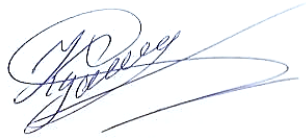
Образовательное частное учреждение высшего образования
«Международный юридический институт»

На правах рукописи



КУЛИКОВ Станислав Борисович

ПОЛИНОРМАТИВНОЕ (ПРАВОВОЕ И НЕПРАВОВОЕ) РЕГУЛИРОВАНИЕ ОТНОШЕНИЙ В КИБЕРПРОСТРАНСТВЕ: ТЕОРЕТИКО-ПРАВОВОЙ АСПЕКТ

Специальность: 5.1.1 – Теоретико-исторические правовые науки

ДИССЕРТАЦИЯ
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
Чердаков Олег Иванович

Москва – 2025

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования обусловлена спецификой устройства киберпространства, в котором наряду с информационными отношениями реализуются разнообразные экономические, политические и культурные взаимодействия, не имеющие аналогов в физической реальности. Отсутствие жестких территориальных рамок и цифровая природа коммуникаций определяют необходимость формирования принципиально новых регулятивных механизмов, соответствующих специфическим условиям виртуального пространства. Недостаточная разработанность теоретико-правовых концепций и фрагментарность действующего правового регулирования свидетельствуют о наличии правовых пробелов, препятствующих динамичному развитию инновационных форм отношений в киберпространстве, создавая угрозы правам субъектов цифрового взаимодействия и осложняя применение норм права в судебной практике.

В свете изложенного возникает целесообразность разработки системы полинормативного регулирования отношений в киберпространстве, обеспечивающей эффективное взаимодействие правовых и неправовых регуляторов.

В теоретическом аспекте система полинормативного регулирования отношений в киберпространстве способствует: а) созданию целостной теоретической модели, отражающей гибридную природу киберпространства, где право выступает не единственным, а системообразующим элементом в сложном комплексе взаимодействующих неправовых регуляторов – технических стандартов (архитектуры «кода»), рыночных механизмов и социальных норм сообществ; б) преодолению методологических ограничений традиционной мононормативной парадигмы, ориентированной, по сути, только на государственно-властное регулирование; в) обеспечению научного базиса для систематизации и анализа всего спектра регулятивных практик, выявлению закономерностей их

взаимодействия и формирования на этой основе принципов метарегулирования, посредством которых право задает целевые ориентиры и юридические рамки для функционирования иных социальных нормативов; г) расширению понятийного аппарата теории права и его объяснительного потенциала.

В практическом аспекте система полинормативного регулирования отношений в киберпространстве обеспечит: а) создание гибких регуляторных моделей, сочетающих законодательные нормы с техническими стандартами и саморегулированием, что повысит эффективность правоприменения за счет прозрачных процедур идентификации субъектов ответственности, сбора и оценки цифровых доказательств, разрешения трансграничных споров; б) минимизацию рисков для бизнеса, определяя зоны ответственности платформ, провайдеров услуг и конечных пользователей.

В этическом аспекте система полинормативного регулирования отношений в киберпространстве способствует: а) обеспечению баланса между технологической эффективностью и гуманистическими принципами; б) легитимизации этических стандартов как полноценных элементов регуляторной системы, созданию механизмов воздействия на поведение субъектов; в) противодействию технологическому детерминизму, формированию институциональных преград для реализации дискриминационных алгоритмов, манипулятивных практик и иных форм неэтичного использования цифровых технологий; г) установлению приоритета защиты человеческого достоинства и базовых прав личности перед коммерческими интересами платформ и утилитарными соображениями технической целесообразности; д) созданию основы для ответственного развития технологий, внедрения в корпоративную культуру и профессиональные стандарты принципа «этики по умолчанию» и презумпции уважения автономии цифровой личности; е) трансформации отношений в киберпространстве в социально ориентированную среду, где технологический прогресс согласуется с фундаментальными моральными ценностями и идеалами справедливого общества.

Актуальность исследования связана с необходимостью модернизации механизма правового регулирования киберпространтва, где традиционные

элементы, такие как нормы права, юридические факты, правоотношения, претерпевают объективные изменения. Нормы сталкиваются с проблемой цифровой экстерриториальности, юридические факты приобретают иную цифровую форму, а структура правоотношений усложняется за счет участия технологических посредников – алгоритмов, смарт-контрактов и прочих. Без глубокого теоретического анализа этих трансформаций невозможно выработать эффективные модели соответствующего правового воздействия.

Комплексный теоретико-правовой анализ отношений и их регулирования в киберпространстве видится своевременным и необходимым. Исследование направлено на формирование целостной системы полинормативного взаимодействия правовых и неправовых регуляторов отношений в цифровой среде, а также на разработку критериев их эффективности и границ применения. Это позволит уточнить основу построения сбалансированного механизма регулирования отношений в киберпространстве по нескольким направлениям, начиная от создания благоприятной среды для развития цифровой экономики и инноваций, через гарантии фундаментальных прав и свобод человека и заканчивая защитой государственных интересов и обеспечением цифрового суверенитета.

Степень научной разработанности темы. Логика исследования построена на классической теории государства и права, разработанной ведущими отечественными теоретиками, такими как: С. С. Алексеев, А. Б. Венгеров, В. В. Лазарев, М. Н. Марченко, Н. И. Матузов, А. В. Малько и другими, заложившими алгоритм восприятия права как основного инструмента организации общественных отношений с его специфической структурой, функциями и др. Этот подход закладывает основу выявления особенностей правовой регуляции отношений в условиях современной цифровизации и раскрывает новаторский научный взгляд, основанный на признании системы полинормативного регулирования отношений в киберпространстве, частью которой является механизм правового регулирования.

Заявленная тема в отечественной и зарубежной научной литературе исследовалась фрагментарно. Тем не менее она отражает целый пласт еще не

решенных научных задач теоретической и практической направленности. Существующие работы часто фокусируются на отдельных, узкоспециализированных вопросах, таких как защита персональных данных, интеллектуальная собственность в сети интернет, цифровые отношения в сфере киберторговли, противостояние киберпреступности и др. В итоге остаются без должного внимания фундаментальные теоретические проблемы, лежащие в основе регулирования отношений в этой цифровой сфере.

Обзор трудов, подготовленных философами и теоретиками права, позволил: а) выявить оценки специалистов качества законодательства, регламентирующего отношения в киберпространстве, установить степень пробелов и коллизий в данной сфере; б) систематизировать основные теории и концепции правовой науки относительно отношений в виртуальном пространстве; в) установить особенности юридических конструкций, используемых для описания правоотношений в названной среде; г) определить подходы учёных к решению вопросов суверенизации интернет-пространства; д) обобщить взгляды теоретиков права по вопросу влияния информационных технологий на традиционные правовые институты; е) раскрыть сущность и динамику изменения представлений о праве, собственности, личности и ответственности в киберпространстве; ж) сформулировать предложения по совершенствованию юридической базы в сфере цифрового взаимодействия.

Зарубежная наука выступила пионером в осмыслении регуляторных процессов в цифровой среде. Фундаментальной работой, заложившей основы полирегуляторной парадигмы, является труд Л. Лессига «Код и другие законы киберпространства», опубликованный в конце XX века. Он ввел концепцию четырех модальностей регулирования, которая стала отправной точкой для большинства последующих исследований. В то же время появились оппоненты названной теории, положившие начало альтернативным суждениям. Против выступали Д. Деннет, Б. Мозес, М. Кастельс, Ян ван Дейк, Ш. Зубофф, Ш. Тёркл, Т. Бёллсторф. Все названные авторы в том или ином контекстах оказали влияние на распространение полирегуляторной теории на просторах интернета.

Отечественная правовая доктрина также внесла значительный вклад в разработку проблематики, связанной с отношениями в виртуальном мире. Первыми комплексными теоретическими исследованиями стали работы специалистов, занимающихся проблемами цифрового права, включая И. Л. Бачило, Д. В. Грибанова, Л. В. Голоскокова, В. Б. Наумова, И. М. Рассолова, Э. В. Талапиной, Л. В. Терентьевой и других. Важный вклад в понимание регулирования правоотношений в цифровой среде внесли публикации А. Я. Капустина, Д. А. Пашенцева, В. Н. Синюкова, Т. Я. Хабриевой, О. И. Чердакова, Н. Н. Черногора и др.

Вместе с тем комплексные исследования, где системно анализируются теоретико-правовые основы регулирования отношений в киберпространстве, пока немногочисленны. Существующие работы, как российских, так и зарубежных авторов, часто носят узкоотраслевой характер. Они в основном концентрируются на проблемах гражданского права, таких как электронная торговля, смарт-контракты (авторы С. В. Маньшина, Е. А. Казанцева), проблемах уголовного права, посвящённых киберпреступности (авторы Т. Л. Тропинина, А. В. Геллера) или международного частного права, посвящённые, в частности, трансграничным спорам (автор Л. В. Терентьева).

Отсутствует единый общетеоретический подход, который бы системно увязывал действие правовых и неправовых регуляторов, анализировал трансформацию механизма правового регулирования и предлагал универсальные критерии оценки его эффективности в цифровой среде. Таким образом, несмотря на наличие значительного массива работ по смежным вопросам, комплексный теоретико-правовой анализ, предпринятый в настоящей диссертации, претендует на восполнение определённого раздела знаний в теории права.

Цель диссертационного исследования состоит в разработке и обосновании системы полинормативного регулирования отношений в киберпространстве, раскрытии её структуры, функций, взаимодействия правовых и неправовых компонентов, а также в преодолении традиционных представлений о механизмах регулирования отношений в цифровой среде.

Для реализации обозначенной цели необходимо решить следующие **научные задачи:**

• раскрыть периодизацию эволюции отечественной и зарубежной правовой мысли по вопросам регулирования отношений в киберпространстве; выявить ключевые этапы и доктрины, обосновать переход к системе полинормативного регулирования отношений в киберпространстве;

• содержательно охарактеризовать современную социально-правовую природу киберпространства, показать специфику правовых и неправовых регуляторов отношений в данной сфере как элементов системы полинормативного регулирования;

• идентифицировать и классифицировать неправовые регуляторы отношений в киберпространстве, определить их сущность и характер взаимодействия с правом;

• раскрыть особенности демаркации границ правового регулирования в киберпространстве, проанализировать существующие модели цифрового суверенитета, обосновать целесообразность внедрения в научный оборот понятия «цифровой государственный киберсуверенитет»;

• сформулировать авторское толкование понятия «механизм правового регулирования отношений в киберпространстве», проанализировать и показать происходящую трансформацию его структурных элементов (правовых средств, методов, процедур);

• выявить специфику действия норм права в механизме правового регулирования отношений в киберпространстве и доказать, что формы их реализации в данной сфере, включая применение, а также и толкование, претерпевают изменения, обусловленные спецификой этой среды;

• доказать, что юридические факты в киберпространстве могут существовать только в цифровой форме, которая позволяет достоверно установить их содержание, участников и момент появления;

• раскрыть особенности обеспечения реализации и защиты прав и законных интересов субъектов отношений в киберпространстве;

• показать специфику возникновения правоотношений в киберпространстве, определить их объекты и субъекты, обосновать различие в толковании понятий «отношения в киберпространстве» и «киберправоотношения», сформулировать понятия «цифровой государственный киберсуверенитет»;

• разработать систему критериев и показателей для оценки эффективности механизма правового регулирования отношений в киберпространстве, учитывающую его гибридный и технологически обусловленный характер;

• сформулировать теоретические выводы и практические рекомендации, направленные на совершенствование системы полинормативного регулирования отношений в киберпространстве;

• систематизировать наработанный научный материал в качестве предложений для повышения эффективности системы полинормативного регулирования отношений в киберпространстве.

Решение перечисленных задач способствует расширению научных представлений о регулировании отношений в киберпространстве, выявлению особенностей системы полинормативной регламентации виртуальных социальных взаимодействий и формированию практических предложений по их оптимизации.

Объектом диссертационного исследования выступают общественные отношения, складывающиеся и трансформирующиеся в киберпространстве в процессе их полинормативного (правового и неправового) регулирования.

Предмет исследования – система полинормативного регулирования, включающая механизм правового регулирования отношений (нормы права, юридические факты, правоотношения) и компоненты неправового регулирования (технические регуляторы, правила алгоритмов, социальные практики, формирующие поведение субъектов в цифровой среде, технологические протоколы, корпоративные стандарты и иные).

Методология и методы исследования. Методологическую основу диссертационного исследования составляют общенаучные, частно-научные и специальные юридические методы познания, что позволило обеспечить

всесторонность, глубину и объективность исследования сложных и многогранных процессов регулирования отношений в киберпространстве.

Диалектический метод, как всеобщий метод познания, использовался на протяжении всей работы для анализа явлений в их развитии, противоречии и взаимосвязи. Он позволил рассмотреть киберпространство не как статичную данность, а как динамично развивающуюся среду. Диалектический подход применялся для анализа сложного, противоречивого взаимодействия правовых и неправовых регуляторов, которые не просто существуют параллельно, а находятся в состоянии единства и борьбы, например, право может как вступать в конфликт с другими регуляторами, так и кооперироваться с ними, имея регулятивный приоритет.

