

МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
**«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ
Н.Г. ЧЕРНЫШЕВСКОГО»**

Кафедра теории государства и права

**Юридическая ответственность за правонарушения
в интернет-пространстве**

АВТОРЕФЕРАТ МАГИСТЕРСКОЙ РАБОТЫ

студентки 3 курса 364 группы
направления подготовки 40.04.01 «Юриспруденция»
юридического факультета
Джабраиловой Элизы Мусаевны

Научный руководитель

доцент, канд. юрид. наук, доцент

_____ 3.С. Байниязова
подпись дата

Заведующий кафедрой

теории государства и права

канд. юрид. наук, доцент

_____ Н.В. Тюменева
подпись дата

Актуальность. В настоящее время, в эпоху информационных систем и средств создания, обработки, использования и распространения информации, одной из важных задач правового государства является построение безопасного информационного общества. Те общественные отношения, которые возникают при формировании такого общества, требуют правового регулирования. Современные технологии, глобальные телекоммуникационные сети, влияющие практически на все сферы человеческой деятельности, меняют не только качество жизни людей, но и влекут за собой рост рисков и угроз в информационной сфере, несут потенциальные угрозы информационной безопасности личности, общества и государства. В то же время правовая база, которая гарантирует основные информационные права и свободы и является основой системы обеспечения информационной безопасности, во многом определяют его возможности.

Российская Федерация вместе с ведущими странами мира активно включилась в процесс построения информационного пространства, главной задачей которого является обеспечение его безопасности.

В соответствии с Указом Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы» государство определило своей целью обеспечение благоприятных условий для применения информационных и коммуникационных технологий, что также предполагает комплексное совершенствование законодательства¹. Поэтому исследование различных правовых аспектов обеспечения информационной безопасности, включая механизмов реализации юридической ответственности за правонарушения в информационном пространстве, является весьма актуальным.

Целью исследования является комплексный анализ понятия и сущности юридической ответственности, ее основных видов, рассмотрение понятий информационного пространства и интернет-пространства, а также

¹ «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы»: Указ Президента РФ от 9 мая 2017 г. № 203 // СЗ РФ. 2017. № 20. Ст. 2901.

выявление проблемных вопросов в рамках изучения механизмов юридической ответственности за правонарушения в информационной сфере. Достижение поставленной цели требует решения следующих **задач**:

1. дать определение понятия «юридическая ответственность» и рассмотреть основные ее виды;
2. исследовать признаки и принципы юридической ответственности;
3. рассмотреть понятия «интернет-пространство» и «информационное пространство» и определить их особенности;
4. проанализировать различные виды правонарушений в интернет-пространстве;
5. изучить меры юридической ответственности за правонарушения в интернет-пространстве;
6. рассмотреть вопросы профилактики правонарушений в информационном пространстве.

Объектом исследования являются общественные отношения в сфере юридической ответственности.

Предмет исследования – содержание понятия юридической ответственности, признаки, принципы и виды, а также ряд актуальных в современных реалиях вопросов применения мер юридической ответственности в информационном пространстве.

Проблемы определения особенностей противоправных деяний в информационном пространстве и выработки направлений по обеспечению мер юридической ответственности за их совершение рассматривались такими учеными, как И.Р. Бегишев, Л.Л. Бошаева, Р.И. Дремлюга, К.Н. Евдокимова, М.А. Ефремова, Л.В. Карасаева, С.И. Коданева, А.И. Коробеев, А.Н. Попов, Е.А. Русскевич, А.И. Чучаев, труды которых составили **теоретическую основу** исследования.

Нормативную основу исследования составили Конституция Российской Федерации, Уголовный Кодекс Российской Федерации, Гражданский Кодекс

Российской Федерации, федеральные законы и иные нормативные правовые акты.

Научная новизна работы заключается в том, что предлагается исследование различных видов правонарушений в информационном пространстве, теоретическое изучение которых позволит улучшить механизм применения мер юридической ответственности за их нарушение.

