На правах рукописи

Савенкова Дарья Дмитриевна

Институт юридической ответственности в системе правового обеспечения информационной безопасности в Российской Федерации

Специальность 12.00.13 – Информационное право

Автореферат диссертации
на соискание ученой степени
кандидата юридических наук

Москва – 2019

Работа выполнена на кафедре информационного права и цифровых технологий Федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)».

Научный руководитель: **Рассолов Илья Михайлович**
доктор юридических наук, доцент

Официальные оппоненты: **Ковалева Наталия Николаевна**
доктор юридических наук, профессор, Федеральное государственное бюджетное образовательное учреждение высшего образования «Саратовская государственная юридическая академия», профессор.
Жернова Влада Михайловна
кандидат юридических наук, Федеральное государственное автономное образовательное учреждение высшего образования «Южно-Уральский государственный университет (национальный исследовательский университет), доцент

Ведущая организация: Федеральное Государственное автономное образовательное учреждение высшего образования «Российский университет дружбы народов»

Защита состоится 03 октября 2019 года в 12.00 на заседании диссертационного совета Д 212.123.03, созданного на базе Московского государственного юридического университета имени О.Е. Кутафина (МГЮА) по адресу: 125993, г. Москва, ул. Садовая-Кудринская, д. 7, стр. 22, зал диссертационного совета.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)» https: https://msal.ru/content/ob-universitete/sovety/dissertatsionnye-sovety/podrobnye-svedeniya-o-zashchitakh-2019/?hash=tab3736

Автореферат разослан «_____»_____ 2019 г.

Ученый секретарь диссертационного совета
доктор юридических наук, доцент **В.Б. Агафонов**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы диссертационного исследования.

Современные информационные технологии получили широкое распространение во всех сферах человеческой деятельности, что обусловило острую необходимость не только научного осмысления того, какие последствия влечет их создание и практическое применение, но и выявление новых рисков, формирующихся в обществе, претерпевающем постоянные изменения, в условиях нарастания вызовов и угроз информационной безопасности. Защита информационного пространства от них является сегодня стратегической и ключевой задачей мировой политики в области обеспечения национальных и международных интересов государств, интеграционных объединений и союзов в контексте развития цифровых экономик. Это, в свою очередь, требует совершенствования механизмов юридической ответственности в информационной сфере.

Тенденции развития информационного общества и активной цифровой трансформации непосредственно взаимосвязаны с реализацией одного из приоритетных и стратегических направлений государственной политики Российской Федерации – обеспечением информационной безопасности от внутренних и внешних угроз таких субъектов, как личность, общество и государство, что закреплено в системе документов стратегического планирования Российской Федерации.[1]

Из указанных документов вытекают важнейшие задачи в сфере развития информационного права, его институтов, включая институт юридической ответственности, представляющий собой совокупность однородных правовых норм, связанных с формированием и обеспечением новой объективной реальности, в которой информационные потоки играют решающую экономическую, социально-

[1] См.: Доктрина информационной безопасности Российской Федерации», утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074; Стратегия национальной безопасности Российской Федерации, утв. Указом Президента РФ от 31 декабря 2015 г. № 683 // СЗ РФ. 2016. № 1 (часть II). Ст. 212; Стратегия научно-технологического развития утв. Указом Президента РФ 1 декабря 2016 г. № 642 // СЗ РФ. 2016. № 49. Ст. 6887.

культурную роль, что немаловажно в условиях роста правонарушений и их особенностей в современном цифровом обществе.

Активное развитие и применение цифровых технологий, а также ускорение цифровизации и возникновения связанных с ней общественных отношений, требует правового регулирования с целью противодействия информационным правонарушениям на территории Российской Федерации.

Очевидно, что существующее правовое регулирование в данной области не в полной мере отвечает требованиям эффективного противодействия новым вызовам и угрозам информационной безопасности, одновременно возрастающим с развитием глобального информационного общества.

Важно учитывать, что динамика роста информационных деликтов как мировая тенденция представляет угрозу информационной безопасности на национальном и международном уровнях.

Благодаря достижениям в информационной сфере последняя становится более открытой и уязвимой, что в значительной степени делает ее «благоприятной» средой для совершения правонарушений. В связи с этим на современном этапе развития постиндустриального общества необходимо развитие национальной системы, направленной на правовое обеспечение интересов личности, общества и государства, включая повышение ответственности за совершение информационных правонарушений.

Степень научной разработанности темы.

Вопросы правового обеспечения информационной безопасности выделялись исследователями на разных этапах формирования информационного права. Среди исследователей правовых проблем в указанной области, включая общие вопросы ответственности в информационной сфере, можно назвать И.Л. Бачило, Л.А. Букалерову, В.А. Копылова, П.У. Кузнецова, А.В. Морозова, М.М. Рассолова, И.М. Рассолова, Т.А. Полякову, А.А. Стрельцова, В.П. Талимончик, А.А. Фатьянова, А.А. Чеботареву и др.