Системно-структурный метод позволил рассмотреть механизм правового регулирования как целостную систему взаимосвязанных элементов. На его основе базируется логика построения работы: первая глава посвящена общетеоретическим основам функционирования системы в целом, а вторая фокусируется на анализе её конкретных составляющих – правовых нормах, юридических фактах и правоотношениях.

Сравнительно-правовой метод применялся для сопоставления различных правовых систем, доктрин и законодательных подходов к регулированию отношений в киберпространстве России, Китая, США, Великобритании, Бразилии, Индии и Южной Кореи. Также данный метод использовался при сравнении подходов разных юрисдикций к определению правовой природы смарт-контрактов и цифровой идентичности.

Формально-логический метод, включая приемы анализа, синтеза, индукции, дедукции, использовался для выработки понятийного аппарата, выявления внутренних противоречий в правовых конструкциях и формулирования выводов.

Историко-правовой метод был использован для изучения эволюции правовой мысли. На его основе была создана периодизация научных публикаций по теме, разделенная на четыре этапа – от середины 90-х годов XX века до первой четверти XXI века, что позволило выявить динамику смещения фокуса научного интереса.

Междисциплинарный подход стал ключевым для раскрытия природы киберпространства, поскольку его регулирование находится на стыке юриспруденции, технических наук, социологии, антропологии и экономики, этики.

Помимо названных, применялся метод правового моделирования и прогнозирования при формулировании предложений по совершенствованию законодательства и предсказании будущих тенденций в правовом регулировании отношений в киберпространстве.

Сочетание указанных методов позволило провести всесторонний и глубокий теоретико-правовой анализ предмета работы, в частности, выявить сущностные характеристики и закономерности регулирования отношений в киберпространстве, а также сформулировать обоснованные выводы и практические рекомендации.

Теоретическую основу исследования составил широкий круг научных трудов отечественных и зарубежных ученых в области теории и истории права и государства, философии права, социологии, антропологии, информационного, гражданского, уголовного и международного права.

Опорой для анализа отечественной правовой доктрины послужили труды ведущих теоретиков права, в том числе С. С. Алексеева, В. М. Баранова, А. А. Васильева, М. Н. Марченко, А. В. Малько, Н. И. Матузова, В. С. Нерсесянца и других.

Нормативно-правовую базу исследования составили международные и внутригосударственные нормативно-правовые акты. В числе международных: Устав ООН, конвенции и рекомендации международных организаций, включая «Будапештскую конвенцию о киберпреступности», документы ЮНСИТРАЛ, руководящие принципы и акты по правам человека, бизнесу и др. Использовалось законодательство ряда зарубежных стран и их объединений. Среди них нормативные правовые акты Европейского Союза GDPR, eIDAS Regulation, «Директива об авторском праве на цифровом едином рынке»; федеральные акты США – CLOUD Act, DMCA, законы отдельных штатов, законодательство Китая, Бразилии, Индии, Южной Кореи и других стран, анализируемое в контексте различных моделей киберсуверенитета.

Российское законодательство представлено Конституцией РФ, федеральными законами «Об информации, информационных технологиях и о защите информации», «О персональных данных», «О связи», «Об электронной подписи», Гражданским кодексом РФ, Уголовным кодексом РФ, подзаконными нормативно-правовыми актами.

В качестве документов стратегического планирования в работе использованы «Доктрина информационной безопасности РФ», «Стратегия развития информационного общества в РФ» и др.

Применялись акты «мягкого права»: корпоративные кодексы, отраслевые стандарты, технические регламенты, хартии и меморандумы, принятые как в России, так и за рубежом, например, такие как «Кодекс этики в сфере искусственного интеллекта», «Хартия «Цифровая этика детства» и др.

Эмпирическую базу исследования составили данные аналитических центров и международных организаций, касающиеся развития цифровых технологий, кибербезопасности и государственной политики в цифровой сфере; материалы правоприменительной практики: решения российских и зарубежных судов по спорам, связанным с отношениями в киберпространстве, в частности, дело American Civil Liberties Union v. Reno, практика административных органов Роскомнадзора, ФАС России и социологические исследования.

Научная новизна диссертационного исследования заключается в разработке системы полинормативного регулирования отношений в киберпространстве, раскрывающей метарегулятивную функцию права, устанавливающего целевые ориентиры и правовые рамки для согласованного действия технических стандартов, корпоративных правил и социальных норм. В рамках этого подхода выявлены и обоснованы ключевые трансформации классического механизма правового регулирования, обусловленные свойствами киберпространства, в частности обоснован переход от традиционной запретительной парадигмы к модели проектирования регулятивной среды, что позволило внести вклад в развитие теории права.

В работе представлена авторская классификация регуляторов, составляющих механизм правового регулирования отношений в киберпространстве, раскрыты специфика и содержание неправового регулирования, разработана модель их взаимодействия, обоснованы критерии взаимосвязи, определены границы правового и неправового регулирования отношений в цифровой среде, сформулированы принципы построения сбалансированной системы полинормативного регулирования, учитывающей необходимость защиты прав пользователей и потребности технологического развития, что позволило преодолеть фрагментарность существующих исследований и создать основу для построения системы, где право и технологии ограниченно дополняют друг друга, а не находятся в состоянии противоречия.

Научная новизна раскрывается в следующих **положениях, выносимых на защиту:**

1. Предложена авторская периодизация эволюции научных взглядов на регулирование отношений в киберпространстве, охватывающая четыре хронологических этапа: интеграционный (вторая половина 1990-х – 2007 гг.), характеризующийся адаптацией цифровых технологий к традиционным правовым институтам; социально-коммуникационный (2008 – 2013 гг.), отмеченный признанием множественности регуляторов на фоне развития социальных сетей; суверенизационный (2014 – 2019 гг.), связанный с усилением государственного регулирования отношений в киберпространстве; и технологически-трансформационный (2020 г. – по н.в.), обусловленный прорывом в области искусственного интеллекта и переходом к практическому регулированию глобальных цифровых платформ. Анализ демонстрирует трансформацию научной парадигмы от решения технико-юридических задач к осмыслению фундаментальных социально-политических проблем, что свидетельствует о переходе от попыток адаптации киберпространства к существующим правовым конструкциям к признанию формирования новой системы полинормативного регулирования, где право взаимодействует с комплексом неправовых регуляторов.

2. Доказано, что социально-правовая природа киберпространства характеризуется гибридным характером отношений, возникающих на стыке виртуальной и физической реальностей, что порождает фундаментальную правовую неопределенность статуса ключевых явлений, таких как: цифровая идентичность; системы искусственного интеллекта; киберсуверенитет, цифровая юрисдикция и иных. Эта неопределенность является главным препятствием для формирования эффективного правового регулирования. Она требует не просто адаптации отдельных норм, а изменения базовых юридических понятий (субъектность, объектность, ответственность, юрисдикция, цифровой государственный киберсуверенитет) применительно к цифровой реальности, основанной на принципах технологической нейтральности и легитимации вспомогательных неправовых инструментов для обеспечения стабильности и предсказуемости цифровых отношений.

3. Определено, что неправовые регуляторы отношений в киберпространстве являются неотъемлемыми элементами сложной системы полинормативного регулирования. Они представляют совокупность социальных норм, включая технические стандарты, рыночные механизмы и иные, не зависящие от воли государства, но оказывающие значительное воздействие на поведение пользователей в процессе цифрового взаимодействия. Их функционирование в киберпространстве имеет свою специфику. Техническая инфраструктура интернета сама по себе выступает регулятором. Протоколы связи (TCP/IP), системы адресации (DNS), стандарты шифрования, архитектура платформ – все это предопределяет возможности и ограничения действий пользователей, часто жестче, чем правовые предписания. Социальные нормы и нормы сетевой этики формируются в виртуальных сообществах (форумах, соцсетях, игровых мирах, профессиональных чатах) спонтанно, через практику взаимодействия субъектов и механизмы общественного одобрения или порицания. Они регламентируют общение, разрешение споров, определение статуса, допустимый контент.

4. Выявлена природа системы полинормативного регулирования отношений в киберпространстве, включающая сочетание различных типов регуляторов, среди

которых правовые нормы, корпоративные правила платформ и соцсетей, внутренние социальные нормы цифровых сообществ, архитектурные и технические ограничения платформ, а также экономические механизмы рынка. Все эти компоненты взаимодействуют, дополняя друг друга, обеспечивая эффективный регуляторный процесс в виртуальной среде, уравновешивая потребности в свободе, безопасности, ответственности и технологическом развитии.

5. Обосновано, что понятия «цифровой суверенитет» и «киберсуверенитет» зачастую используются как взаимозаменяемые синонимы, что ведет к размыванию их сущностного содержания и, как следствие, к неверной интерпретации. В этой связи предлагается новая дефиниция «цифровой государственный киберсуверенитет», которая выражает юридически обусловленную способность государства проецировать свою власть в цифровую среду для регулирования общественных отношений, возникающих в рамках установленной юрисдикции, с целью защиты прав и законных интересов пользователей (участников цифровых отношений). Это позволяет отражать полноту полномочий государства в цифровой среде, включая контроль, защиту и регулирование всего комплекса процессов и ресурсов, сети связи, базы данных, вычислительные мощности и системы управления. Доказано, что раскол международного сообщества на три лагеря: сторонников полной суверенизации киберпространства (Россия, Китай), адептов глобального «открытого интернета» (США, Великобритания) и государств, придерживающихся компромиссной модели киберсуверенитета, – породил дискуссию о демаркации границ правового регулирования и установлении юрисдикции в рамках виртуальной территории.

6. Выявлено консолидирующее значение механизма правового регулирования отношений (МПР) в киберпространстве, интегрирующего правовые средства, методы и процедуры, являющегося основным элементом системы полинормативного регулирования, обеспечивающим её эффективность, гарантирующим законность, безопасность и инновации в цифровом пространстве. Ключевым условием функционирования данного механизма является его постоянная адаптация к уникальным характеристикам цифровой среды, что

необходимо для сохранения баланса между защитой интересов участников виртуальных отношений, безопасностью и развитием инноваций. В современных условиях МПР трансформируется под задачи цифровой экономики, цифровой торговли и новых социальных цифровых отношений, что актуализирует поиск баланса между автоматизацией юридических процессов и сохранением человеческого контроля над принятием ключевых решений, влияющих на основополагающие права и свободы человека.

7. Доказано, что традиционные формы реализации правовой нормы как основного регулятора в киберпространстве претерпевают кардинальную трансформацию, детерминированную спецификой цифровой среды. Классические параметры действия нормы – во времени, пространстве, и по кругу лиц – фундаментально видоизменяются. Темпоральные характеристики, выраженные в мгновенности и непрерывности действий, затрудняют точную фиксацию юридически значимого момента, при этом правовые последствия могут наступать отсроченно. Экстерриториальный характер цифровых взаимодействий размывает традиционную пространственную привязку, что порождает ключевую проблему определения применимой юрисдикции. Идентификация субъектов существенно осложняется вследствие широкого применения технологий анонимизации, псевдонимизации и неверифицируемых виртуальных личностей (аватаров, никнеймов). Совокупность этих факторов свидетельствует о недостаточности классических правовых подходов и обусловливает объективную необходимость не просто адаптации отдельных норм, но и формирования системы полинормативного регулирования, способной эффективно регламентировать отношения в киберпространстве.

8. Предложено авторское толкование дефиниции «юридические факты в киберпространстве» – это конкретные действия или события, происходящие в цифровой среде, которые в силу правовых норм влекут возникновение, изменение или прекращение правоотношений и порождают соответствующие правовые последствия. Их природа может быть чисто виртуальной (отправка электронного сообщения) либо представлять собой действия в физическом мире, имеющие

последствия в цифровой среде (поломка сервера). Установлено, что юридические факты в киберпространстве влияют на создание новых правовых регуляторов и институтов, трансформируют правоприменительную практику, формируют виртуальный активизм, предоставляют новые возможности для правозащитной деятельности. Раскрыта природа действий, формирующих юридический факт в киберпространстве, и событий, составляющих основу юридического факта.

9. Доказана целесообразность введения в научный оборот понятия «виртуальная личность». Её можно рассматривать как цифровой образ, создаваемый пользователем в киберпространстве, обладающий признаками анонимности, фиктивности и не совпадающий с идентичностью физического лица-носителя. Высказано обоснованное суждение о нецелесообразности наделения «виртуальной личности» статусом самостоятельного субъекта правоотношений. Будучи лишенной собственной воли, правоспособности и дееспособности, а также существуя исключительно в зависимой от технических систем цифровой среде, она не обладает фундаментальными атрибутами правосубъектности. Таким образом, идея о придании ей юридического статуса, равно как и системам искусственного интеллекта, остается в плоскости теоретических дискуссий, не находя подтверждения ни в одной действующей юрисдикции.

