодательства поможет решить задачу построения информационного общества, а решение данных задач должно совершенствоваться посредством:

- систематизации законодательства (приведении действующих нормативных документов в единую четко структурированную, упорядоченную и согласованную систему);
- актуализации и обновления системы законодательства (своевременное изменение и отмена устаревших актов);
- совершенствования процесса подготовки и принятия нормативных актов (законотворческие процессы должны быть прозрачными и открытыми);

– создания четкого механизма, направленного на исполнение законов и других нормативных актов. Стандартизация и лицензирование в сфере информационно-коммуникационных технологий.

Таким образом, в третьей главе исследована система законодательства об ответственности за информационные правонарушения. Выявлены отдельные несоответствия норм законодательства и их неэффективность применения к постоянно меняющимся мошенническим схемам в информационном пространстве.

В данной главе рассмотрены основные видны ответственности, закрепленные в законодательной базе.

В третьей главе существенное внимание уделено проблемам института ответственности за информационные правонарушения, угрожающие национальной безопасности. Выявлены основные векторы, способствующие развитию системы законодательства, учитывающей развитые цифровые и информационно-телекоммуникационные технологии.

Заключение

В первой главе выпускной квалификационной работы исследованы теоретические аспекты информационных правонарушений как угрозы национальной безопасности. В частности, в данной главе изучены правовые основы национальной безопасности. Раскрыт основные документы, затрагивающие вопросы обеспечения национальной безопасности РФ.

В данной главе существенное внимание уделено исследованию понятия информационных нарушений, выделению их основных видов и классификаций. Следует отметить, что на основании проведенного исследования в первой главе определено влияние информационных правонарушений на национальную безопасность страны.

Существенное внимание уделено интересам России в области обеспечения информационной безопасности, раскрыты потенциальные угрозы, которые могут быть реализованы в случае реализации информационных правонарушений.

Проведенное исследование показало, что главной целью обеспечения национальной безопасности выступает поддержание состояния защищенности всех важных интересов личности, общества, государства, которые обеспечивают благоприятные условия для жизни.

В Конституции РФ применяется понятие «безопасность», которая в общем смысле рассматривается как национальная безопасность, так она заложена в основу других видов безопасности, охватывающих конституционно-правовые отношения.

В этой связи большинство положений, раскрываемых в Конституции РФ можно отнести как к основе национальной безопасности. Именно они затрагивают ключевые общественные отношения, защита которых входит в задачи обеспечения национальной безопасности.

К важному документу в правовых основах по обеспечению национальной безопасности относится Стратегия о национальной

безопасности РФ. При этом, обеспечение национальной безопасности невозможно без защиты информационного пространства и усиления информационной безопасности страны.

В результате исследования установлено, что правонарушение представляет собой юридический факт, действия, противоречащие нормам права.

При этом, информационным правонарушениям характерны общие и специальные признаки, имеющие существенное значение для данного класса правонарушений.

Правонарушения относятся к юридическим фактам. Неправомерные действия в информационной области могут нести отрицательные последствия для граждан, общества и государства в целом.

В условиях цифровизации национальная безопасность не представляется возможной без усиленной защиты информационной безопасности гражданина, населения и государства.

За последние несколько лет произошло существенное изменение мира. Это связано с расширением цифровой трансформации, появлением новых телекоммуникационных связей, финансовых трансакций, распространение Интернета.

Соответственно такие условия увеличивают доступность третьих лиц к различной личной, коммерческой информации, что вызывает определенные угрозы и риски нарушения национальной безопасности.

Усиление защиты интересов личности и общества, которая выражается в сохранности информации защите от несанкционированного доступа к ней является важнейшей задачей для обеспечения национальной безопасности.

В результате исследования установлено, что распространение различных финансово-хозяйственных операций через сеть Интернет спровоцировало появление новых видов угроз и рисков, которые напрямую влияют на национальную безопасность.

К числу таких угроз можно отнести хакерские атаки, внедрение вирусных программ в государственные цифровые системы, разведывательные операции со стороны иностранных государств, нанесение урона путем реализации информационной войны против государства, блокирование программ и систем социально-значимых объектов и др.