Вопросам юридической ответственности посвящены работы таких ученых-правоведов, как С.Н. Братусь, А.С. Дугенец, С.Г. Келина, С.А. Комаров, М.Д. Липинский, Г.А. Прокопович, О.А. Степанов. М.Д. Шаргородский, Д.А. Шиндяпина и др.

В настоящее время отмечается тенденция проведения научных исследований, касающихся юридической ответственности, в основном по отраслевому принципу, в рамках административного, уголовного, гражданского и иных отраслей права.[2]

Представляется, что научные исследования, связанные с развитием института юридической ответственности за правонарушения в информационной сфере, в условиях перехода к цифровой экономике и необходимости защиты цифровых прав требуют интегративного, междисциплинарного подхода. Такая комплексная отрасль юридической науки, какой является информационное право, имеет свой предмет и свои методы правового регулирования, различные правовые институты, включая, как уже говорилось выше, и институт юридической ответственности за правонарушения в информационной сфере. Однако в проводившихся ранее исследованиях правовой природы информационных правонарушений не учитывался комплексный (междисциплинарный) подход с позиции информационного права к вопросам юридической ответственности, ее месте в системе правового обеспечения информационной безопасности.

В диссертационном исследовании для более четкого уяснения правовой природы правоотношений, связанных с юридической ответственностью за информационные правонарушения, обосновывается необходимость выделения их в самостоятельную группу для углубленного анализа и расширения научных знаний об их сущности и специфике, поскольку ключевые объекты и субъекты, а также средства совершения правонарушений относятся к информационной сфере

[2] См., например: Федотов О.А., Административная ответственность за правонарушения в сфере обеспечения информационной безопасности: дисс. канд. юрид. наук. М., 2003 г.; Суслопаров А.В., Информационные преступления: дисс. канд. юрид. наук. Красноярск, 2008 г.; Букалерова Л.А., Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы автореф. докт. юрид. наук. М., 2007 г.; Устьева Л.Г., Уголовная ответственность за коррупционные информационные преступления: дисс. канд. юрид. наук. Тамбов, 2010 г.; Автаева О.Ю. Гражданские правонарушения (Сущность и состав): дисс. канд. юрид. наук. М., 2004 г.

и, соответственно, информационное право должно при этом играть определяющую роль.

Для развития цифрового и информационного общества, в связи с ростом вызовов и угроз и возрастающими рисками, нужна эффективная система предупреждения информационных правонарушений, основанная на научно-методологических подходах, сформированных правовой наукой. Для выявления сущностных характеристик информационных правонарушений требуется более комплексное исследование применения отраслевых юридических методов в этой области. Указанные причины повлияли на авторскую мотивацию в выборе темы исследования и на формирование теоретических и практических предложений по развитию межотраслевого института юридической ответственности за правонарушения в области информационной безопасности в Российской Федерации.

Объектом диссертационного исследования являются общественные отношения, связанные с юридической ответственностью за правонарушения в сфере обеспечения информационной безопасности.

Предмет диссертационного исследования – совокупность правовых норм, регулирующих вопросы ответственности за правонарушения в сфере обеспечения информационной безопасности в Российской Федерации, теоретические проблемы, а также правоприменительная практика в рассматриваемой области.

Целью диссертационного исследования является теоретическое обоснование разработанных новых научных положений, связанных с закономерностями, определяющими основные направления развития института юридической ответственности за правонарушения в области информационной безопасности в условиях перехода к цифровым технологиям.

Для достижения поставленной цели необходимо решение следующих **задач исследования**:

1) проанализировать субъектный состав информационных правонарушений в области информационной безопасности и выделить его особенности

в современных условиях глобального информационного общества и цифровой экономики;

2) выявить признаки и составляющие информационного правонарушения;

3) исследовать и научно обосновать современный правовой подход к определению понятия и особенностям юридической ответственности в сфере правового обеспечения информационной безопасности;

4) обосновать межотраслевой, комплексный характер и место института юридической ответственности за правонарушения в сфере обеспечения информационной безопасности в системе информационного права;

5) раскрыть особенности правонарушений в информационной сфере, совершаемых юридическими лицами в условиях трансграничности.

Методологическую основу исследования составили общенаучные методы познания, анализ и синтез, формально-юридический, диалектический и дедуктивный методы. Сравнительно-правовой метод научного познания применялся при анализе зарубежных и российских правовых актов. Историко-правовой метод использовался для исследования изменений нормативных правовых актов, актов ненормативного характера, а также актов, утративших юридическую силу.