10. Сформулирована дефиниция «эффективность механизма правового регулирования отношений в киберпространстве», которая рассматривается как комплексный показатель достижения целей правового воздействия на общественные отношения в цифровой среде посредством системы взаимосвязанных правовых норм, институтов, процедур и инструментов, адаптированных к особенностям виртуальной реальности. Эффективность достигается за счёт синтеза двух взаимодополняющих групп критериев оценки – юридических и технологических. Юридические критерии связаны с обеспечением формального качества, легитимностью и исполнимостью норм. Технологические критерии устанавливают практическую реализуемость, результативность правовых предписаний с помощью технических средств; определяют адаптивность правовых норм к динамичной цифровой среде.

Теоретическая значимость исследования состоит в развитии фундаментальных теоретико-правовых положений о правовом и неправовом регулировании общественных отношений в киберпространстве через обоснование использования системы полинормативного регулирования, что обусловлено специфическими свойствами динамично развивающейся виртуальной среды, объективными потребностями совершенствования и повышения эффективности названной системы, а также проблемами защиты прав пользователей в условиях формирования новых социально-правовых порядков.

Практическая значимость диссертации состоит в том, что её выводы и рекомендации могут быть использованы в нормотворческой, правоприменительной, экспертно-аналитической и образовательной деятельности для оценки и повышения эффективности регулирования отношений в киберпространстве.

В работе предложена оригинальная авторская модель цифрового государственного киберсуверенитета, построенная на разграничении ключевых подходов к его реализации в мире и выделении в его структуре технологического, информационного и юрисдикционного уровней, что позволяет комплексно оценивать и формировать национальную политику в этой сфере.

Выводы исследования могут быть полезны для судебной и иной правоприменительной практики. В частности, анализ специфики юридических фактов в киберпространстве, предоставляет правоприменителям и практикующим юристам теоретический инструментарий для правильной квалификации деяний, сбора и оценки электронных доказательств, для ориентации в сложных трансграничных спорах.

Разработанная система критериев и показателей немаловажна для осмысления эффективности правового регулирования (включая новаторское разделение на юридические и технологические показатели) и представляет собой готовый соответствующий методический инструмент. Он может быть использован регуляторами (например, Роскомнадзором, ФАС) для аудита действующих

нормативно-правовых и правоприменительных актов, планирования регуляторной политики в рассматриваемой сфере.

Анализ неправовых регуляторов (правил платформ, этических кодексов, рыночных механизмов) позволяет бизнесу лучше понимать всю сложность регуляторной среды, выстраивать стратегии и разрабатывать собственные эффективные правила саморегулирования («мягкое право»).

В образовательной и научной сферах материалы диссертации, систематизирующие эволюцию правовой мысли и предлагающие новый концептуальный подход к восприятию киберпространства, могут быть использованы при подготовке учебных курсов и пособий по «Цифровому праву», «Информационному праву», при содержательном развитии разделов «Механизм правового регулирования», «Правоотношения», «Реализация права» в курсе «Теории государства и права».

Положения и выводы диссертации способствуют развитию правосознания и правовой культуры как общего, так и профессионального уровней, в частности, расширению представлений о многообразии социальных норм, действующих в виртуальной среде, ориентируют на соблюдение законности, правомерное поведение субъектов в киберпространстве.

Степень достоверности результатов исследования обоснована актуальностью выбранной темы, целью и задачами, раскрытыми в работе, применением комплексной и адекватной предмету исследования методологии, опорой на обширную, репрезентативную и критически осмысленную базу источников, логической последовательностью и внутренней непротиворечивостью работы, а также научной новизной выводов, которые органично вытекают из проведенного исследования. Положения и выводы подкрепляются всесторонним содержательным анализом большого массива официальных и научных источников, что минимизирует риск односторонних или поверхностных заключений. Существенное значение играют материалы правоприменительной практики (решения российских и зарубежных судов, практика Роскомнадзора),

эмпирический материал аналитических центров. Это связывает теоретические построения с реальной действительностью.

Апробация результатов исследования. Основные положения и выводы диссертационной работы докладывались на международных и всероссийских научно-практических конференциях, форумах, круглых столах и научных семинарах: Общероссийский студенческий диспут «Трансформация исторических событий как технология ведения информационной войны» (Общественная палата Российской Федерации, г. Москва, 24 апреля 2020 г.); IV Международная научно-практическая конференция «Эра человека и машины: историческая динамика государственно-правовых перемен» (Московский государственный университет им. О. Е. Кутафина (МГЮА), г. Москва, 25 ноября 2022 г.); Всероссийская межвузовская научно-практическая конференция «Формирование и развитие новой парадигмы юридической науки в условиях современного общества» (Международный юридический институт, г. Смоленск, 8 декабря 2022 г.); XIII Международная научно-практическая конференция «Юридическая наука: история, современность, перспективы» (Астраханский государственный университет им. В. Н. Татищева, г. Астрахань, 10 февраля 2023 г.); Научная дискуссия «CYBERПРОСТРАНСТВО – среда информационного противостояния» (Тверской государственный университет, г. Тверь, 02 ноября 2023 г.); Конференция «Преступность XXI века: теория и практика противодействия» (Международный юридический институт, г. Москва, 25 апреля 2025 г.); Круглый стол «Искусственный интеллект: вызовы и перспективы» (РЭУ им. Г. В. Плеханова, г. Москва, 20 ноября 2025 г.); X Международный форум «Россия: образ будущего», Международная конференция «Правовая архитектура России будущего» (Финансовый университет при правительстве РФ, г. Москва, 26 ноября 2025 г.); II Всероссийская научно-практическая конференция «Научная стратегия развития Российской Федерации: политика, право, идеология» (Международный юридический институт, г. Москва, 04 декабря 2025 г.).

Материалы исследования обсуждались на кафедре теории права и государственно-правовых дисциплин, использовались при подготовке учебного

электронного курса по дисциплине «Теория государства и права», на кафедре цифрового права и информационных технологий по дисциплине «Основы информационных технологий» ОЧУ ВО «Международный юридический институт» и Высшей школе права ФГБОУ ВО «Югорский государственный университет», а так же положения работы и выводы автора внедрены в деятельность ООО «Центр по содействию бизнесу».

Результаты исследования представлены в 8 научных публикациях в рецензируемых научных изданиях, утвержденных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации. Общий объем опубликованных работ составляет 3,7 п. л.

Структура диссертации определена целью и задачами исследования. Рукопись диссертации состоит из введения, двух глав, включающих 9 параграфов заключения и списка литературы.

Глава 1 ОТНОШЕНИЯ В КИБЕРПРОСТРАНСТВЕ КАК ОБЪЕКТ СИСТЕМЫ ПОЛИНОРМАТИВНОГО РЕГУЛИРОВАНИЯ

1.1 Эволюция взглядов о регулировании отношений в киберпространстве: от традиционных правовых конструкций к полинормативной парадигме

Развитие отечественной и зарубежной юриспруденции свидетельствует о том, что традиционные теоретико-правовые конструкции, сформировавшиеся для регулирования отношений в физическом мире, оказываются недостаточными для адекватного осмысления и упорядочения уникальной среды, которой является киберпространство. Данное обстоятельство породило один из наиболее значимых вызовов для теории права, стимулировав интенсивный поиск новой регуляторной парадигмы, способной учесть специфику цифровой реальности. Анализ существующих теоретических исследований в этой области позволяет не просто обобщить накопленные знания, но и выявить ключевые этапы эволюции правовой мысли, проследить смену доминирующих доктрин и определить фундаментальные научные проблемы, которые и сегодня остаются в центре академических дискуссий.

Развитие отечественной и зарубежной юриспруденции свидетельствует о том, что цифровая трансформация общества породила принципиально новый вызов для правовой науки – необходимость осмысления регуляторных парадигм в пространстве, где традиционные юридические механизмы сталкиваются с технологическим детерминизмом, трансграничностью и спонтанно формирующимися социальными нормами. Киберпространство, возникшее как глобальная среда без физических границ, эволюционировало в сложный полирегуляторный ландшафт, где национальные законодательные системы вынуждены конкурировать с алгоритмическим управлением платформ, криптоэкономическими моделями децентрализованных автономных организаций (DAO) и этическими кодексами цифровых сообществ. Этот онтологический

дуализм – сосуществование правового поля, укорененного в Вестфальской системе государственного суверенитета, и спонтанно возникающих неправовых регуляторов – формирует эпистемологический разрыв, преодоление которого требует междисциплинарного синтеза юриспруденции, компьютерных наук, экономики и социологии, истории и философии.

Специалисты в области отраслевых правовых наук, занимающиеся киберпространством и отношениями, возникающими в виртуальной среде в последние десятилетия, подготовили множество работ, заслуживающих внимания, что позволило сформировать аналитический обзор и систематизировать контент с целью использования в данном исследовании.

Мировоззренческий подход, предложенный философами права в области киберпространства, способствует глубокому анализу современных процессов трансформации правоотношений под влиянием цифровых технологий, формируя основу для разработки адекватных юридических инструментов и нормативов, соответствующих новым реалиям XXI века. Об этом свидетельствует далеко не полный перечень диссертационных работ, приведённых в рукописи.[1]

Рассмотрение виртуальной реальности с позиций философии права позволило исследователям ответить на вопросы, каким образом классические правовые категории, такие как субъектность, объектность, ответственность, собственность и другие трансформируются в условиях цифровой реальности, описать специфику возникновения новых форм отношений по поводу цифровой

---

[1] Бондаренко Т. А. Виртуальная реальность в современной социальной ситуации: автореф. дис. … д-ра философ. наук. - Ростов-на-Дону, 2007. – 53 с.; Бодров А. А. Виртуальная реальность как когнитивный и социокультурный феномен: автореф. дис. … д-ра философ. наук. – Самара, 2007. – 34 с; Гутман И. Е. Компьютерные виртуальные игры: культурно-антропологические аспекты анализа: дис. канд. … философ. наук. – Санкт–Петербург, 2009. – 193с.; Кириллова А. А. Проблема виртуальной реальности, социально-философский аспект: автореф. дис. . канд. философ. наук. – Мурманск, 2009. – 20 с.; Ковалевская Е. В. Виртуальная реальность: философско-методологический анализ: автореф. дис. … канд. философ. наук. – Москва, 1998. – 22 с.; Малышко А. А. Философские проблемы виртуальной реальности (историко-философский аспект): автореф. дис. … канд. философ. наук. – Мурманск, 2008. – 24 с.; Опенков М. Ю. Виртуальная реальность: онто-диалогический подход: автореф. дис. … д-ра философ. наук. – Москва, 1997. – 38 с.; Орехов С. И. Виртуальная реальность: исследование онтологических и коммуникативных основ: дис. д-ра философ. наук. – Омск, 2002. – 332 с. и др.

собственности, алгоритмической ответственности, взаимодействия субъектов сетевых сообществ. Названные вопросы были раскрыты в диссертационном исследовании Н. Ю. Кликушиной.[1]

В киберпространстве зародилась новая этика поведения, нормы общения и морали, отличные от классических представлений. Философско-правовые подходы раскрывают возникновение уникальных форм отношений между людьми, корпорациями и государством в виртуальном пространстве, отражают особенности сетевого общества, что подтверждается в диссертационных исследованиях Р. И. Вылкова и С. С. Носовой.[2]

Цифровые технологии формируют иное восприятие справедливости, свободы, законности, о чём свидетельствуют разработки российских философов. Это отражается в философских дискуссиях. Названные аспекты нашли отражения в работах И. Г. Опариной, Е. Г. Цуркан, Э. В. Ходенкова.[3]

Виртуальная среда порождает специфические формы самоидентификации личности, создавая пространство для анонимности, множественности ролей и виртуальных аватаров. Эти явления требуют переосмысления личной ответственности, приватности и безопасности, что является предметом исследования и находит отражение в научных трудах философов права, в частности, Ж. Е. Вавилова.[4]

Философско-правовые работы, перечисленные выше, позволили заимствовать знания, необходимые для разработки новых и уточнения уже

---

[1] Кликушина Н. Ю. Виртуализация действительности в сознании субъекта как элемент социальной реальности: автореф. дис. … канд. философ. наук. – Омск, 2007. – 24 с.

[2] Вылков Р. И. Киберпространство как социокультурный феномен, продукт технологического творчества и проектная идея: автореф. дис. … канд. философ. наук. – Екатеринбург, 2009. – 24 с.; Носова С. С. Метаморфозы цифрового сетевого общества: социально-философский анализ: автореф. дис. … канд. философ. наук. – Томск, 2022. – 24 с.

[3] Опарина И. Г. Интернет в современном обществе: социально-философский анализ: автореф. дис. ... канд. философ. наук. – Красноярск, 2005. – 24 с.; Цуркан Е. Г. Социокультурная динамика и интернет-технологии: социально-философский анализ: дис. ... канд. философ. наук. – Москва, 2021. – 244 с.; Ходенкова Э. В. Сущность Интернета вещей: социально-философский анализ: автореф. дис. ... канд философ. наук. – Томск, 2019. – 18 с.