В работе сформулированы теоретические выводы и **положения, выносимые на защиту:**

1. обосновывается вывод о том, что институт юридической ответственности за правонарушения в информационном пространстве представляет собой сложное и многоаспектное явление;
2. правонарушения в информационной сфере имеют сложную структуру, обусловленную единством юридического, информационного и социального элементов, что предопределяет многообразие методов и средств государственного правового регулирования информационных отношений, профилактики информационных деликтов, а также разработку эффективных мер по борьбе с информационными правонарушениями;
3. доказывается, что правонарушения в интернет-пространстве совершаются преимущественно в области поиска, создания, обработки, защиты, хранения, передачи, получения и использования всевозможных знаний об окружающем мире с использованием информационных средств и технологий работы с информацией разной формы;
4. в ходе исследования были сделаны выводы о том, что правонарушения в информационном пространстве обладают общими признаками: анонимность, неперсонофицированность, высокой латентность, доступность людям невысоких социальных и возрастных возможностей, транснациональный и интеллектуальный характер,

быстрый рост и широкая распространенность данного явления в настоящее время

5. проведенный анализ законодательства в области информации позволяет заключить, что юридическая ответственность за противоправные деяния в информационной сфере, будучи системой охранительных правовых норм, представляется межотраслевым структурным образованием, гарантирующим безопасность общественных отношений в информационной сфере и направленным на защиту интересов государства, общества и отдельной личности;
6. обосновывается вывод о необходимости совершенствования уголовного законодательства, в котором должны быть представлены новые определения видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий;
7. стремительное развитие общественных отношений в сфере информационной безопасности в условиях активного становления информационного общества и возникновения новых рисков безопасного взаимодействия в интернете-пространстве определяет влияние социальных факторов на рост компьютерной преступности и появление в ближайшем будущем новых мер предупреждения преступности в интернете.

Методологическая основа исследования. Методологические способы, использованные в работе для решения поставленных задач: диалектический, системный, формально-юридический, логический, структурно-функциональный. Данные методы позволят наиболее последовательно и полно рассмотреть поставленные вопросы в рамках цели и задач исследования.

Практическая значимость исследования определяется сделанными по его итогам выводами и рекомендациями, которые могут быть использованы в вопросах правоприменения.

Структура исследования включает введение, две главы, разделенные на параграфы, заключение и список использованных источников.

Основное содержание работы

Во введении обосновывается актуальность темы исследования, определяются объект и предмет исследования, его цель и задачи, определяются методологическая и теоретическая основы работы, раскрывается научная новизна исследования, формулируются основные положения, выносимые на защиту, выявляется научная значимость работы.

В первой главе «Общая характеристика института юридической ответственности» раскрыто содержание юридической ответственности, ее признаки, принципы и основные виды.

Юридическая ответственность представляет собой предусмотренную правовыми нормами обязанность субъекта права претерпевать неблагоприятные для него последствия за совершенное правонарушение, а также меру государственного принуждения, связанную с претерпеванием виновным лишений личного или имущественного характера. Важно, что привлекать к юридической ответственности имеет право только компетентный властный субъект, наделенный соответствующими полномочиями, и привлечение к ответственности может осуществляться только в строго установленном порядке и форме.

Ответственность – это сложное и многоаспектное понятие, которое может быть представлено в виде внутренней и внешней формы. Внутренняя ответственность отражает личные ценности и убеждения, представляя собой осознание субъектом долга перед самим собой. Внешняя ответственность обусловлена социальными нормами и требованиями и подразумевает ответственность перед другими субъектами.

Применение мер юридической ответственности к нарушителям правопорядка является одним из основных способов реализации правоохранительной функции государства. Юридическая ответственность независимо от ее видов реализуется в строгом соответствии с принципами, установленными в рамках правовой системы, к которым относятся принципы законности, справедливости, обоснованности, гуманизма, целесообразности,

однократности, неотвратимости, своевременности, объективности, презумпции невиновности.

Наряду с освещением вопроса об ответственности в противоправном поведении и рассмотрением принципов юридической ответственности большое внимание в юриспруденции уделяется анализу содержания и особенностей видов юридической ответственности за правонарушения. Государственная деятельность в области применения различных видов юридической ответственности строго регламентируется действующим законодательством.

Исследователи в научных трудах отмечают несколько классификаций юридической ответственности, среди которых выделяют следующие виды юридической ответственности. По отраслевой принадлежности принято выделять уголовную, гражданскую (гражданско-правовую), конституционную, административную, дисциплинарную, материальную, налоговую, международно-правовую ответственность.

Во второй главе «Механизм реализации юридической ответственности за правонарушения в информационном пространстве» рассмотрены понятие «информационное пространство», виды правонарушений в информационном пространстве и вопросы обеспечения мер юридической ответственности за правонарушения в интернет-пространстве.