Теоретическую основу исследования составляют труды известных теоретиков права С.С. Алексеева, В.К. Бабаева, Н.А. Власенко, А.Б. Венгерова, В.Б. Исакова, В.П. Казимирчука, Д.А Керимова, А.В. Корнева, А.В. Малько, Г.В. Мальцева, Н.И. Матузова, М.Н. Марченко, В.Д. Перевалова, А.С. Пиголкина, В.М. Сырыха, М.М. Рассолова, Ю.А. Тихомиров, В.Ф. Яковлева и др., а также таких ученых в области информационного права, как А.Б. Агапов, Р.В. Амелин, Ю.М. Батурин, И.Ю. Богдановская, И.Л. Бачило, Е.А. Войникайнис, Е.К. Волчинская, Л.В. Воронцова, О.А. Городов, А.К. Жарова, В.А. Копылов, П.У. Кузнецов, В.Н. Лопатин, М.М. Рассолов, И.М. Рассолов, А.В. Минбалеев, А.В. Морозов, В.Б. Наумов, Т.А. Полякова, А.Г. Серго, А.А. Стрельцов, Н.И. Соловяненко, А.А. Смирнов, Э.В. Талапина, А.А. Тедеев, Л.К. Терещенко, Л.В. Филатова, А.А. Фатьянов, М.А. Федотов и др.

Кроме того, в процессе исследования использовались труды ученых в области административного и уголовного права Д.Н. Бахраха, С.Н. Братуся, В.Б. Вехова, Д.В. Винницкого, А.Г. Волеводза, Ю.В. Гаврилина, В.Е. Козлова, С.Ю. Головиной, А.И. Горева, Г.М. Денисова, В.А. Дозорцева, О.С. Иоффе, А.А. Кармолицкого, А.Н. Кокотова, В.В. Крылова, О.Е. Кутафина, А.Б. Агапова, Ю.И. Ляпунова, Г.К. Матвеева, В.И. Майорова, В.А. Мещерякова, С.М. Паршина, В.В. Поповой, А.И. Рарога, Б.В. Россинского, А.Н. Савенкова, А.П. Сергеева, В.И. Синайского, Н.С. Таганцева, Ю.А. Тихомирова, Т.Я. Хабриевой, Р.Л. Хачатурова, А.А.Чернова, Г.Ф. Шершеневича.

Диссертантом изучались и использовались работы, связанные с правовым обеспечением информационной безопасности и преступлениями в сфере компьютерной информации, П.Г. Андреева, И.Л. Бачило, Л.А. Букалеровой, Н.Н. Куняева, В.Н. Лопатина, Т.М. Лопатиной, А.В. Полушкина, Т.А. Поляковой, И.М. Рассолова, Е.В. Семизоровой, А.В. Суслопарова, Л.Г. Устьева, Л.К. Терещенко, А.И. Химченко.

Нормативная основа исследования состоит из международных правовых актов, Конституции Российской Федерации, федеральных конституционных законов, федеральных законов, включая правовые нормы административного, уголовного, гражданского, трудового, информационного и иных отраслей российского законодательства.

В рамках поставленных задач исследования был проанализирован опыт правового регулирования в рассматриваемой сфере в ряде зарубежных государств (Соединенные Штаты Америки, Китайская Народная Республика, Социалистическая Республика Вьетнам и ряд государств-участников СНГ).

В исследовании в качестве **эмпирической основы исследования** использовались информационно-аналитические и официальные статистические данные в области ответственности за информационные правонарушения и данные о состоянии преступности в информационной сфере, постановления Пленумов Верховного Суда Российской Федерации и иная судебная практика.

Научная новизна диссертационного исследования определяется межотраслевым подходом к юридической ответственности в сфере обеспечения информационной безопасности, в основу которого положены общеправовые позиции и представления, отраслевые знания, а также действующие нормы правового регулирования в информационном, гражданском, административном, уголовном, трудовом и в иных отраслях права.

Проведенный анализ процессов формирования национальных подходов к обеспечению информационной безопасности в зарубежных государствах, включая вопросы и механизмы юридической ответственности как публичного инструмента воздействия на субъекты правонарушений, позволил выявить особенности механизмов ответственности в информационной сфере.

Предложена авторская модель межотраслевого института юридической ответственности за правонарушения в сфере правового обеспечения информационной безопасности, в рамках которой помимо традиционных выделены новые механизмы ответственности, имеющие сложную правовую природу и обусловленные развитием информационных и цифровых технологий, расширением общественных отношений в данной сфере (обеспечение безопасности критической информационной инфраструктуры, новые киберугрозы и др.). Появляются особые механизмы ответственности, являющиеся по своей природе административными (в зарубежной правовой доктрине – публичными), но имеющие и информационно-правовую специфику (механизм блокирования запрещенных информационных ресурсов (сайтов) в сети Интернет).

Научная новизна содержится в выносимых на защиту теоретических и практических выводах и предложениях, в том числе информационно-правовых, направленных на совершенствование института ответственности за правонарушения в сфере информационной безопасности, а также совершенствование российского законодательства.

Результаты исследования позволили сформулировать и обосновать следующие основные **положения, выносимые на защиту:**

1. Обосновывается вывод о межотраслевом характере института юридической ответственности за правонарушения в системе правового обеспечения информационной безопасности в Российской Федерации, который предложено рассматривать как массив однородных правовых норм, объединенных базовыми категориями и понятиями информационной сферы (информация, объекты информатизации, информационные системы, сайты в информационно-телекоммуникационной сети Интернет, сети связи, информационные технологии, деятельность субъектов, связанных с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений), закрепляющих юридическую ответственность за правонарушения в области обеспечения информационной безопасности.