[4] Вавилова Ж. Е. Конструирование идентичности в условиях виртуализации общества: автореф. дис. канд. … философ. наук. – Казань, 2019. – 24 с.

имеющихся понятий, формирования научного аппарата и дефиниций, без которых невозможно раскрыть специфику правового и неправового регулирования отношений в киберпространстве.

Для системного анализа массива научного контента по исследуемой теме мы разделили его на несколько блоков. Законодательные акты и иные регулятивные документы, затрагивающие отношения в киберпространстве, вынесены непосредственно в отдельные параграфы работы и в данном обзоре фигурировать не будут.

Блоки выстроены в последовательности так, чтобы просматривалась логическая связь между научными задачами, раскрывающими отношения в киберпространстве. Первый блок включает отечественные диссертационные и монографические исследования. Во втором блоке представлены научные статьи отечественных и зарубежных авторов. В третьем блоке дана характеристика учебно-научному контенту. Данный подход позволил структурировать и обобщить доступный материал, вписывающийся в рамки темы.

Диссертационные и монографические работы, составляющие эмпирическую базу исследования, определённые в первый блок, можно разделить по тематике и отраслевому признаку.

Работы, посвящённые теоретическим вопросам права, раскрывающие специфику отношений в цифровой среде, представлены в небольшом количестве. Среди прочих выделим диссертацию Д. В. Грибанова «Правовое регулирование кибернетического пространства как совокупности информационных отношений».[1] Это одна из первых диссертационных работ выполненная по научной специальности 12.00.01 – «Теория и история права и государства; история учений о праве и государстве». В ней осуществлён анализ кибернетического пространства как уникального явления современной общественной жизни, нуждающегося в правовой организации, выявлении его информационной сущности, обосновании необходимости выделения его в качестве самостоятельного объекта правового

[1] Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: дис. ... канд. юрид. наук. – Екатеринбург, 2003. – 227 с.

регулирования, создания теоретической основы для последующих научных исследований и законодательного урегулирования.

В целом, автор исследования реализовал поставленные задачи, однако в положениях, выносимых на защиту, указал необходимость принятия «блока новых законодательных актов» и предложений по разрешению юридических проблем. Между тем он их не систематизировал и не уточнил, в какой отрасли права они должны быть реализованы.

Отметим, что В 2006 году была сделана попытка на уровне докторской диссертации сформулировать концепт модернизации российского права с учётом наступающих цифровых реалий, изменений не только экономики, но и появления нового вида общественных кибернетических отношений. Автор рукописи диссертации «Модернизация российского права: теоретико-информационный аспект» Л. В. Голоскоков[1] предложил информационную модернизацию права в контексте теории сетевого права, которую использовал как основу для решения ряда теоретических проблем. Проведённое исследование позволило расширить теоретическое содержание указанных категорий и выявить методологический потенциал для трансформации механизмов регулирования правоотношений в киберпространстве в режиме реального времени.

В рамках исследования предложена концепция модернизации правовой системы, основанная на глубокой интеграции информационно-коммуникационных технологий и права, направленная на автоматизацию процессов правотворчества и правореализации. Продемонстрирована эвристическая ценность теории сетевого права для развития отраслевых юридических наук и правовой системы в целом. В работе систематизированы и определены фундаментальные принципы, методы и структура сетевого права, а также уточнена дефиниция «метаправа».

С методологической точки зрения, метаправо интерпретируется в качестве переходного механизма к правовой системе, интегрированной с сетевыми компьютерными технологиями. Подобная интеграция детерминирует возможность

[1] Голоскоков Л. В. Модернизация российского права: теоретико-информационный аспект: дис. ... д-ра. юрид. наук. – Краснодар, 2006. – 423 с.

динамического формирования и корректировки правовых норм в режиме реального времени адекватно потребностям оперативного правового управления. Данный подход создаёт предпосылки для разработки превентивных правовых механизмов, нацеленных на минимизацию рисков возникновения кризисных ситуаций.

В исследовании детализированы механизмы автоматизированного правотворчества и правореализации. Обоснована концепция «метапаспорта» — технологического интерфейса, обеспечивающего интеграцию метаправа с актуальной правовой средой. Внедрение данного элемента предназначено для трансформации традиционной правовой системы на основе новых принципов и методов в действующее сетевое право, которое устанавливает прямую и обратную мгновенную правовую связь между индивидом (субъектом права) и институтами государственной власти.

Л. В. Голоскоков установил системные различия между традиционной и сетевой парадигмами права и предложил оптимизировать соотношение континуального и дискретного начал в праве через усиление дискретной составляющей, что соответствует фундаментальным принципам компьютерной обработки, хранения и передачи данных.

Практическая имплементация предложенной концепции предполагает реализацию следующих мер. Во-первых, рекомендуется внедрение формата дистанционного судопроизводства с обязательной цифровой фиксацией процессуальных действий. Во-вторых, предлагается принцип географического распределения судей, что позволит минимизировать риски коррупционного давления и административного влияния на локальном уровне. В-третьих, обосновывается необходимость поэтапного перехода к системе электронных расчетов с автоматизированной регистрацией транзакций. В-четвертых, акцентируется важность смещения фокуса с карательных мер на превентивные, в частности, путем разработки средств сетевого права, технологически блокирующих коррупционные операции с наличными средствами. Наконец, предлагается институционализировать и внедрить систему безопасного дистанционного электронного голосования в избирательных процессах.

Всё перечисленное отчасти уже реализовано, включая безналичные цифровые расчёты, цифровой рубль, цифровизацию судебной деятельности, дистанционное голосование и иное, что подчёркивает научную прозорливость автора. В то же время можно констатировать, что метаправо и метапаспорт представляют инструменты, способные преобразовать повседневную жизнь и бизнес-процессы, их внедрение открывает перспективные возможности, однако требует тщательной проработки нормативных документов и технологий для обеспечения максимальной безопасности и удобства пользователей.

Материалы названной докторской диссертации послужили методологическим примером для решения задач в исследовании правового и неправового механизма регулирования отношений в киберпространстве и подтолкнули к формулированию ряда новых теоретических конструкций.

Значительный вклад в отечественную теорию права внес И.М. Рассолов, диссертация которого «Право и Интернет. Теоретические проблемы»[1] способствовала развитию целого направления теории права. В представленной работе осуществлена концептуализация понятия «интернет-право», раскрыта его отраслевая специфика и идентифицированы источники. Дана развернутая характеристика информационно-правовой деятельности в сети Интернет, а также проанализирована сущность правоотношений, регламентируемых этой отраслью. В научный оборот введена и детализирована категория «интернет-отношение», проанализированы его структурные элементы: субъектный и объектный состав, субъективные права и юридические обязанности участников, а также инициирующие их юридические факты.

Автором не только определены ключевые методы и средства регулятивного воздействия в интернет-среде (правовое регулирование, саморегулирование, воздействие через нормы морали, этикета, обычаев и традиций), но и конкретизировано место интернет-права в системе права и юридических наук.

[1] Рассолов И. М. Право и Интернет. Теоретические проблемы: дис. ... д-ра. юрид. наук. – Москва, 2008. – 357 с.

Значимым результатом исследования является разработка механизма правового регулирования информационной деятельности международных организаций и формулировка основ концепции права виртуального пространства. Проведённый компаративный анализ правового опыта ряда стран (Франции, США, Великобритании, Германии и др.) позволил обосновать необходимость разработки целостной теории права виртуального пространства. В работе также освещены вопросы правосознания и правовой культуры субъектов интернет-отношений, выдвинута инициатива по разработке национального кодекса, направленного на поддержание высоких культурно-правовых стандартов в сети. Проанализированы положения законодательства об ответственности в сфере противодействия киберпреступности в свете положений Конвенции о киберпреступности; сформулированы предложения по развитию доктрины информационного права и совершенствованию уголовного законодательства в указанной сфере.

Названное исследование представляет собой одну из первых попыток научной систематизации накопленных знаний в контексте генезиса цифровой экономики и формирования нового типа виртуальных общественных отношений, что обусловило его существенный вклад в развитие общей теории права.

Необходимо отметить, что теоретические положения, разработанные И.М. Рассоловым, были критически переосмыслены, дополнены и интегрированы в контекст диссертационного исследования с учетом новейших достижений правовой науки в данной области

Работа Р. Ф. Азизова «Правовое регулирование в сети Интернет: сравнительно - и историко-правовое исследование»[1] представляет авторское восприятие ключевых особенностей правового регулирования отношений в сети интернет. В ней сделана попытка дополнить теоретико-правовое знание посредством выявления ключевых теоретико-правовых проблем, возникающих в связи с развитием сети интернет. Нужно констатировать, что автор решал поставленные задачи исключительно на базе своего восприятия заявленной темы.

[1] Азизов Р. Ф. Правовое регулирование в сети Интернет: сравнительно- и историко-правовое исследование: дис. ... канд. юрид. наук. – Санкт-Петербург, 2017. – 331 с.

В связи с чем возникает вопрос о правильности определения объекта и предмета исследования.

Так, например, объект исследования сформулирован как «правовые тексты, которые выступают в качестве источников, а также определяют теоретико-методологические предпосылки исследования»,[1] далее перечисляются виды этих текстов.

Предмет исследования определён в виде «системных правовых проблем правового регулирования отношений в сети интернет и, в тех случаях, где объект исследования позволяет сделать соответствующие выводы, наиболее типичные подходы их решения, а также преимущества и недостатки таких подходов».[2]

По существу, автор смешал объект научного познания (то, что изучается, т.е. отношения, система регулирования, проблемы) с источниковой – эмпирической – базой исследования (то, на основе чего изучается, – правовые тексты). Объект исследования – это то, на что направлен процесс познания, та часть объективной или субъективной реальности, которую исследователь изучает. В данном случае объектом исследования могут быть общественные отношения, складывающиеся в сети интернет и требующие правового регулирования, или само правовое регулирование этих отношений как система норм и институтов. Объект должен быть сущностным, а правовые тексты – это материал для анализа этого объекта.

Предмет исследования является конкретизацией тех сторон и свойств объекта, которые будут непосредственно анализированы. Правовые тексты (нормативно-правовые акты, судебные прецеденты, доктринальные тексты) – это источники информации об объекте исследования, материалы, на основе анализа которых делаются выводы об объекте. Предмет — это конкретный аспект, свойство, грань объекта, которая непосредственно изучается в данном исследовании.

---

[1] Азизов Р. Ф. Правовое регулирование в сети Интернет: сравнительно - и историко-правовое исследование: автореф дис. ... канд. юрид. наук. – Санкт- Петербург, 2017. – С.9.
[2] Там же.

Неточность, допущенная автором, по нашему мнению, привела к нарушению логики исследования и трудностям в понимании того, что является предметом изучения — сами тексты или регулируемые ими отношения. Полагаем, что смешение этих фундаментальных понятий указывает на методологическую ошибку автора.

Диссертация А. С. Анисимовой «Механизм правового регулирования интернет-отношений: проблемы теории и практики»[1] раскрыла авторский подход к разработке основ общетеоретической концепции механизма правового регулирования интернет-отношений и определения путей его оптимизации. Исследователь рассмотрела интернет-право как межотраслевой комплексный правовой институт, определила сущность интернет-отношений как объекта правового регулирования, сформулировала понятие механизма правового регулирования интернет-отношений, показала его структурные элементы, выявила специфические особенности, провела анализ законодательства, регулирующего интернет-отношения и определила перспективные пути его развития, предложила рекомендации по совершенствованию правовой политики.

В работе не содержится ни одного раздела, посвященного архитектуре и алгоритмам как самостоятельным элементам регулирования. Не учтена уникальная специфика самого объекта исследования киберпространства. Автор воспроизвела традиционную теоретико-правовую конструкцию механизма правового регулирования на интернет-отношения, упуская из фокуса ключевые альтернативные регуляторы, которые в киберпространстве играют не меньшую, а иногда и большую роль, чем право. Речь идет о концепции «код как закон» (Code is Law), популяризированной Лоуренсом Лессигом,[2] согласно которой архитектура сети, протоколы, алгоритмы платформ сами по себе являются мощнейшими регуляторами, устанавливающими, что возможно, а что невозможно в цифровой среде.

---

[1] Анисимова А. С. Механизм правового регулирования интернет-отношений: проблемы теории и практики: дис. ... канд. юрид. наук. – Саратов, 2019. – 222 с.

[2] Lessig, L. Code and other laws of cyberspace, Version 2.0. – New York: Basic Books. – 2006. – 391 p.

Названная работа раскрыла методологические нюансы при описании механизма правового регулирования отношений в киберпространстве, это, в свою очередь, позволило учесть, актуализировать, дополнить и разработать новые научные положения, обозначенные в нашей диссертации.