Процесс защиты информационной безопасности характеризуется непрерывным взаимосвязанным применением превентивным и оперативных мер, направленных на обеспечение национальной безопасности. К таким мерам можно отнести:

- технические, а именно в области контроля над информацией в сети Интернет, импортозамещения программного обеспечения;
- организационные, в том числе направленные на разработку и принятие соответствующих нормативных документов;
- меры, производимые в сфере защиты национальных систем от хакерских атак;
- аналитические, проводимые обществом и государством;
- пропагандистские, реализуемые как на международном, так и на внутреннем уровне;
- меры, обеспечивающие информационную безопасность на международном уровне;
- кадровые, позволяющие обеспечить квалифицированных специалистов в области IT-безопасности и др.

Вышеперечисленные меры не являются исчерпывающими. Они должны обеспечивать минимизацию новых вызовов и угроз в информационной сфере.

Во второй главе выпускной квалификационной работы рассмотрена классификация информационных правонарушений, угрожающих национальной безопасности. В данной главе исследованы информационные преступления, представлены основные статьи, устанавливающие уголовную ответственность за такие преступления. Особое внимание уделено изучению

административных и гражданско-правовых информационных правонарушений.

Указаны меры административных наказаний правонарушения в информационном пространстве. Во второй главе раскрыты дисциплинарные информационные правонарушения, изучены видны дисциплинарных наказаний за такие правонарушения.

В результате исследования выявлено, что безустанное распространение информационных технологий, формирование единого мирового информационного пространства сформировали возможность делового сотрудничества, общения людей по всему миру.

При этом, возникает острая проблема в том, что в настоящее время отсутствует законодательное регулирование информационного пространства как в пределах отдельно взятой страны, так и на мировом уровне. Это породило множество разных видов преступлений в информационной среде.

Необходимо отметить, что преступления в информационной сфере могут наносить огромный ущерб не только отдельным гражданам, но и организациям, государственным структурам.

Тем самым, такие преступления могут оказывать негативное влияние на развитие отдельных отраслей, в целом экономику страны, национальную безопасность государства.

Как показывает практика, преступления, которые совершаются в информационно-телекоммуникационной сфере очень сложно раскрыть и доказать при судебном рассмотрении.

Примерами могут выступать факты звонков мошенников, которые представляются сотрудниками правоохранительных органов и требуют раскрыть персональные данные, данные об открытых счетах в банках, затем добиваются перевода денежных средств путем обмана на их счета. Бывают инциденты, когда злоумышленники направляют сообщения своим жертвам о необходимости срочно перечислить денежные средства за родственника, попавшего в беду.

Новая сфера информационного пространства не могла обойтись без преступлений. В этой связи стали появляться новые виды преступлений, такие как:

- IT-преступления;
- киберпреступность.

Проведенное исследование показало, что за последние годы большая часть финансовых преступлений совершается с использованием электронных платежных систем в информационном пространстве. Это порядка 10000 преступлений в год.

Кроме вышеуказанных, большое распространение получают преступления, связанные с неправомерным доступом к информации, а также разработкой и распространением вредоносных компьютерных программ.

Дестабилизация работы информационной структуры негативно влияет на функционирование государственных систем управления, что напрямую нарушает национальную безопасность страны и общества.

Консервативные взгляды нормотворческих органов формируют позитивную основу для последующего распространения преступлений с информационной среде.

По-нашему мнению, сократить преступления в информационной среде можно только с помощью комплексного механизма, учитывающего интересы всех стран и охватывающего информационное пространство.

В третьей главе выпускной квалификационной работе исследована система законодательства об ответственности за информационные правонарушения.

Выявлены отдельные несоответствия норм законодательства и их неэффективность применения к постоянно меняющимся мошенническим схемам в информационном пространстве.

В данной главе рассмотрены основные видны ответственности, закрепленные в законодательной базе.

В третьей главе существенное внимание уделено проблемам института ответственности за информационные правонарушения, угрожающие национальной безопасности. Выявлены основные векторы, способствующие развитию системы законодательства, учитывающей развитые цифровые и информационно-телекоммуникационные технологии.

Проведенное исследование показало, что за правонарушения в информационной среде может наступать:

- уголовная ответственность;
- административная ответственность;
- дисциплинарная ответственность.

Меры наказания за преступления в информационной среде закреплены в УК РФ. В зависимости от видов информационных преступлений меры наказаний могут отличаться.

Однако проведенное исследование показало, что в настоящее время возникаю значительные сложности в расследовании информационных преступлений.