Правовые нормы различных отраслей, составляющие институт юридической ответственности, объединены такими базовыми категориями сферы обеспечения информационной безопасности, как: информация ограниченного доступа, персональные данные, информационные угрозы, объекты критической информационной инфраструктуры, а также деятельность субъектов, связанная с обеспечением информационной безопасности, использованием информационных технологий.

Выявлено, что нормы анализируемого межотраслевого института находят свое отражение как в отраслевых кодексах Российской Федерации, так и в базовом Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[3], а также и в других законах, регулирующих информационные отношения в области обеспечения безопасности критической информационной инфраструктуры, защиты персональных данных, деятельности средств массовой информации, связи и др.

2. Доказывается, что в системе обеспечения информационной безопасности информационные правонарушения представляют особую правовую конструкцию,

[3] СЗ РФ. 2006. № 31. (1 ч.). Ст. 3448.

выраженную в применении специальных мер принуждения в информационной сфере, таких как: блокирование информационного ресурса, сайта и информации; установление обязанностей блокирования персональных данных; признание сайта в сети Интернет копией заблокированного сайта; ограничение доступа к копии заблокированного сайта; приостановление деятельности сетевого издания и др. Закономерности развития общественных отношений в сфере информационной безопасности в условиях стремительного развития цифровых технологий определяют появление в ближайшем будущем новых мер принуждения в отношении как отдельных видов информации, так и информационных объектов, действий субъектов и др.

Предлагается понимать под блокированием информационного ресурса осуществление комплекса организационно-правовых мер для обеспечения ограничения доступа к информации, сайту или веб-сервису на основании решения уполномоченного органа или суда.

Ограничение доступа к информационным ресурсам рассматривается как мера, реализующая превентивную, карательную, охранительную и иные функции юридической ответственности.

3. Автором обосновывается, что расширение мер принуждения в информационной сфере и появление новых санкций во многом обусловлено возникновением новых специальных субъектов информационного права (роботы, автоматизированные агенты, международные компании трансграничной торговли, и др.), обладающих специальным режимом регистрации или учета, специальной правосубъектностью, набором уникальных прав и обязанностей и другими особенностями. Это позволяет законодателю создать систему мер принуждения за совершение ими правонарушений с учетом особенностей современных цифровых технологий.

4. Обоснована необходимость закрепления правового механизма мониторинга киберинцидентов и компьютерных атак для обеспечения безопасности единого пространства доверия Евразийского экономического союза. Для создания единой цифровой среды взаимодействия в рамках ЕАЭС предлагается на основе

международных соглашений создать информационную систему предупреждения и обнаружения компьютерных атак и развития механизмов взаимодействия субъектов единого пространства доверия.

Указанная система позволит реализовать такие функции, как: выявление признаков проведения компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак; прогнозирование ситуации в области обеспечения информационной безопасности ЕАЭС; осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты; организация и проведение научных исследований в сфере разработки и применения средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак.

5. В целях организационно-правового обеспечения формирования пространства доверия и обеспечения международной информационной безопасности предлагается разработка соглашения о взаимодействии государств-участников ЕАЭС и создании координационного органа в области обеспечения кибербезопасности, а также формирования единого Межгосударственного реестра правонарушений в информационной сфере государств-участников ЕАЭС.

Включение в данный реестр повлечет для субъектов в дополнение правонарушения применение дополнительных санкций, например, блокирование информационных ресурсов на территории ЕАЭС, ограничение доступа к государственным закупкам, к персональным данным граждан и т.д.

6. В целях совершенствования системы информационной безопасности от различных вызовов и угроз предлагается закрепить в информационном законодательстве принцип презумпции безопасности объектов критической информационной инфраструктуры, который устанавливает, что объекты критической информационной инфраструктуры считаются защищенными, пока организационно-правовое обеспечение безопасности указанных объектов

соответствует требованиям, закрепленным в нормативных правовых актах в сфере обеспечения информационной безопасности.

Применение данного принципа позволит обоснованно квалифицировать правонарушения в целях повышения эффективности правоприменительной практики в сфере обеспечения информационной безопасности.

7. В настоящее время за нарушение требований о безопасности критической информационной инфраструктуры Российской Федерации установлена только уголовная ответственность. Доказывается необходимость введения также административной и дисциплинарной ответственности субъектов критической информационной инфраструктуры за нарушение порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, утвержденного приказом ФСБ России от 24 июля 2018 г. № 367 «Об утверждении Перечня информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации».[4]

8. Обосновано предложение о включении в соглашения (пользовательские соглашения), заключаемые пользователями с владельцами сервисов и услуг в сети Интернет, положений, предоставляющих возможность выбора пользователем (физическим или юридическим лицом) российской юрисдикции для обеспечения своих прав и законных интересов, гарантированных российскими нормами о юридической ответственности за правонарушения в сфере обеспечения информационной безопасности.

[4] Официальный интернет-портал правовой информации URL: http://www.pravo.gov.ru, 10.09.2018 (дата обращения 10 декабря 2018 г.)