Одна из теоретических работ, подготовленная в рамках научной специальности 5.1.1. – «Теоретико-исторические правовые науки», затрагивает вопросы правового регулирования отношений, связанных с цифровизацией частной жизни.[1] Её автор, Д. А. Авдеев, предложил концепцию правового регулирования сферы частной жизни в условиях цифровизации общественных отношений. Он акцентировал внимание на подготовке предложений для юридической практики, попытался установить сущностные свойства и юридическое значение процесса цифровизации частной жизни, охарактеризовал механизм правового регулирования отношений в цифровой среде, описал его интегративную сущность, выявил основные варианты (модели) взаимодействия юридических и неюридических средств в механизме правового регулирования частной жизни, раскрыл специфику влияния цифровых технологий на правовой статус личности и гарантии обеспечения неприкосновенности частной жизни в условиях цифровизации.

В диссертации имеются как положительные моменты, так и спорные суждения. Например, размытость в разграничении «механизма правового регулирования» и «правового обеспечения». Так, вторая глава посвящена механизму, а третья глава – правовому обеспечению. В теории права эти понятия тесно связаны и могут пересекаться. Гарантии обеспечения неприкосновенности, описанные в третьем параграфе третьей главы, являются частью как механизма регулирования, так и правового обеспечения.

Тем не менее, названная диссертация, несмотря на её дискуссионность, позволила выявить некоторые важные методологические аспекты и использовать их в процессе подготовки данного исследования.

---

[1] Авдеев Д. А. Правовое регулирование отношений, связанных с цифровизацией частной жизни: дис. ... канд. юрид. наук. – Владимир, 2024. – 203 с.

Помимо теоретических трудов, раскрывающих особенности виртуальной среды и специфику отношений в киберпространстве, при подготовке данного исследования изучено значительное число диссертационных работ по гражданско-правовому блоку, затрагивающих круг отношений, связанных с правовым регулированием электронной торговли, электронных сделок, электронных договоров, смарт-контрактов, электронных документов в договорных отношениях и иных, показывающих особенность виртуальных правоотношений.[1]

Мы не будем останавливаться на подробном анализе их содержания. Выделим лишь общие тенденции, выявленные диссертантами, и при этом отметим, что тематика и круг затрагиваемых научных задач и проблем с начала двухтысячных годов и по 2025 год существенно изменились.

Если в нулевые годы диссертационные исследования затрагивали вопросы формирования национальных и международных правовых стандартов электронной торговли, включая правила идентификации сторон, признание юридической силы электронных документов, соблюдения международных обязательств, сравнения законодательства разных государств по вопросам гражданско-правовых отношений в интернет-пространстве, с акцентом на особенностях национального

[1] Симонович П. С. Правовое регулирование отношений, связанных с совершением сделок в электронных информационных сетях в России, США и ЕС: автореф. дис. ... канд. юрид. наук. – Москва, 2004. – 25 с.; Карев Я. А. Правовое регулирование использования электронных документов в договорных отношениях: автореф. дис. ... канд. юрид. наук. – Москва, 2005. – 34 с.; Красикова А. В. Гражданско-правовое регулирование электронных сделок: автореф. дис. ... канд. юрид. наук. – Волгоград, 2005. – 22 с.; Паперно Е. Л. Правовое регулирование электронной торговли в России, Германии и США: автореф. дис. ... канд. юрид. наук. – Москва, 2006. – 22 с.; Горшкова Л. В. Правовые проблемы регулирования частноправовых отношений международного характера в сети Интернет: автореф. дис. ... канд. юрид. наук. – Москва, 2005. – 30 с.; Моченов В. Ю. Правовое регулирование электронной коммерции: автореф. дис. ... канд. юрид. наук. – Москва, 2006. – 25 с.; Кулик Т. Ю. Особенности правового регулирования договоров, заключаемых в электронной форме: автореф. дис. ... канд. юрид. наук. – Краснодар, 2007. – 34 с.; Костюк И. В. Гражданско-правовое регулирование электронной торговли: дис. ... канд. юрид. наук. – Казань, 2007. – 213 с.; Миненкова Н. В. Международно-правовое и национально-правовое регулирование электронной торговли: автореф. дис. ... канд. юрид. наук. – Москва, 2008. – 26 с.; Рыков А. Ю. Гражданско-правовое регулирование сделок в глобальной компьютерной сети «Интернет»: автореф. дис. ... канд. юрид. наук. – Москва, 2009. – 30 с.; Зайнутдинова Е. В. Смарт-контракт в гражданском праве: автореф. дис. ... канд. юрид. наук. – Красноярск, 2022. – 25 с.; Якубов М. Л. Правовое регулирование отношений из «смарт-контрактов», заключаемых кредитными организациями: автореф. дис. ... канд. юрид. наук. – Москва, 2025. – 22 с. и др.

регулирования и возможности унификации законодательства в данной сфере, то после 2018 года наметилась иная тенденция. Она связана с появлением проблематики, раскрывающей специфику правоотношений, возникающих в связи с использованием систем искусственного интеллекта, робототехники, затрагивающих отношения по поводу виртуального имущества, виртуальной собственности и иных. Это свидетельствует о том, что юридическая наука следует в фарватере технологического развития.

В большинстве исследований отмечаются противоречия между традиционным правом и новыми реалиями цифровой среды, подчёркивается необходимость внесения изменений в действующие правовые конструкции.

Практически в каждой диссертации предлагается уникальный взгляд на исследуемую проблему. Например, С. В. Щёголева провела комплексный анализ мирового опыта использования цифровых подписей и сформулировала рекомендации по улучшению российского законодательства в свете передовых мировых практик. [1]

Правовые аспекты использования электронной цифровой подписи и её юридическое оформление, особенности использования в документах, международные стандарты и технологии подтверждения её подлинности раскрыты в диссертации В. И. Квашнина.[2]

В работах С. В. Маньшина и Е. А. Казанцева предложены авторские подходы к формированию теории договора применительно к электронной среде, обозначены практические меры для урегулирования конфликтов, возникающих в ходе электронной торговли.[3]

---

[1] Щёголева С. В. Законодательное регулирование использования цифровых подписей в странах с развитой рыночной экономикой: сравнительно-правовой анализ: автореф. дис. ... канд. юрид. наук. – Москва, 2011. – 23 с.

[2] Квашнин В. И. Правовые аспекты использования электронной цифровой подписи в договорных отношениях с участием предпринимателей: дис ... канд. юрид. наук. – Санкт-Петербург, 2010. – 250 с.

[3] Маньшин С. В. Гражданско-правовое регулирование применения электронно-цифровой подписи в сфере электронного обмена данными: дис. ... канд. юрид. наук. – Москва, 2001. – 200 с.; Казанцев Е. А. Гражданско-правовое регулирование договорных отношений, осложненных электронным элементом: автореф. дис. ... канд. юрид. наук. – Барнаул, 2007. – 22 с.

Анализ диссертационных работ, подготовленных в последние годы, позволил выделить некоторую тенденцию, а именно сдвиг научных интересов специалистов в области гражданско-правовых отношений к проблемам использования цифровых активов, цифровизации конкретных сфер деятельности. В качестве примеров можно привести работы П. М. Морхата,[1] А. А. Щитовой.[2]

Некоторые исследования подготовлены с учётом междисциплинарной связи – на стыке права и технологий. В качестве примеров можно привести диссертацию А. Я. Гасанова «Гражданско-правовое регулирование оказания услуг с использованием цифровых технологий»,[3] автор доказал зависимость гражданско-правовой сферы от современных технологий и отметил необходимость адаптации правовой системы к новым реалиям цифрового мира.

В диссертационной работе С. В. Никитенко «Международно-правовое регулирование использования искусственного интеллекта в области медицины»[4] раскрыты основополагающие положения специального международно-правового режима, регламентирующего отношения, связанные с разработкой и применением систем искусственного интеллекта (СИИ) в медицинской сфере. Автором идентифицированы ключевые детерминанты, влияющие на содержание международно-правовых норм, призванных упорядочить научные достижения и технологические инновации. Работа определяет международно-правовые основы обеспечения безопасности в контексте недопущения вмешательства в сферу здоровья человека и формулирует принципы использования научно-технических достижений, включая СИИ, в здравоохранении.

В числе предложенных автором условий обеспечения безопасности применения систем искусственного интеллекта в медицине — совершенствование

---

[1] Морхат П. М. Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы: автореф. дис. ... канд. юрид. наук. – Москва, 2018. – 45 с.

[2] Щитова А. А. Правовое регулирование информационных отношений по использованию систем искусственного интеллекта: автореф. дис. ... канд. юрид. наук. – Москва, 2022. – 29 с.

[3] Гасанов А. Я. Гражданско-правовое регулирование оказания услуг с использованием цифровых технологий: автореф. дис. ... канд. юрид. наук. – Москва, 2022. – 25 с.

[4] Никитенко С. В. Международно-правовое регулирование использования искусственного интеллекта в области медицины: дис. ... канд. юрид. наук. – Санкт-Петербург, 2023. – 423 с.

защиты персональных данных, усиление контроля за оборотом медицинских изделий и модификация процедуры получения информированного добровольного согласия на медицинское вмешательство. Особое внимание уделено особенностям деликтной ответственности за вред, причинённый в результате использования систем искусственного интеллекта при оказании медицинских услуг, а также сформулированы авторские подходы к решению данной правовой проблемы.

Отдельный пласт научных изысканий составляют работы, посвящённые фундаментальным дискуссионным вопросам. К числу таковых относится докторская диссертация Л. В. Терентьевой,[1] в которой проведён комплексный анализ отношений, связанных с установлением судебной юрисдикции по трансграничным частноправовым спорам в киберпространстве. Автором построена оригинальная концепция, включающая принципы, основания и условия ограничения такой юрисдикции.

В исследовании раскрыты специфические черты судебной юрисдикции по трансграничным частноправовым спорам, эксплицировано содержание адаптивного подхода к применению территориально обусловленных юрисдикционных привязок. Продемонстрирована специфика реализации территориальной и экстерриториальной юрисдикции в киберпространстве, выявлены современные тенденции в установлении судебной юрисдикции. В рамках работы также проведён анализ процедуры рассмотрения доменных споров и дана оценка перспектив имплементации национальными правопорядками специального механизма ограничительных тестов, разработанных для установления юрисдикции в отношении споров, возникающих в киберпространстве.

Названная диссертация послужила примером логического построения научного контента и формирования понятийного аппарата.

Так как в рукописи нашего исследования затронуты некоторые аспекты, связанные с отношениями в сфере кибербезопасности, защите прав пользователей,

[1] Терентьева Л. В. Судебная юрисдикция по трансграничным частноправовым спорам в киберпространстве: автореф. дисс. … докт. юрид. наук. – Москва, 2021. – 61 с.

считаем целесообразным представить анализ диссертационных работ, подготовленных по уголовному праву и криминологии. Их можно разделить на несколько блоков. Прежде всего, в их числе работы, затрагивающие проблемы, связанные с экономическими преступлениями, совершаемыми в киберпространстве; диссертации, раскрывающие вопросы уголовно-правовой защиты авторских прав в виртуальном мире; исследования, посвящённые уголовно-правовой защите от деструктивного интернет-контента и иные.

Можно констатировать, что одной из первых диссертаций, посвящённых киберпреступности, была работа Т. Л. Тропининой.[1] Автор сформулировала дефиницию «киберпреступность», отграничив её от понятия «компьютерная преступность», выявила и охарактеризовала криминологические значимые признаки, раскрыла проблемы уголовно-правовой борьбы на международном и национальном уровнях. Одновременно показана степень общественной опасности киберпреступлений, проанализированы меры уголовно-правовой борьбы с ними, разработаны предложения, направленные на повышение эффективности уголовно-правового регулирования и совершенствования уголовного законодательства.

Учитывая, что рукопись готовилась в начале двухтысячных годов, а защита диссертации состоялась в 2005 году, работа отражала острые проблемы того периода, не теряющие актуальности по сей день. При этом можно отметить, что диссертационное исследование кажется незавершённым из-за отсутствия параграфа о профилактике киберпреступлений, а тема профилактической работы в виртуальной среде автором практически не затрагивалась.

Работа А. В. Геллера[2] заслуживает отдельного внимания, так как автор попытался сформулировать концепт обеспечения уголовно-правовой защиты электронной информации и интернета. Диссертант провёл уголовно-правовой и криминологический анализ компьютерных преступлений и на его основе

---

[1] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. ... канд. юрид. наук. – Владивосток, 2005. – 26 с.

[2] Геллер А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: автореферат дис. ... канд. юрид. наук. – Москва, 2006. – 24 с.

разработал меры по предупреждению компьютерной преступности, внёс предложения по совершенствованию уголовного законодательства как одного из средств предупреждения киберпреступности, раскрыл содержание правовой защиты информации и сущность правового воздействия на сферу интернета, проанализировал зарубежное законодательство об ответственности в сфере борьбы с преступностью в виртуальном пространстве и на его примере показал сильные и слабые стороны. В целом, содержание диссертации отражает тенденции российской уголовно-правовой политики, характерные для начала двухтысячных годов.