Кроме этого, ответственность за многие преступления в информационной среде не раскрываются в нормах законодательства. Это связано с тем, что неустанно развиваются цифровые технологии, создавая не только возможности для совершения различных финансово-хозяйственных операций, но провоцирующих появление новых видов преступлений.

Как было отмечено ранее за административные информационные правонарушения наступает административная ответственность, которая регулируется КоАП РФ.

За административные информационные нарушения КоАП РФ предусмотрены такие меры наказания, как:

- предупреждение;
- административный штраф;
- конфискация орудия совершения или предмета административного правонарушения;

– административный арест и др.

Важно понимать, что стремительное развитие сети интернет, широкое применение информационно-телекоммуникационных технологий не только в повседневной жизни, бизнес-среде, но и в управлении государством создает новые угрозы национальной безопасности.

В современных условиях процессы, происходящие внутри государства тесно взаимосвязаны с глобальной интеграцией в общемировую информационную сферу.

Влияние факторов мирового информационного пространства происходит ежедневно.

Следствием такого влияние является распространение информации, которая не всегда может отражать реальную действительность.

Кроме этого возрастают факты распространения информации, имеющей агрессивную, противоречивую направленность, носящую скрытый негативный подтекст.

Все эти обстоятельства отрицательно влияют на стабильность в обществе, создавая определенный дисбаланс, что создает угрозу национальной безопасности страны.

Следует осознавать, что в современных условиях создается противоречивая обстановка, при которой происходят процессы трансформации информационного общества.

В настоящее время особую угрозу может вызывать информационная война, которая не только дестабилизирует государственную систему, но и может запустить волну общественного протеста. Все это может быть спровоцировано злоумышленниками, имеющими цель нарушить национальную безопасность отдельно взятой страны.

В этой связи остаются нерешенными вопросы обеспечения действенной правовой охраны информационной среды, установления разных мер юридической ответственности за совершение преступлений в

информационном пространстве и с использованием цифровых и информационно-телекоммуникационных технологий.

Проведенное исследование позволило установить, что современная правовая система в области защиты от информационных правонарушений является не до конца развитой. Она не учитывает скорость совершенствования цифровых технологий и быстроту появления новых мошеннических схем в области информационного пространства.

При этом возникают существенные проблемы привлечения к ответственности за совершенные преступниками информационные правонарушения.

Отсутствуют адекватные реальным условиям меры защиты граждан и государства от несанкционированного доступа к конфиденциальной личной и государственной информации.

Принимая во внимание вышеуказанные особенности необходимо понимать, что регулирование интернет-взаимоотношений посредством различных механизмов и законодательных мер является проблематичным и не всегда возможным в практике. В первую очередь, это связано с отсутствием проработанной законодательной базы, затрагивающую информационную среду. В этой связи представляется необходимым системно провести изменения в соответствующих нормах законодательства с учетом специфики отношений и возможностей информационного пространства.

Таким образом, в результате проведенного исследования достигнута целью выпускной квалификационной работы и решены все поставленные задачи.

Список используемой литературы и используемых источников

1. Ажибеков М.К. Угрозы безопасности в информационной сфере. Наука, новые технологии и инновации Кыргызстана. 2021.№ 6. С. 30-35.
2. Аношкина, А. А. Информационный терроризм как угроза национальной безопасности / А. А. Аношкина. — Текст: непосредственный // Молодой ученый. — 2020. — № 20 (310). — С. 245-247. — URL: https://moluch.ru/archive/310/70172/ (дата обращения: 13.09.2022).
3. Бартош А. А. Эволюция стратегии национальной безопасности России [Электронный ресурс] // Научная электронная библиотека elibrary/ru. URL: https://elibrary.ru/item.asp?id=26331085 (дата обращения: 25.08.2022).
4. Бойкова А.В. анализ преступлений с использованием информационных технологий и мер противодействиям. Индустриальная экономика. 2021. № 5-12. С. 1158-1161.
5. Бородин К.В. Объекты и субъекты правового регулирования борьбы с распространением вредной информации в сети Интернет // Информационное право. 2016 № 2 С. 13–17.
6. Вепрев С.Б., Нестерович С.А. Динамика преступлений, совершаемых в сфере новых информационных технологий. Расследование преступлений: проблемы и пути их решения. 2019. № 2 (24). С. 55-60.
7. Гребеньков А.А. Информационные преступления и ведение информационной войны: уголовно-правовое противодействие. Законность и правопорядок в современном обществе. 2016. № 31. С. 119-123.
8. Григорьев О.В. К вопросу о реализации административной ответственности за правонарушения в информационной сфере. Символ науки: международный научный журнал. 2022. № 1-1. С. 38-41.
9. Гриняев С.Н., Мареев П.Л., Медведев Д.А. Национальная безопасность России: сущность, виды, понятийный аппарат / Российский государственный университет нефти и газа (НИУ) имени И.М. Губкина. — М.: АНО ЦСОиП, 2021 — 172 с.