Информационное пространство, согласно Указу Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы», представляет собой совокупность информационных ресурсов, которые созданы субъектами информационной сферы, совокупность средств взаимодействия таких субъектов, их информационных систем и необходимой информационной инфраструктуры.

Важно подчеркнуть, что в нашем исследовании понятия «информационное пространство» и «интернет-пространство» являются взаимозаменяемыми. Интернет представляет собой глобальное информационное пространство, не ограниченное государственными границами

и являющееся эффективным средством доступа к информационным ресурсам и распространения массовой информации.

В процессе информатизации общества появилась новая категория правонарушений, пока не имеющая однозначного толкования. В уголовно-правовой литературе для обозначения общественно-опасных деяний, совершаемых с использованием информационных технологий, используются различные понятия: «компьютерные преступления», «преступления в сфере компьютерной информации», «интернет-преступления», «киберпреступления», «преступления в сфере обращения цифровой информации», «преступления, совершаемые в информационной среде», «преступления в сфере информационных технологий» и др.

Преступления в сфере компьютерной информации - законодательное определение преступлений, предусмотренных главой 28 УК РФ, под которыми понимаются «запрещенные уголовным законом виновные посяательства на безопасность в сфере использования компьютерной информации, причинившие существенный вред или создавшие угрозу причинения такого вреда личности, обществу или государству». К ним относятся следующие преступления: неправомерный доступ к компьютерной информации (ст. 272 УК РФ); создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ); нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ); неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

В Международной Конвенции ООН о преступности в сфере компьютерной информации утверждается необходимость сотрудничества государств в борьбе против киберпреступлений и отмечается, что для эффективного противодействия правонарушениям в сфере компьютерной информации необходимо оперативное международное сотрудничество в области уголовного права. Следует отметить, что компьютерные системы могут

выступать в качестве объекта посягательства киберпреступника и орудия совершения преступления, что позволяет проводить различия между правонарушениями, совершаемыми в информационном пространстве. Они подразделяются на 2 группы: преступления против конфиденциальности, целостности и доступности компьютерных данных и систем и правонарушения, связанные с использованием компьютерных средств.

Кроме того, в целях повышения эффективности мер по предотвращению киберпреступлений путем укрепления международного сотрудничества в этой сфере, поддержки технической помощи и создания потенциала в целях предупреждения киберпреступности, особенно в интересах развивающихся стран, 25 октября 2025 года была подписана Конвенция ООН против киберпреступности.

Необходимо отметить, что глава 28 УК РФ охватывает не весь объем общественно опасных деяний, совершаемых в информационной среде. Уголовное законодательство РФ в данном направлении не в полной мере отвечает потребностям практики. В соответствии с действующим законодательством к информационным преступлениям, помимо предусмотренных главой 28 УК РФ, следует отнести, в частности: насильственные действия сексуального характера, совершенные в информационной сфере в отношении малолетнего (ст. 132 УК РФ); нарушение тайны сообщений граждан (ст. 138 УК РФ); нарушение авторских и смежных прав (ст. 146 УК РФ); мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ); незаконное изготовление и оборот порнографических материалов или предметов (ст. 242 УК РФ); сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») (п. «б» ч. 2 ст. 228.1 УК РФ).

Значительным пробелом в УК РФ является отсутствие нормы, устанавливающей юридическую ответственность за приобретение или сбыт

цифровой информации, заведомо добытой преступным путем. В законодательстве отсутствуют какие-либо составы преступлений, связанных с совершением общественно опасных деяний при помощи искусственного интеллекта. Это может свидетельствовать о том, что законодатель не в состоянии в полной мере реагировать на стремительные изменения, происходящие в современном цифровом мире, и регулировать возникающие в результате этих изменений отношения.

Одним из главных документов, регламентирующих информационную безопасность, является Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года № 646, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Основным законом, юридически описывающим понятия и определения в области правового регулирования в сфере информации, информационных технологий, а также регулирующим отношения при осуществлении права на производство, поиск, получение и распространение информации при применении информационных технологий, является Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Нарушение требований Федерального закона «Об информации, информационных технологиях и о защите информации» влечет дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

В условиях возрастающего значения социальных сетей в процессе информирования граждан значительно увеличились и угрозы их использования в незаконных целях. Согласно ст. 3 Федерального закона от 8 августа 2024 № 303-ФЗ «О внесении изменений в Федеральный закон "О связи" и отдельные законодательные акты Российской Федерации» в случае, если объем аудитории персональной страницы превышает 10 тыс. пользователей, владелец социальной сети обязан предоставить в Федеральную службу по надзору в

сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) сведения, позволяющие его идентифицировать.