Среди множества работ, подготовленных по уголовно- криминологической проблематике, выделяются диссертации об уголовно-правовой защите авторских и смежных прав. Необходимо отметить, что данная тема широко исследовалась и в рамках гражданского права.

В качестве примера возьмём работы Е. В. Толстой[1] и А. И. Кананович.[2] Для обеих работ характерно то, что они были подготовлены практически в одно и то же время 2011 – 2013 годы, следовательно, отражали тенденции того времени. Однако Е. В. Толстая попыталась сформулировать теоретические выводы о составляющих уголовно-правовую характеристику посягательствах на авторские и смежные права в Рунете и разработать на их основе конкретные предложения по решению проблемы надлежащей уголовно-правовой охраны данных прав на законодательном и правоприменительном уровнях, в то время как А. И. Кананович сконцентрировалась на выработке рекомендаций по повышению эффективности российского уголовно-правового регулирования отношений по использованию авторских прав в глобальной сети Интернет, вследствие чего обе работы имеют

[1] Толстая Е. В. Посягательства на авторские и смежные права в российском сегменте сети Интернет: уголовно-правовая характеристика: автореф. дис. … канд. юрид. наук. – Москва, 2011. – 22 с.

[2] Кананович А. И. Уголовно-правовая защита авторских прав в глобальной сети интернет: на примере законодательств России и Франции: автореф. дис. ... канд. юрид. наук. – Москва, 2013. – 29 с.

принципиальные отличия, но могут быть использованы как взаимодополняющие в развитии темы обеспечения уголовно-правовой защиты авторских прав.

Помимо названных проблем по уголовно-криминологическому направлению исследовались отношения, связанные с экономическими преступлениями в киберпространстве,[1] с защитой несовершеннолетних от преступных посягательств, совершаемых с использованием сети интернет,[2] противодействия компьютерной преступности[3] и иное.

Анонсированные выше диссертации позволили накопить знания и методологический опыт для формирования научного контента в данной работе, что, с одной стороны, дало возможность определить уровень и сложность рассматриваемой нами темы, а с другой стороны, избежать повторов и констатации уже полученных результатов.

Анализ научного материала не будет исчерпывающим без учета соответствующих монографий, послуживших источником получения научной информации о правовых и неправовых регуляторах отношений в киберпространстве.

Среди множества работ выделим несколько имеющих, по нашему мнению, принципиально важное значение для осмысления парадигмы развития правовых и неправовых отношений в киберпространстве.

Отправной точкой анализа является концепция множественности регуляторов, сформулированная Лоуренсом Лессигом, согласно которой поведение в киберпространстве определяется не только законом (Law), но и

---

[1] Простосердов М. А. Экономические преступления, совершаемые в киберпространстве, и меры противодействия им: автореф. дис. ... канд. юрид. наук. – Москва, 2016. – 28 с.

[2] Кузнецова Е. В. Предупреждение делинквентного поведения несовершеннолетних, продуцируемого контентом сети интернет: автореф. дис. … канд. юрид. наук. – Курск, 2019. – 25 с.; Туркулец В. А. Защита несовершеннолетних от преступных посягательств, совершаемых с использованием сети «Интернет»: дис. ... канд. юрид. наук. – Москва, 2023. – 249 с.

[3] Евдокимов К. Н. Противодействие компьютерной преступности: теория, законодательство, практика: автореф. дис. … докт. юрид. наук. – Москва, 2022. – 73 с.; Летёлкин Н. В. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей: включая сеть «Интернет»: автореф. дис. ... канд юрид. наук. – Нижний Новгород, 2018. – 24 с.

архитектурой кодом (Architecture/Code), рынком (Market) и социальными нормами (Norms).[1]

Данная работа в среде исследователей занимающихся изучением отношений в киберпространстве, является базовой и фундаментальной, так как изменила подход к пониманию процессов регулирования в цифровой среде. Лоуренс Лессиг пришёл к выводу, что традиционное представление о праве как о единственном регуляторе является в корне неверным применительно к киберпространству. Он ввёл концепцию четырех модальностей регулирования, которые в совокупности определяют границы возможного поведения онлайн.

Закон (Law) – традиционные юридические нормы, которые угрожают санкциями за их нарушение (ex post). Его действие в киберпространстве ограничено проблемами юрисдикции и правоприменения.

Социальные нормы (Norms) – неписаные правила и обычаи, поддерживаемые сообществом. Нарушение этих норм влечет за собой социальное осуждение, остракизм.

Рынок (Market) – экономические силы, которые через цены, спрос и предложение регулируют доступ к технологиям, услугам и информации. Рынок делает определенные действия либо более дорогими, либо более дешевыми.

Архитектура, или Код (Architecture/Code), – самый важный для киберпространства регулятор. Это технические стандарты, программный код и аппаратные средства, которые создают саму среду. В отличие от закона, который можно нарушить, предписания кода часто нарушить физически невозможно. Если в коде сайта нет функции копирования текста, то пользователь (без специальных навыков) не сможет его скопировать.

Лессиг доказал, что «код – это закон». Именно архитектура определяет, будет ли киберпространство местом свободы или тотального контроля. Например, технологии шифрования создают архитектуру приватности, в то время как системы идентификации создают архитектуру контроля. Государство и корпорации могут

[1] Lessig L. Code and other laws of cyberspace, Version 2.0. – New York: Basic Books. – 2006. – 391 p.

влиять на код, чтобы достичь своих целей регулирования гораздо эффективнее, чем с помощью традиционных законов. Эта работа закладывает фундамент для понимания того, что правовые отношения в киберпространстве неразрывно связаны с его технической структурой, которая сама по себе является мощным регулятором.

Монографию И. М. Рассолова «Право и Интернет. Теоретические проблемы»[1] можно позиционировать как научный ответ Л. Лессингу. В ней сделана попытка комплексного теоретико-правового осмысления проблем, порожденных интернетом. Автор рассмотрел сущность интернет-отношений, их специфику, проблемы правового статуса субъектов и объектов, а также предложил концепцию формирования «интернет-права». Данная работа важна для понимания того, как российская доктрина начала адаптироваться к новой цифровой реальности, признавая недостаточность традиционного правового инструментария.

Учёный одним из первых обосновал идею «интернет-права» не как новой отрасли, а как комплексного межотраслевого правового института, включающего нормы конституционного, административного, гражданского, уголовного и информационного права. Он показал, что регулирование киберпространства невозможно вписать в рамки одной отрасли — это является отходом от классической парадигмы. И. М. Рассолов отметил уникальные черты интернет-отношений (виртуальность, глобальность, анонимность) и доказал, что они требуют особого механизма правового регулирования. Выявил их влияние на традиционные юридические конструкции (договор, сделку, правонарушение).

В отличие от ранних киберлибертарианских идей, И. М. Рассолов доказал объективную необходимость правового вмешательства государства для защиты прав и свобод личности, обеспечения безопасности и правопорядка в сети. Этот труд стал переходным этапом в научной мысли и обеспечил признание уникальности цифровых отношений, осознание пределов традиционного права и начало поиска новых комплексных правовых решений для их регулирования.

---

[1] Рассолов И. М. Право и Интернет. Теоретические проблемы. – М.: Норма, 2009. – 383 с.

Монография В. Б. Наумова «Право и Интернет: Очерки теории и практики»[1], наряду с монографией И. М. Рассолова, является одним из основополагающих трудов о российском «интернет-праве». Автор провёл теоретический анализ с обобщением ранней правоприменительной практики, рассмотрел и раскрыл дефиниции: доменное имя, электронная коммерция, ответственность провайдеров и юрисдикция. В работе показано, как теоретические проблемы находят отражение в конкретных практических кейсах и как формировались первые подходы к их решению.

Автор подробно исследовал и описал организационно-правовые аспекты саморегулирования и правила регистраторов доменных имен в сети интернет на примере организации ICANN. Он показал, что наряду с государственными законами в интернете действуют мощные частные и общественные регуляторы, создающие свои собственные правила. В работе детально рассматриваются сложности применения традиционного права к интернет-отношениям на примере определения юрисдикции при разрешении споров о доменных именах, показано, что традиционные подходы, основанные на физическом местонахождении ответчика, часто не работают.

В монографии уделено большое внимание техническим деталям функционирования сети (например, системе доменных имен DNS), показано, как технические особенности напрямую влияют на правовые отношения и их регулирование. Значение монографического исследования в том, что показана неразрывная связь права, техники и саморегулирования. Автор подтвердил на практике, что государственные законы – лишь один из элементов в сложной экосистеме управления интернетом.

Представляя коллективные работы, можно выделить среди прочих монографию Т. Я. Хабриевой и Н. Н. Черногора «Право в условиях цифровой реальности».[2] Данная работа Института законодательства и сравнительного

[1] Наумов В. Б. Право и Интернет: Очерки теории и практики : монография. – М.: Книжный дом «Университет», 2002. – 432 с.
[2] Право в условиях цифровой реальности: монография / отв. ред. Т. Я. Хабриева, Н. Н. Черногор. – М.: Проспект, 2020. – 368 с.

правоведения при Правительстве РФ раскрывает консолидированную точку зрения группы учёных на влияние цифровизации на различные отрасли права, государство, правосознание и правовую систему в целом. Это российский государственно-центричный подход к новой регуляторной парадигме. В работе признаются вызовы цифровизации, но решение проблемы видится через адаптацию и усиление роли государства и права.

Авторы оспаривают идеи об «отмирании» права в цифровую эпоху. Они утверждают, что право трансформируется: появляются новые объекты (цифровые права), новые субъекты, меняются правовые формы, но роль права как основного социального регулятора сохраняется и даже усиливается.

Названная работа показывает, насколько противоположны взгляды отечественных правоведов по вопросу регламентации отношений в киберсреде.

Монография «Трансграничные отношения в киберпространстве: правовое регулирование, кибербезопасность, разрешение споров»[1] представляет суждения группы исследователей о влиянии трансграничных процессов на правовые и экономические аспекты функционирования киберпространства. Особое внимание уделено вопросам трансграничной передачи и обработки персональных данных, проблемам международной юридической компетенции и разрешению споров в виртуальных средах. Коллектив авторов предложил концептуальную основу для регулирования интеллектуального права в условиях современных IT-технологий. В целом, монография повторяет уже устоявшиеся и принятые в отечественном праве каноны.

В работе «Концепция цифрового государства и цифровой правовой среды» авторский коллектив в составе М. В. Залоило, Д. А. Пашенцева, Н. Н. Черногора.[2] раскрыл вопросы трансформации государства и правовой среды под воздействием цифровых технологий. Дана характеристика «цифрового государства», «цифрового

[1] Трансграничные отношения в киберпространстве: правовое регулирование, кибербезопасность, разрешение споров : монография / Канашевский В. А., Шахназаров Б. А., Терентьева Л. В., Засемкова О. Ф. – М.: Проспект, 2024. – 136 с.

[2] Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. – М.: Инфра-М, 2022. – 244 с.

правительства», «цифрового правосудия». В монографии сделан вывод, что главный правовой регулятор отношений в киберпространстве — государство, которое само является объектом цифровой трансформации, и это кардинально меняет всю регуляторную парадигму. Авторы показывают, что право выступает не только как инструмент, с помощью которого государство регулирует цифровую среду, но и само становится объектом цифровизации. Появляются электронные нормативные акты, машиночитаемое право, автоматизированные системы правоприменения (например, камеры фиксации нарушений ПДД). Анализ платформ показывает, как архитектура и алгоритмы становятся ключевыми посредниками в правоотношениях между государством и личностью. Это не только упрощает взаимодействие, но и создает новые формы контроля и сбора данных.

В монографии раскрыто авторское видение того, как в условиях цифрового государства должны меняться гарантии прав человека, как обеспечить прозрачность и подотчетность алгоритмических решений, принимаемых государственными органами. Это попытка найти баланс между эффективностью государственного управления и защитой личности в новых реалиях отношений в киберпространстве.

Следующая коллективная работа «Трансформация права в цифровую эпоху»[1] – это сборник суждений по различным аспектам цифровизации, начиная от этических, заканчивая вызовами и рисками внедрения цифровых инструментов в жизнь общества. В монографии изложено понимание интеграции цифровых технологий в правовые и политические институты.

Исследователи отметили, что российское право до сих пор не урегулировало множество сложных отношений в интернет-среде, включая правовой режим использования криптовалюты, разность подходов российской и зарубежной судебных систем к восприятию криптовалюты. В монографии сделан акцент на амбивалентности цифровой эпохи. С одной стороны, цифровые технологии

[1] Трансформация права в цифровую эпоху: монография / Министерство науки и высшего образования РФ, Алтайский государственный университет; под ред. А. А. Васильева. – Барнаул: Изд-во Алт. ун-та, 2020. – 432 с.