10. Джафарова Н.Т. Административно-правовое регулирование отношений, складывающихся в интернет-пространстве / Н.Т. Джаварова // Юридическая наука и правоохранительная практика. - 2020. №4. - С.74-81.

11. Дубровин И. Р., Дубровин Е. Р. Современная система национальной безопасности Российской Федерации [Электронный ресурс] // Сайт Военное обозрение. URL: https://topwar.ru/159640-sovremennaja-s istema-nacionalnoj-b ezopasnosti-rossijskoj- federacii-i-ee.html (дата обращения: 12.07.2022).

12. Золоева З.Т., Золоев С.Т. Экстремизм в интернете - проблема информационного общества : в сборнике: молодые ученые в решении актуальных проблем науки. Материалы VIII Международной научно-практической конференции. 2018. С. 305-307.

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

14. Ким В. О. Проблемы национальной безопасности на современном этапе развития общества // Философия права. 2017. №3 (82). URL: https://cyberleninka.ru/article/n/problemy-natsionalnoy-bezopasnosti-na-sovremennom-etape-razvitiya-obschestva (дата обращения: 28.06.2022).

15. Кодекс Российской Федерации об административных правонарушениях" от 30.12.2001 N 195-ФЗ (ред. от 24.09.2022)

16. Комаров А.А. О критериях общественной опасности, преступлений в сфере высоких технологий // Актуальные вопросы права, экономики и управления: сборник статей IX МНПК. Пенза, 2017. С. 243-245.

17. Курбенков В.А., Ушкань А.В Некоторые аспекты выявления информационных следов преступлений, совершаемых с использованием информационных технологий. Научный альманах. 2019. № 1-1 (51). С. 80-83.

18. Лапин Ю.С. Понятие права граждан на информацию [Электронный ресурс] / Ю.С. Лапин. – Режим доступа: URL:

https://cyberleninka.ru/article/n/ponyatie-prava-grazhdan-na-informatsiyu/viewer (дата обращения: 17.08.2022).

19. Лохбаум В.А.Типологизация административных наказаний за правонарушения в информационном пространстве. Вестник ГОУ ДПО ТО "ИПК и ППРО ТО". Тульское образовательное пространство. 2020. № 2. С. 104-111.

20. Мамцов К.Г., Ачилов Н.Р. Киберпреступность как угроза национальной безопасности // Молодой исследователь Дона. 2022. №1 (34). URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-ugroza-natsionalnoy-bezopasnosti (дата обращения: 13.09.2022).

21. Мельничук М.А. Актуальные тенденции правового регулирования доступа к информации в России и за рубежом [Электронный / М.А. Мельничук. – Режим доступа: URL: file:///C:/Users/%D0%92%D0%BB%D0%B0%D0%B4/Downloads/aktualnye-tendentsii-pravovogo-regulirovaniya-dostupa-k-informatsii-v-rossii-i-za-rubezhom%20(3).pdf (дата обращения: 23.08.2022)

22. Новиков В.К., Голубчиков С.В., Троицкая М.Ю., Сербин М.В., Баранова А.В. Дисциплинарная ответственность за нарушение законодательства в области защиты информации. Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. 2018. № 4. С. 162-165.

23. Овсянникова Т.А., Пещеров Г.И Проблема преступлений в области информационных технологий в условиях современного информационного пространства. Современное уголовно-процессуальное право - уроки истории и проблемы дальнейшего реформирования. 2020. Т. 2.№ 1 (2). С. 88-92.