В период проведения специальной военной операции, проводятся ряд правовых мероприятий, направленных на регулирование деятельности граждан по производству, передаче и распространению информации в сети Интернет. Особое внимание со стороны государства уделяется государственному контролю за деятельностью иностранных агентов. Согласно статье 2 Федерального закона от 11 марта 2024 № 42-ФЗ «О внесении изменений в статью 11 Федерального закона «О контроле за деятельностью лиц, находящихся под иностранным влиянием» и отдельные законодательные акты Российской Федерации» запрещена «реклама в средствах массовой информации, в сообщениях и материалах средств массовой информации в информационно-телекоммуникационных сетях информационных ресурсов иностранных агентов».

В целях защиты граждан, общества и государства от правонарушителей, использующих цифровые технологии, разработки технических и правовых мер противодействия таким противоправным деяниям 30 декабря 2024 года Правительство Российской Федерации утвердило Концепцию государственной системы противодействия преступлениям, совершаемым с помощью информационно-коммуникационных технологий. Важным направлением данной работы является совершенствование уголовного законодательства, в котором должны быть представлены новые определения видов преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, а также принятие на региональном и муниципальном уровнях соответствующих целевых программ по профилактике совершаемых с помощью цифровых технологий правонарушений.

Наиболее важной проблемой борьбы с правонарушениями является их предупреждение, устранение причин и условий, порождающих вредные и опасные для общества деяния. В рамках Министерства внутренних дел выработана практика по разработке и размещению на своих персональных

сайтах специальных памяток для граждан РФ по поведению в различных жизненных ситуациях, в частности по поведению в компьютерной сети Интернет.

В связи с тем, что чаще всего жертвами интернет-преступников становятся субъекты, абсолютно не сведущие в вопросах личной кибербезопасности, становится важным проведение общей и индивидуальной виктимологической профилактики правонарушений. Необходимо организовывать регулярные профилактические беседы с подростками и пенсионерами, входящими в особую группу риска, поднимать вопросы о возможных способах совершения преступлений в Интернете.

Существенным является контроль за работой особых отделов правоохранительных органов, специализирующихся на мониторинге и расследовании преступлений, совершаемых в информационном пространстве.

В заключении подводятся итоги работы.

Юридическая ответственность решает задачи обеспечения социальной стабильности, охраны общества от преступных посягательств, упрочения государства. Кроме того, знания о понятии, признаках, видах и принципах юридической ответственности имеют исключительно важное значение для формирования правосознания юриста и его последующей практической деятельности.

Профилактика правонарушений в информационном пространстве становится задачей первостепенной важности, поскольку решение проблемы на стадии превенции может позволить существенно сократить риски и негативные последствия от совершения противоправных деяний, наносящих вред обществу. Для достижения этой цели необходимо применить целый комплекс различных мер и задействовать многие социальные институты, активно привлекать государственные и негосударственные структуры, а также укрепить межведомственное сотрудничество в данной сфере.

В работе было отмечено, что согласно сведениям Главного информационно-аналитического центра Министерства внутренних дел

Российской Федерации наблюдается рост преступлений в информационном пространстве, в связи с чем выдвигается ряд предложений по предотвращению или снижению их роста, включающие комплект мер правового, технического и образовательного характера:

1. законодательство о защите детей в интернет-пространстве – разработка нормативного правового акта, направленного на защиту несовершеннолетнего от опасного контента, ограничение доступа к сайтам с контентом сексуального насилия над детьми и пропагандой суицида;
2. повышение квалификации сотрудников правоохранительных органов в области цифровых технологий;
3. создание централизованной системы мониторинга интернет-трафика для выявления подозрительной активности и своевременного реагирования на угрозы;
4. фильтрация контента – разработка системы автоматического удаления запрещенного контента, включая экстремистские призывы, рекламу наркотических средств и детскую порнографию;
5. информационная грамотность – подготовка программ по повышению осведомленности граждан о рисках, связанные с неосторожным использованием интернета, обучение несовершеннолетних основам информационной безопасности.

Эти меры помогут создать эффективную систему профилактики и противодействия киберпреступности, обеспечивая безопасность граждан и стабильность государства в условиях активного развития цифрового общества.