повлекли за собой позитивные изменения: оперативность и трансграничность коммуникаций, сокращение издержек в производстве и государственном управлении, создание умных технологий помощи престарелым и больным людям, сокращение последствий от человеческого фактора в здравоохранении, образовании и иные. С другой стороны, цифровизация общества несет в себе риски и угрозы. В монографии предложен консервативный взгляд на перспективы цифрового развития общества. Авторский коллектив настаивает на поиске механизмов, в том числе этических и правовых, способствующих нейтрализации негативных аспектов цифровизации, таких как: проблема тотального контроля за поведением человека, риски признания правосубъектности роботов для потерпевших, вмешательство в частную жизнь человека при обработке данных, «цифровое рабство» и зависимость человека от технологий, психические последствия использования цифровых устройств, особенно несовершеннолетними, и т.п.

В целом, в работе представлено скептическое восприятие сценариев цифровизации отношений и перспективы интеграции систем искусственного интеллекта в реальную жизнь, что подтолкнуло нас к формированию некоторых суждений по поводу ускорения процессов технологического изменения отношений в реальном мире.

Анализ монографических материалов позволяет сделать вывод о том, что парадигма правового и неправового регулирования отношений в киберпространстве характеризуется следующими чертами: а) преобладанием различных способов регулирования, т.е. отношения в киберпространстве определяются отечественным и зарубежным законодательством, правилами частных платформ; нормами, установленными сетевыми сообществами и технологическими ограничениями, заложенными в коде; б) эффективностью «кода», подтверждением, что технологическая архитектура является мощным и прямым регулятором, зачастую предопределяющим возможности как государственного права, так и рыночных и социальных норм; в) существующим конфликтом интересов между правовыми и неюридическими регуляторами, когда

право может вступать в конфликт с другими регуляторами и, наоборот, кооперироваться с ними. Очевидно, что произошёл некоторый сдвиг в доктрине. Правовая наука отошла от первоначального киберлибертарианства и признала необходимость регулирования, но продолжает дискутировать о его моделях — от государственно-центричного суверенного подхода до концепций многостороннего управления и саморегулирования.

Из представленных научных суждений, изложенных в монографиях, можно сделать вывод о том, что для эффективного и сбалансированного порядка в киберпространстве недостаточно одного лишь «хорошего закона». Необходимо понимание и гармоничное управление всей сложной экосистемой регуляторов, влияющих на цифровую жизнь человека и общества.

Научные статьи отечественных и зарубежных авторов, используемые в данной работе, мы отнесли во второй аналитический блок. Они представляют основу материалов дискуссионного характера, в связи с чем их аналитический обзор интегрирован в текст, поэтому отдельный анализ считаем нецелесообразным. В то же время отметим явно просматривающуюся хронологическую неравномерность выхода публикаций, затрагивающих тему регулирования отношений в киберпространстве. Соответственно, считаем целесообразным сделать периодизацию и дать характеристику основных проблем, раскрытых в научных статьях.

В освещении темы формирования отношений в киберпространстве в научных изданиях можно выделить несколько периодов. В качестве хронологической шкалы, позволяющей сделать временные отсечки, возьмём интервал с середины 90-х годов XX века и по сей день. Почему девяностые – потому, что в эти годы началась активная интеграция интернета в социальное пространство, создавались цифровые платформы, формировались отношения в виртуальном пространстве, менялось восприятие виртуальной реальности, что привлекло внимание представителей юридического научного сообщества и стимулировало появление значительного количества научных публикаций.

На первом этапе, который мы определили в рамки второй половины 90- х гг. по 2007 год, были опубликованы научные статьи, затрагивающие тему интернета как новой социальной реальности, обсуждались вопросы виртуального права, проблемы адаптации традиционного права к новому явлению – коммерческому и общедоступному интернету. В информационном пространстве заняли лидерство преимущественно зарубежные публикации, раскрывающие природу киберпространства, его влияние на международное право и национальные интересы, особенности регулирования виртуальных отношений. Это обусловлено ростом значимости глобальной сети интернет, появлением новой исследовательской среды, объекта и предметы изучения.

Работы носили преимущественно гражданско-правовой и предпринимательский характер. Ученые интегрировали цифровые технологии в существующие рамки договорного права, права интеллектуальной собственности, анализировали законодательство США и ЕС, документы ЮНСИТРАЛ, считавшиеся передовыми для своего времени. Альтернативные регуляторы если и упоминались, то в контексте технических стандартов и саморегулирования доменной системы (ICANN).

Второй этап можно назвать эрой социальных сетей, мы его определили в рамки 2008 – 2013 годов. Он ознаменован ростом социальных сетей (Facebook (продукт компании Meta, деятельность которой признана экстремистской и запрещена в РФ), Twitter, ВКонтакте), появлением блогосферы и платформ с пользовательским контентом (YouTube). Фокус научного интереса резко сместился к исследованиям сложных виртуальных взаимодействий, роли платформ, и информационного контента. Количество публикаций возросло в разы. Появились темы об ответственности информационных посредников за незаконный контент (клевету, нарушение авторских прав, призывы к насилию), о защите персональных данных в социальных сетях, о проблеме приватности, об обеспечении интеллектуальных прав, о «сетевом этикете», об использовании в отношениях в киберпространстве неправовых регуляторов.

Затронутые темы перестали быть чисто юридическими, для их научного анализа подключились социологи, политологи, специалисты по медиа. Юридические исследования стали междисциплинарными, признавая, что закон – лишь один из множества регуляторов, посредством которых можно регламентировать отношения в киберпространстве.

Третий этап укладывается в пределы 2014 – 2019 годов, именно в данное время начинается процесс суверенизации интернета, государство пытается регулировать киберпространство, наблюдается закат периода вседозволенности в интернете, который многими рассматривался в концепции киберпанка. В публичном пространстве развернулась дискуссия о свободе в интернете, суверенном киберпространстве, юрисдикции в виртуальной среде. На фоне роста геополитической напряженности, разоблачений Эдварда Сноудена и первых скандалов с вмешательством в выборы, концепция национального суверенитета в киберпространстве выходит на первый план. Большинство публикаций сместили дискурс научных дискуссий из частноправовой плоскости в публично-правовую и международно-правовую. Многие статьи касались проблем геополитического характера. В фокусе оказалось не саморегулирование интернета, а то, как государство должно регулировать саморегулирующиеся системы и глобальные платформы.

Четвёртый этап мы связали с развитием систем искусственного интеллекта и датировали его начало 2020 годом. Он определяется двумя ключевыми тенденциями: а) технологическим прорывом в области искусственного интеллекта; б) переходом от обсуждения к практическому регулированию глобальных цифровых платформ.

Большинство научных публикаций затрагивали этические аспекты интеграции систем искусственного интеллекта и робототехники в бытовую сферу. Дискутировался вопрос о месте правовых регуляторов в киберпространстве, актуализировалась тема интернет-права, обсуждалась проблема предвзятости алгоритмов, защита прав человека в условиях применения систем искусственного интеллекта, регулирование генеративных моделей, цифровые экосистемы и

платформы, правовой режим цифровых активов, концепция цифровых прав (право на доступ к интернету, право на забвение, право на цифровую идентичность), правовые аспекты метавселенных, вопросы виртуальной собственности в новых иммерсивных средах.

Особенностью многих научных статей можно считать их междисциплинарность. Появились работы на стыке права, этики, технологий и экономики. Правовое регулирование становится все более сложным, сочетая в себе элементы конкурентного, потребительского, информационного и международного права.

Систематизируя сказанное, отметим, что анализ публикаций в хронологической динамике показывает эволюцию научных взглядов от решения локальных, технико-юридических задач (как подписать электронный документ) к осмыслению глобальных, социально-политических и философских проблем (кто контролирует информационную реальность, как обеспечить права человека в эпоху ИИ и власти платформ). Научный дискурс прошел путь от попыток вписать киберпространство в существующую правовую парадигму до признания того, что само киберпространство формирует новую, полицентрическую реальность регулирования, где право вынуждено взаимодействовать с неправовыми регуляторами.

Следующий раздел аналитического блока посвящён учебно-научной литературе, в которой прямо или косвенно рассматриваются вопросы правового или неправового регулирования отношений в киберпространстве.

Почему мы придаём важное значение учебно-научной литературе, вполне понятно: «цифровое право» появилось вследствие развития цифровых технологий и интернета, которое консервативная часть теоретиков права считает «придуманным», и, как следствие, в противовес данному суждению в качестве аргументов появились учебники, раскрывающие суть и содержание «цифрового права». Сама дискуссия о цифровом праве – это показатель степени раскола в стане теоретиков права.

Среди множества учебников можно выделить работы фундаментального характера, в которых сформулированы концептуальные подходы к цифровому пространству и отношениям, складывающимся в нём, учебники с упором на отраслевое освещение отношений в киберпространстве и учебный контент общеинформативного характера о цифровой среде. Таким образом, выделились три категории учебно-научной литературы.

В первую категорию попадает учебник И. М. Рассолова «Право и Интернет. Теоретические проблемы».[1] В работе представлен авторский подход, раскрывающий специфику взаимодействия права и киберпространства. С позиций общей теории права и информационного права разработана и предложена концепция права кибернетического пространства (интернет-права). Определены методологические основания и системообразующие принципы действия правовых норм в условиях киберпространства, раскрыта физическая модель «пространство-время» применительно к цифровой среде. Проанализированы системные взаимосвязи и взаимодействие права кибернетического пространства со смежными регулятивными системами: цифровым правом, правовым обеспечением электронной коммерции, а также с формирующимся правом гуманитарных технологий.

Значительный раздел исследования посвящен анализу детерминационного влияния права на цифровую среду, а также разработке научно обоснованной классификации отдельных видов преступлений, совершаемых с использованием сети Интернет.

Данный учебник позволил систематизировать ранее полученные знания в области теории права с учётом их проекции на киберсреду.

Работа В. Б. Наумова «Право и Интернет: Очерки теории и практики»[2] представляет собой одно из ранних комплексных исследований, посвященных правовому регулированию сети Интернет в Российской Федерации. В ней

---

[1] Рассолов И. М. Право и Интернет. Теоретические проблемы / И. М. Рассолов. – 2-е изд., доп. – М.: Норма: ИНФРА-М, 2017. – 383 с.

[2] Наумов В. Б. Право и Интернет: Очерки теории и практики : монография. – М.: Книжный дом «Университет», 2002. – 432 с.

рассматриваются вопросы защиты интеллектуальной собственности, ответственности информационных провайдеров, правового статуса средств массовой информации и защиты персональных данных в цифровой среде. Автор проводит компаративистский анализ законодательных инициатив США, Индии и стран ЕС, а также анализирует релевантную российскую судебную практику, в частности, по спорам о доменных именах и нарушениях авторских прав. Отличительной особенностью работы является ее выраженная практическая направленность, в отличие от более теоретизированных исследований того периода.

Учебник «Цифровое право»[1] под редакцией В. В. Блажеева и М. А. Егоровой систематизирует нормативное регулирование и правоприменительную практику в цифровой сфере. В издании предложена характеристика законодательного и юрисдикционного комплекса «Цифровое право» с учетом теоретических, институциональных, технико-прикладных и дидактических аспектов, основанная на опыте преподавания в Университете имени О. Е. Кутафина (МГЮА).

Вторую категорию представляет учебник и практикум В. В. Архипова,[2] в котором изложена его методологическая позиция. Автор предлагает анализ правоотношений различной отраслевой принадлежности, опосредованных интернет-пространством. При этом автор высказывает сомнения в легитимности термина «интернет-право», считая его не устоявшимся в доктрине, а лишь рабочим обозначением предметной области. Подобная позиция выглядит дискуссионной, поскольку она изложена в учебнике, который по своей структуре и содержанию посвящен именно систематизации знаний в рамках этого «несуществующего» права.

Следующий учебник, отнесённый во вторую категорию, под авторством Д. А. Ловцова «Информационное право»[3] сосредоточил материалы, посвященные

---

[1] Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. – М.: Проспект, 2021. – 640 с.

[2] Архипов В. В. Интернет-право: учебник и практикум для бакалавриата и магистратуры / В. В. Архипов. - 2-е изд., перераб. и доп. – М.: Изд-во Юрайт, 2020. – 275 с.

[3] Ловцов Д. А. Информационное право: учебник для вузов. – М.: Изд-во Юрайт, 2024. – 411 с.

именно информационному праву. В данном издании рассматриваются ключевые вопросы, касающиеся правового регулирования информационных процессов и отношений в современной информационной среде, предлагается анализ нормативных актов, судебной практики и международных стандартов, относящихся к различным аспектам информационного права. Среди особенностей учебника можно выделить подробный анализ специфики информационных правоотношений, особенности регулирования массовых коммуникаций и киберпреступлений, наличие практико-ориентированных заданий и упражнений, схематический материал, облегчающий его понимание.

Третья категория учебников общеинформативного характера в обзоре представлена учебником «Право и цифра: Машиночитаемое право, цифровые модели-двойники, цифровая формализация и цифровая онто-инженерия в праве».[1] Отношение к подобному учебно-научному контенту двоякое, так как сама обсуждаемая тема не имеет однозначной оценки.