Соответствие диссертации паспорту специальности.

Данная диссертационная работа соответствует по своему содержанию пунктам 19, 25, 26, 27, 28 паспорта специальности 12.00.13 «Информационное право», рекомендованного Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ.[5]

Теоретическая и практическая значимость исследования состоит в обосновании выводов, расширяющих знания, в целях развития теоретико-практических конструкций юридической ответственности за правонарушения в сфере информационной безопасности.

Выводы и предложения, сделанные в исследовании и содержащие концептуальные, теоретические и прикладные положения, могут быть использованы в нормотворческом процессе, в том числе при формировании концепций проектов нормативных правовых актов, касающихся правового обеспечения информационной безопасности, а также рекомендаций для государств-участников Шанхайской организации сотрудничества, БРИКС и ЕАЭС по совершенствованию правового регулирования ответственности за информационные правонарушения, кроме того, в учебном процессе и при разработке учебных курсов и научно-методических программ по информационной безопасности.

Степень достоверности и апробация результатов исследования.

Настоящая работа подготовлена на кафедре информационного права и цифровых технологий Московского государственного юридического университета им. О.Е. Кутафина (МГЮА), где она рецензировалась и обсуждалась.

---

[5] Работа соответствует следующим пунктам паспорта специальности 12.00.13 «Информационное право»: «Правовое регулирование отношений в области обеспечения информационной безопасности личности, общества и государства. Международные проблемы правового регулирования обеспечения защиты информации» (п. 19), «Ответственность за нарушения информационного законодательства. Проблемы юридической ответственности в информационном праве» (п. 26), «Проблемы международного сотрудничества в правовом регулировании и развитии информационной среды, в том числе в рамках региональных форм сотрудничества» (п. 27), «Организационно-правовые проблемы международной информационной безопасности» (п. 28), «Правовое регулирование информационных отношений, формирующихся в экономической сфере (в сфере электронной экономической деятельности, информационной экономики, электронной коммерции)» (п. 25) // URL: vak.ed.gov.ru/documents/10179/0/12.00.13.docx/c7468066-ecb0-4498-abef-00f95ef69f0f (дата обращения 10.12.2018).

Достоверность и обоснованность выводов, полученных в результате исследования, подтверждается использованием вышеуказанной методологии, изучением достаточного объема научной литературы, нормативных источников, а также оперированием эмпирическими данными (данными судебной и правоприменительной практики), исследованными автором в процессе работы над диссертацией.

Основные положения диссертационного исследования отражены в семи научных статьях, три из которых – в журналах, входящих в перечень рецензируемых научных журналов и изданий, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации (ВАК при Минобрнауки России) общим объемом (2,32 п.л.).

Отдельные положения диссертационного исследования прошли апробацию и обсуждались на международных и всероссийских научно-практических конференциях, семинарах, круглых столах, в числе которых: Круглый стол «Совершенствование деятельности подразделений предварительного следствия органов внутренних дел по расследованию преступлений в сфере компьютерной информации, совершаемых против собственности» (г. Москва, 2017 г.); Научный семинар «Научно-исследовательские проблемы противодействия экстремизму в информационном пространстве Интернета», (г. Москва, 2017 г.); Научно-методический семинар «Совершенствование методического обеспечения преподавания учебной дисциплины «Расследование преступлений в сфере компьютерной информации» (г. Москва, 2017 г.); Круглый стол «Токены и ICO в правовом поле России» (г. Москва, 2017 г.); Международная научно-практическая конференция «Современное гражданское обязательственное право и его применение в гражданском судопроизводстве» (г. Москва, 2017 г.); Всероссийский круглый стол «Актуальные вопросы обеспечения кибербезопасности» (г. Москва, 2018 г.); Международный научный семинар для молодых ученых по вопросам информационного права и правового обеспечения информационной безопасности (г. Москва, 2018 г.); Международная научно-практическая конференция «Информационное пространство: обеспечение информационной безопасности

и право» – Первые Бачиловские чтения (г. Москва, 2018 г.); Всероссийский семинар «Актуальные проблемы проведения судебной компьютерной экспертизы» (г. Москва, 2018 г.); Научно-методический семинар «Особенности расследования преступлений в сфере компьютерной информации» (г. Москва, 2018 г.); Семинар-совещание «Противодействие преступлениям, связанным с хищением электронных денежных средств, совершаемых дистанционным способом» (г. Москва, 2019 г.); Международная научно-практическая конференция «Вторые Бачиловские чтения» (г. Москва, 2019 г.).

Структура и объем диссертационного исследования определяется целью и задачами диссертационного исследования, включающего введение, три главы, заключение и библиографический список.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИОННОГО ИССЛЕДОВАНИЯ

Во введении автором обосновывается актуальность темы диссертационного исследования, определяются цель и задачи, объект и предмет исследования, анализируется степень научной разработанности темы, научная новизна, теоретическая и практическая значимость работы, раскрываются методологическая, теоретическая, нормативная и эмпирическая основы исследования, формулируются новые или содержащие элементы новизны положения, выносимые на защиту, приводятся сведения об апробации результатов и структуре диссертационного исследования.