24. Осенькина К.В., Ширманов Е.В. К вопросу о привлечении к административной ответственности за правонарушения в информационной сфере. В сборнике: Актуальные проблемы уголовного права и процесса, уголовно-исполнительного права и криминалистики. Материалы VIII научно-

практической конференции. Редколлегия: Г.П. Кулешова [и др.]. 2019. С. 162-167.

25. Пименов А.Н Проблемы государственного регулирования в области информации, защиты информации и противодействия информационным угрозам. Современный ученый. 2022. № 2. С. 302-304.

26. Прокопенко А.Н., Старостенко И.Н Основные направления международного сотрудничества России в области противодействия преступности в социальных сетях. Проблемы правоохранительной деятельности. 2018. № 4. С. 53-59.

27. Романова Е.А., Головнин О.К. Обеспечение производства по делам об административных правонарушениях в автоматизированной информационной системе. В сборнике: XIV КОРОЛЁВСКИЕ ЧТЕНИЯ. Сборник трудов международной молодежной научной конференции, посвящённой 110-летию со дня рождения академика С. П. Королёва, 75-летию КуАИ-СГАУ-СамГУ-Самарского университета и 60-летию со дня запуска первого искусственного спутника Земли: в 2 томах. 2017. С. 93-94.

28. Савенкова Д.Д. Правовое обеспечение информационной безопасности в российской федерации и развитие института ответственности за правонарушения в информационной сфере. В сборнике: Динамика институтов информационной безопасности. Правовые проблемы. Сборник научных трудов. Отв. ред. Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. 2018. С. 118-124.

29. Суханов А.Г. Положения по совершенствованию административной ответственности за правонарушения в информационной сфере / А.Г. Суханов // Национальная безопасность России: актуальные аспекты. - 2019. С. 65-68.

30. Талагаева Е.В., Губайдуллина Э.Х. Преступления в информационной сфере. В сборнике: Инновационные технологии в образовании и науке. Сборник материалов Международной научно-

практической конференции. В 2-х томах. Редколлегия: О.Н. Широков [и др.]. 2017. С. 232-235.

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

32. Трудовой кодекс Российской Федерации" от 30.12.2001 N 197-ФЗ (ред. от 14.07.2022) (с изм. и доп., вступ. в силу с 25.07.2022)

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

34. Усмонова, Н. Р. Правовое обеспечение национальной безопасности Российской Федерации / Н. Р. Усмонова. - Текст: непосредственный // Молодой ученый. - 2018. - № 44 (230). - С. 189-191. - URL: https://moluch.ru/archive/230/53437/ (дата обращения: 13.09.2022).

35. Хохлова О.М. Общественное согласие в социально-политической сфере современного общества: монография. Красноярск: Сибирский федеральный университет, 2016. 176 с.

36. Чирков Д.К., Саркисян А.Ж. Преступность в сфере телекоммуникаций и компьютерной информации как угроза национальной безопасности страны // Russian Journal of Economics and Law. 2013. №3 (27). URL: https://cyberleninka.ru/article/n/prestupnost-v-sfere-telekommunikatsiy-i-kompyuternoy-informatsii-kak-ugroza-natsionalnoy-bezopasnosti-strany (дата обращения: 13.09.2022).

37. Шевко Н.Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юридического института МВД России. № 1 (1). Т. 1. 2016. С. 13-16.

38. Щукин В.М., Синодов И.А., Балаева Д.Р. Проблемные вопросы участия органов внутренних дел российской федерации в выявлении, предупреждении и пресечении правонарушений в информационно-телекоммуникационных сетях (включая сеть интернет), сервисах, социальных сетях, виртуальных играх, как элемента обеспечения национальной

безопасности в условиях возникновения новых угроз // Пробелы в российском законодательстве. 2020. Т. 13. № 7. С. 157-161

39. Юрченко И.А Преступления против безопасности информации, преступления против информационной безопасности, преступления информационной направленности: определение понятий. В сборнике: Уголовное право: стратегия развития в XXI веке. Материалы XIV Международной научно-практической конференции. Министерство образования и науки Российской Федерации; Московский государственный юридический университет имени О. Е. Кутафина (МГЮА). Москва, 2017. С. 477-480.

40. Moskalev G.L. Information crimes in the structureof russian extremist and terrorist criminal practice // Journal of Siberian Federal University. Humanities and Social Sciences. 2020. Т. 13. № 10. С. 1590-1599.