Глава первая «Юридическая ответственность как комплексный институт правового обеспечения информационной безопасности в Российской Федерации», состоящая из четырех параграфов, раскрывает комплексный подход к институту правового обеспечения информационной безопасности в Российской Федерации на основе применения междисциплинарного подхода и анализа его особенностей с позиций информационного права.

В первом параграфе первой главы «Формирование института юридической ответственности в информационном праве» автором проведено исследование

ответственности, как общей правовой категории и отраслевых норм, связанных с юридической ответственностью за информационные правонарушения. Подчеркивается необходимость поиска новых конструкций механизмов ответственности, определения новых принципов исходя из сложности состава субъектов, необходимости обеспечения развития института юридической ответственности в области информационных правонарушений в рамках правовых систем международных и региональных интеграционных образований.

На основе вывода о комплексном характере информационного права, как отрасли права, а также анализа различных субъектов и объектов правонарушений в информационной сфере и отраслевых норм, диссертантом сделан вывод о том, что правовое обеспечение информационной безопасности имеет также комплексную природу (характер) и институт ответственности необходимо рассматривать как часть системы правового обеспечения информационной безопасности.

Во втором параграфе «Место института юридической ответственности в системе правового обеспечения информационной безопасности» автором исследуются вопросы самого содержания понятия ответственности и подходов к нему, развития учений и данного термина с позиции как теории права, философии, социологии, так и отраслевых юридических учений, и представлений. Рассмотрены законодательные подходы к сущности и к содержанию ответственности за правонарушения в инфосфере и информационной безопасности в Российской Федерации.

С позиции информационного права рассмотрены особенности субъектов данных правоотношений и на основе анализа и широкого подхода к классификации таких субъектов сделан вывод о том, что унифицированные подходы к субъектам информационных отношений и информационной безопасности на современном этапе способствуют развитию системы юридической ответственности и процессу институализации юридической ответственности в информационной сфере, а в условиях трансграничности экономики и расширения информационных потоков появляются новые субъекты информационных правоотношений, такие как международные компании трансграничной торговли, путем создания юридических

фикций с наделением их статусом субъектов правоотношений с особыми механизмами привлечения к ответственности производителей робототехники и разработчиков искусственного интеллекта.

В параграфе третьем «Особенности информационных правоотношений в сфере обеспечения информационной безопасности в Российской Федерации» проанализированы подходы к институту юридической ответственности, особенности правоотношений в сфере обеспечения информационной безопасности в Российской Федерации. Рассмотрены нормы отраслей законодательства (уголовного, гражданского, административного и трудового) и различные составы правонарушений, преступлений и проступков.

Автором отмечена тенденция усиления административной ответственности за информационные правонарушения и сделан вывод о том, что среди правовых средств, используемых для правового обеспечения юридической ответственности в области информационной безопасности, особое место занимают именно административно – юрисдикционные средства и именно в Кодексе об административных правонарушениях Российской Федерации обеспечивается информационная безопасность по целому спектру направлений.

В параграфе четвертом «Принципы юридической ответственности за правонарушения в сфере обеспечения информационной безопасности» диссертантом исследованы основные принципы юридической ответственности и отмечено, что единая система принципов информационной безопасности, как на доктринальном, так и на нормативном уровне в настоящее время не сформировалась. Проанализированы принципы информационного права, которые одновременно являются фундаментальными и универсальными для других отраслей права, к которым автор отнес: законность, равенство всех перед законом и судом, гуманизм и демократизм.

В связи с необходимостью обеспечения устойчивого развития современного мира и информационного пространства, сделан вывод о необходимости развития сотрудничества государств для создания новых правовых инструментов и механизмов с целью развития эффективной системы международной

информационной безопасности и совершенствования национального законодательства, укрепления международного сотрудничества.

Учитывая важность сферы обеспечения безопасности критической информационной инфраструктуры (далее – КИИ) Российской Федерации и защиты прав субъектов КИИ при проведении проверок, диссертантом предложено закрепить в информационном законодательстве принцип презумпции безопасности объектов КИИ, обозначающий защищенность КИИ и ее устойчивое функционирование при соответствии КИИ требованиям информационной безопасности таких объектов и соблюдении нормативных правовых актов в сфере информационной безопасности, до тех пор, пока в ходе плановых и внеплановых проверок Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК России) не выявлены нарушения и/или несоответствия требованиям безопасности.

Глава вторая диссертационного исследования «Юридическая ответственность и обеспечение информационной безопасности» состоит из трех параграфов и посвящена теоретическим, практическим и международно-правовым аспектам вопросов ответственности в сфере обеспечения информационной безопасности.

В параграфе первом главы второй «Международно-правовые аспекты обеспечения информационной безопасности» автором проанализированы основные международно-правовые подходы к обеспечению информационной безопасности с позиций информационного права и международно-правовые документы, предусматривающие противодействие использованию информационных технологий в преступных целях.

Отмечено, что: противодействие угрозам в информационном пространстве приобретает новое значение и особую актуальность в глобальном масштабе, а данное направление становится одним из приоритетных не только в национальной политике государств, но и на международном уровне; в рамках СНГ также предпринимаются меры по укреплению международного сотрудничества по противодействию информационным правонарушениям.

Среди основных угроз информационному пространству автором выделены: вирусные и троянские программы, целевые кибератаки, фишинг.

Кроме того, отмечена необходимость нормативного утверждения порядка информирования федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности значимых объектов КИИ в данной сфере в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» и Положением «Об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности» для ликвидации правовых лакун и совершенствования правового регулирования безопасности в финансово-кредитной сфере и критической информационной инфраструктуры.

В параграфе втором главы второй «Зарубежный опыт правового регулирования юридической ответственности в сфере обеспечения информационной безопасности» автором аккумулированы правовые подходы к ответственности за обеспечение информационной безопасности в таких странах, как: Республика Беларусь, Республика Узбекистан, Китайская Народная Республика (далее – КНР), Соединенные Штаты Америки (далее – США), Социалистическая Республика Вьетнам (далее – Вьетнам) и сделан вывод о том, что административно-правовые и уголовные меры ответственности, несмотря на их разнообразие становятся неотъемлемой частью нормативного правового регулирования сферы обеспечения информационной безопасности.

Как показывает сравнительно-правовой анализ подходов к вопросам юридической ответственности в сфере обеспечения информационной безопасности в Республиках Беларусь и Узбекистан, в сравнении с Российской Федерацией имеются свои особенности регулирования, например, большее количество составов преступлений в уголовном законодательстве**, иной состав диспозиций в уголовном законодательстве (кодексах).** В Республике Беларусь в настоящее время отсутствует регулирование (и нормы ответственности) отношений в области персональных данных, а Уголовный кодекс Республики Узбекистан содержит нормы ответственности за нарушение правил информатизации, которая не предусмотрена в российском уголовном законодательстве.

Как показывает анализ законодательства США, КНР и Вьетнама, необходимо уделять вниманию вопросам кибербезопасности. В последние годы в указанных странах разработаны соответствующие стратегические документы, что свидетельствует об обеспокоенности государств вопросами кибербезопасности и борьбы с киберпреступлениями. При этом в уголовном праве США отдельные составы являются более детальными по сравнению с уголовным законодательством РФ, а в Закон о кибербезопасности КНР включено 16 статей, содержащих конкретные санкции за нарушение отдельных норм в области кибербезопасности, а также предусмотрены различные механизмы санкций, среди которых: аннулирование или отзыв лицензий, конфискация незаконного дохода; приостановление деятельности; закрытие сайта.

В Законе Вьетнама «О сетевой информационной безопасности» большое внимание уделено принципам регулирования, терминам и понятиям, а нормы ответственности содержат отсылочную конструкцию, характерную для законодательств стран-участников СНГ. Опыт Вьетнама может быть применим и на территории стран СНГ, в частности Российской Федерации, поскольку структура законов является схожей, а обширный понятийный аппарат может способствовать улучшению правовых конструкций регулирования общественных отношений в сфере обеспечения информационной безопасности.

В параграфе третьем главы второй «Место и роль института юридической ответственности в системе правового обеспечения информационной безопасности в Российской Федерации» автором проанализировано содержание таких понятий, как «ответственность», «информационная безопасность», «защита информации» и обоснован вывод о том, что в условиях трансформации, происходящей в современном обществе, и в правовой системе при переходе в цифровую эпоху, некоторые вопросы по обеспечению информационной безопасности имеют потребность в системном правовом регулировании, а юридическая ответственность в области обеспечения информационной безопасности в условиях развивающейся цифровой экономики носит межотраслевой, комплексный характер и сегодня создаются предпосылки (формирование норм ответственности в различных

отраслях права, усложненный субъектный состав, расширение сфер, в которых необходимо обеспечивать информационную безопасность) даже для выделения категории «информационные правонарушения».

А обозначенные автором в рамках данного параграфа вопросы, связанные с обеспечением безопасности объектов критической информационной инфраструктуры и ответственностью в данной сфере, дополнительно подчеркивают межотраслевой характер института юридической ответственности за правонарушения в информационной сфере на современном этапе с учетом аналогичного регулирования в зарубежных странах.

При этом одним из наиболее актуальных организационно-правовых механизмов в институте юридической ответственности в информационной сфере является ограничение работы (блокирование) сайта или другого сетевого ресурса. При этом данный механизм, по мнению диссертанта, имеет сложную юридическую природу: это одновременно и превентивное средство (обеспечительная мера), и мера защиты от неправомерных действий и информации, причиняющей вред или являющейся противоправной, и санкция за совершение правонарушения.

Под блокированием сайта диссертантом предлагается понимать осуществление на основании решения уполномоченного органа или суда комплекса мер для обеспечения невозможности использования информации, сайта или веб-сервиса.

Глава третья диссертационного исследования «Развитие института юридической ответственности за правонарушения в информационной сфере в условиях «цифровизации» общества», состоящая из двух параграфов, содержит анализ и предложения по улучшению нормативного правового регулирования отношений, связанных с ответственностью в информационной сфере в условиях цифровой экономики.

В параграфе первом главы третьей «Цифровая экономика как фактор развития института юридической ответственности за правонарушения в сфере обеспечения информационной безопасности» диссертантом исследуются некоторые положения Программы «Цифровая экономика», утвержденной правительством РФ 28 июля 2017 года (утратила силу) и национальная программа «Цифровая экономика РФ»,

утвержденная президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол № 16 от 24 декабря 2018 года). Автором отмечена актуальность формирования единого пространства доверия в рамках ЕАЭС. В связи с отсутствием в указанных стратегических документах механизмов обеспечения безопасности единого пространства доверия автором предложено дополнить раздел «Информационная безопасность» национальной программы «Цифровая экономика РФ» мероприятием по созданию информационной системы предупреждения и обнаружения компьютерных атак в рамках ЕАЭС, путем подписания международных соглашений и создания механизма взаимодействия субъектов единого пространства доверия. Также в национальной программе «Цифровая экономика РФ» в разделах «Нормативное регулирование цифровой среды» и «Информационная безопасность» диссертантом предлагается предусмотреть меры (вехи), направленные на формирование пространства доверия и обеспечения международной информационной безопасности на основе единого межгосударственного реестра правонарушений в информационной сфере государств-участников ЕАЭС.

Параграф второй главы третьей «Проблемы и направления развития правового регулирования юридической ответственности за правонарушения в сфере обеспечения информационной безопасности» посвящен вопросам обеспечения суверенитета и юрисдикции в информационном пространстве.

На основе анализа подходов к суверенитету и с учетом роста информационного шума, вредоносной информации, киберугроз, угроз информационной безопасности, диссертантом предлагается создание международного механизма сотрудничества путем создания межнационального реестра вредоносной информации в рамках БРИКС, ШОС, ЕАЭС и др., а также установить определенные правила сотрудничества в глобальном информационном пространстве в области безопасности критической информационной инфраструктуры с учетом возрастающих вызовов и угроз.

Кроме того, автором диссертационного исследования на основе анализа различных пользовательских соглашений между пользователями и владельцами

сервисов и услуг в сети Интернет предложен подход, выраженный в возможности выбора пользователем (физическим или юридическим лицом) российской юрисдикции в целях защиты своих прав в сфере обеспечения информационной безопасности и применения соответствующих российских норм о юридической ответственности за правонарушения в этой сфере.

В заключении автором отражены и обобщены результаты исследования, а также высказаны предложения по совершенствованию института юридической ответственности в системе правового обеспечения информационной безопасности в Российской Федерации и их применение в научной и практической деятельности.

ПУБЛИКАЦИИ ПО ТЕМЕ ДИССЕРТАЦИИ

Статьи, опубликованные в ведущих рецензируемых научных журналах и изданиях, указанных в перечне ВАК при Минобрнауки Российской Федерации:

1) Савенкова Д.Д. «Юридическая ответственность за правонарушения в области обеспечения информационной безопасности как институт информационного права: понятие, виды, актуальные проблемы» // Образование и право, № 11, М., 2017, С. 136-144. (0.5 п.л.).

2) Савенкова Д.Д. «Кибербезопасность финансово-кредитных организаций в условиях новых вызовов и угроз в цифровом пространстве» // Право и государство: теория и практика, № 4 (160), 2018, С. 126-131. (0.25 п.л.).

3) Савенкова Д. Д. Актуальные вопросы развития института юридической ответственности в сфере обеспечения информационной безопасности в условиях цифровизации // Проблемы права № 1 (70), 2019, С. 91-95 (0.3 п.л.).

Статьи, опубликованные в иных изданиях и сборниках научных статей:

4) Савенкова Д.Д. «Актуальные проблемы юридической ответственности в сфере обеспечения информационной безопасности (понятие, основания возникновения, виды) Информационное пространство: обеспечение

информационной безопасности и право. Сб. науч. трудов / Под ред. Т.А. Поляковой, В.Б. Наумова, А.В. Минбалеева. М.: ИГП РАН, 2018, С. 474 -482 (0.5 п.л.).

5) Савенкова Д.Д. «Правовое обеспечение информационной безопасности в Российской Федерации и развитие института ответственности за правонарушения в информационной сфере» // Динамика институтов информационной безопасности. Правовые проблемы. Сб. науч. трудов / Отв. ред. Т.А. Полякова, В.Б. Наумов, Э.В. Талапина. – Москва: ИГП РАН – Издательство «Канон +» РООИ «Реабилитация», 2018, С. 118-124. (0.37 п.л.)

6) Савенкова Д.Д. «Направления взаимодействия госорганов и финансово-кредитных учреждений по противодействию киберпреступности» IT News № 05 (271) • май – июнь 2018, С. 16-17. (0.1 п.л.)

7) Савенкова Д.Д. «Противовирусное средство» для безопасности цифровой экономики // IT-WEEKLY, № 40, М. 2018, С. 14-18. (0.3 п.л.)