Резюмируя вышеизложенное, можно предположить, что большинство учебников ориентированы на подготовленного читателя, имеющего теоретические знания о праве, цифровой среде и социальном кибернетическом пространстве. Дискуссия о «цифровом праве» как самостоятельной отрасли права свидетельствует о существующем разногласии в подходах отечественных теоретиков права, что само по себе уже проблема, требующая научного осмысления.

Анализ показывает, что правовая природа отношений в киберпространстве определяется не только традиционными правовыми механизмами, но и неюридическими регуляторами, такими как технологическая архитектура (код), рыночные модели и социальные нормы цифровых сообществ, что вместе составляет полирегуляторную систему, отличающуюся отсутствием единого центра нормотворчества и универсальной иерархии, где эффективность

[1] Понкин И. В. Право и цифра: Машиночитаемое право, цифровые модели-двойники, цифровая формализация и цифровая онто-инженерия в праве: учебник / И. В. Понкин, А. И. Лаптева. – М.: Буки Веди, 2021. – 174 с.

регулирования определяется не только государственной легитимностью и принуждением, но и архитектурой среды, договорными условиями и общественным признанием.

Исследование полинормативной системы регулирования отношений в киберпространстве имеет фундаментальное значение для современной теории права, что обусловлено специфическими свойствами динамично развивающейся виртуальной среды, объективными потребностями совершенствования и повышения эффективности названной системы, а также проблемами защиты прав пользователей в условиях формирования новых правовых порядков.

Отечественная наука внесла значимый вклад в осмысление цифровой трансформации. Исследователи предвосхитили эпоху «сетевого права» и цифровизации правовых процессов (электронное правосудие, цифровой рубль), обосновали возможность существования «интернет-права» как комплексного межотраслевого института, признав уникальность виртуальных отношений, эмпирически подтвердили роль саморегулирования (на примере ICANN) и неразрывную связь права с технической инфраструктурой.

Значительный объем научных исследований по темам, связанным с виртуальным пространством, свидетельствует о растущей актуальности проблематики, творческом поиске решений, регламентирующих различные аспекты социальных взаимодействий в киберпространстве.

1.2 Социально-правовая природа киберпространства: сущность, структура и специфика

Киберпространство представляет уникальную социальную среду, обеспечивающую коммуникацию пользователей и реализацию различных проектов в экономических, политических, культурных, военных и других сферах. Это, в свою очередь, порождает специфические правоотношения, которые формируются в процессе такого взаимодействия и значительно отличаются от традиционных правоотношений. Для углубленного понимания правовой природы

отношений, возникающих в виртуальной среде, необходимо рассмотреть «киберпространство» в социально-правовом аспекте. Такой подход позволит выявить ключевые характеристики киберпространства и раскрыть особенности его правовой природы.

Часто можно встретить суждение о том, что киберпространство – это «виртуальное пространство, в котором коммуницируют подключенные к сети компьютеры или другие цифровые средства (например, мобильные устройства). Для связи компьютеров чаще всего используется интернет. Поэтому это информационное, а не кибернетическое пространство. Киберпространство также определяется в качестве нового типа социального пространства, в котором встречаются пользователи интернета».[1]

Автор диссертационного исследования Е. А. Родина считает, что киберпространство сходно с обычным физическим пространством, поскольку в нем есть аналоги перемещения, например, при переходе по гиперссылкам от одного сайта к другому, оно является бесконечным по количеству сайтов, только в сети World Wide Web свыше 1,7 млрд. пользователей, и количество продолжает расти. Она воспринимает киберпространство как совокупность проводных и беспроводных сетей связи, аппаратных средств и программных продуктов, обеспечивающих возможность произвольной коммуникации между любыми пользователями.[2]

В рамках научной концепции М. В. Мигулевой киберпространство интерпретируется как инструментальный комплекс, используемый различными социальными институтами для хранения и трансляции традиций, социальных норм и ценностных ориентиров. Параллельно оно само обладает признаками социального института, выполняя соответствующие социокультурные функции. С точки зрения автора, киберпространство находится в отношении взаимной детерминации с культурными системами и оказывает существенное влияние на

[1] Касьянов В. В., Нечипуренко В. Н. Социология Интернета : учебник: 1-е изд.. – М.: Изд-во Юрайт, 2018. – С. 97-100.
[2] Родина Е. А. Противодействие криминальной виктимизации пользователей сети «интернет» в киберпространстве: дис. ... кандидата юридических наук. – Саратов, 2022. – С.22.

формирование индивидуального и коллективного мировоззрения, ценностных структур, а также на процессы распространения идеологий.[1]

В философском дискурсе данное понятие раскрывается как метафорическая абстракция, используемая в философских и технологических исследованиях, репрезентирующая виртуальную реальность как современное воплощение ноосферы.

Не бесспорны суждения о том, что киберпространство – это виртуальное пространство, в котором коммуницируют подключенные к сети компьютеры и другие цифровые средства через интернет,[2] или киберпространство – это место совершения определенных действий без участия объектов и субъектов реального мира в физическом воплощении.[3]

По утверждению Л. В. Терентьевой, «киберпространство - управляемая широким кругом субъектов искусственная телекоммуникационная среда реализации общественных отношений, функционирование и поддержание которой осуществляется посредством программно-технической инфраструктуры в виде ее физической части и нефизической (виртуальной) части».[4]

Дискуссионное суждение высказал М. А. Федотов, считавший, что «если конституционное право является основой всех других отраслей права то, пока Конституция не обретет своего интернет-измерения, всякие попытки правового регулирования деятельности в киберпространстве методами национального законодателя обречены на неудачу. Если представить, что информационно-коммуникационные сети – это не просто новое средство коммуникации, а новая сфера обитания человеческой цивилизации, новая сфера человеческой активности

---

[1] Мигулева М. В. Киберпространство как социальный институт: признаки, функции, характеристики // Научный журнал «Дискурс-Пи». – 2020. – № 4 (41). – С. 199–212

[2] Касьянов В. В., Нечипуренко В. Н. Социология Интернета : учебник: 1-е изд.. – М.: Изд-во Юрайт, 2018. – С. 97–100.

[3] Тюканова В. Р., Шумов П. В. Цифровизация нормотворчества. IT-технологии и киберпространство как средства и место реализации правоотношений // Скиф. Вопросы студенческой науки. – 2022. – № 11 (75). – С. 138–142.

[4] Терентьева Л. В. Правовое регулирование отношений в киберпространстве: вопросы управления и юрисдикции // Материалы XV Международной конференции «Право и Интернет», Москва, 27-28 октября 2022 г. – URL: https://ifap.ru/pi/15/pres11.pdf (дата обращения: 25.02.2023).

и новая сфера применения права, то легко понять, что информационное право должно иметь особый метод правового регулирования, ибо регулирование общественных отношений будет осуществляться в первую очередь в киберпространстве».[1]

Особенность киберпространства не позволяет экстраполировать традиционный подход к оценке действия правовой нормы в пространстве, во времени и по кругу лиц. Дело в том, что киберпространство не имеет территориальной, точнее географической определенности, категория время в привязке к киберпространству не базируется на конкретном часовом поясе, а круг лиц, обитающих в киберпространстве, не имеет материальной основы.

Получается, что киберпространство проявляется только при условии наличия соответствующего технического оборудования, программного обеспечения, интернет сети, позволяющей осуществить коммуникацию и выстраивать правоотношения.

Ещё одна особенность киберпространства связана с тем, что человек может взаимодействовать с ботом (алгоритмом), например, в контексте электронной коммерции и финансовых операций. Общение человека с ботом может быть частью правоотношений между людьми, где бот выступает как инструмент коммуникации и автоматизации процесса.

Проведенный анализ существующих подходов позволяет заключить, что в научном дискурсе киберпространство преимущественно отождествляется с интернетом, компьютерными технологиями и цифровыми коммуникациями. Широко распространена его интерпретация в качестве специфической среды или виртуального мира, что имплицитно приписывает ему пространственные характеристики. Данный подход, по нашему мнению, представляется дискуссионным.

---

[1] Федотов М. А. Конституционные ответы на вызовы киберпространства // Lex russica. – 2016. – № 3 (112). – С. 164–182. – URL: https://lexrussica.msal.ru/jour/article/view/57/58 (дата обращения: 24.03.2023)

В этой связи следует обратиться к позиции А. Деформ, которая аргументированно утверждала, что «киберпространство не является ни географическим пространством, ни местом, ни средой, ни миром, ни даже территорией». Этот тезис ставит под сомнение правомерность применения традиционных пространственных категорий к принципиально новой цифровой реальности.[1]

Можно частично согласиться с указанной позицией, поскольку ассоциация киберпространства с трехмерной объективностью представляет собой иллюзию. Киберреальность конституируется исключительно через активацию технических средств, способных: транслировать цифровой контент; обеспечивать коммуникационное взаимодействие пользователей; предоставлять доступ к сетевым ресурсам; создавать условия для осуществления экономической и иной социально значимой деятельности; формировать предпосылки для возникновения специфических правоотношений в цифровой среде.

Важно подчеркнуть, что в киберпространстве формируются правоотношения нового технологического порядка, где человек выступает центральным субъектом. Без человеческого участия существование виртуального мира теряет социальный и правовой смысл.

Современная практика демонстрирует становление в киберпространстве особого типа общественных отношений – виртуальных отношений. Их объектами выступают цифровые активы, обладающие потребительскими свойствами и коммерческой ценностью, что подтверждается готовностью субъектов осуществлять их монетизацию, а также формированием развитой системы их правового признания и оборота, включая законодательное закрепление понятия «цифровые права», судебную защиту интересов владельцев токенов и криптоактивов, установление налогового режима совершаемых с ними операций, что в совокупности свидетельствует об объективном процессе

[1] Desforges A. Representations of Cyberspace: A Geopolitical Tool // Cyberspace: Political Issues. – 2014. – Vol. 1, no. 152-153. – P. 67–81. – URL: https://www.cairn-int.info/abstract-E_HER_152_0067--representations-of-cyberspace-a-geopolit.htm (дата обращения: 24.03.2023).

институционализации новых видов имущественных прав в цифровой среде и необходимости их комплексного теоретико-правового осмысления.

На основании вышеизложенного предлагаем своё восприятие киберпространства. Основываемся на том, что данное пространство эфемерно, подвержено быстрым изменениям, не имеет физической сущности. При этом инфраструктура, поддерживающая киберпространство, вполне материальна и включает высокотехнологичные компоненты - серверы, устройства хранения данных, кабели, трансляторы и множество других. Границы киберпространства не тождественны границам физического пространства, они не имеют координат. Киберпространство рассеяно повсюду, его нельзя указать на карте мира.

Можно рассматривать киберпространство как **среду, созданную при помощи программно-аппаратных комплексов с возможностью формирования симулякров, установления коммуникаций, осуществления различных видов виртуальной деятельности, включая образование, торговлю, управление и иную, позволяющую виртуальные отношения переводить в плоскость правоотношений в рамках одной или нескольких юрисдикций**.

Киберпространство выступает как комплексная виртуальная субстанция, сформированная в результате действий людей, программ и сервисов в интернете посредством высоких технологий, служащая для решения различного рода задач. В ней складываются отношения, которые требуют правовой регламентации и, соответственно, правовой охраны.

Специфика отношений в киберпространстве детерминирована их информационной природой и виртуальным характером взаимодействия, опосредованного использованием технических средств. Данные особенности обусловливают существенное отличие правовой природы отношений в киберпространстве от традиционных правоотношений, складывающихся в физическом мире.

В юридической науке дефиниция «правовая природа» применяется для обозначения сущностных характеристик правовых явлений, их качественной определённости и места в системе права. Указанная категория позволяет

идентифицировать правовой режим соответствующего объекта или явления, а также определить адекватные механизмы их правового регулирования. Применительно к отношениям в киберпространстве это предполагает необходимость разработки специальных правовых моделей, учитывающих их цифровую онтологию и трансграничный характер.

Авторы статьи «Правовая природа как категория правоведения» констатировали, что выявить правовую природу явления — это значит охарактеризовать его определенным образом, определить место в системе правовых категорий, институтов, подчеркнув при этом, что категория «правовая природа» имеет методологическое значение. [1]

С. С. Алексеев рассматривал правовую природу как «внутреннюю юридическую сущность явлений, выражающуюся в их социальном качестве и назначении»,[2] в то время как Н. И. Матузов определял правовую природу как «совокупность социально-юридических свойств явления, обусловленных его объективной сущностью и местом в системе общественных отношений, регулируемых правом».[3] В. В. Лазарев предполагал, что правовая природа объекта состоит в совокупности правовых признаков, характеризующих его сущность и определяющих его юридический статус.[4]

Иную позицию транслировал В. М. Сырых. Он отмечал, что правовая природа какого-либо явления раскрывается через установление его юридических признаков, отличающих его от других социальных явлений и позволяющих определить его место в системе правового регулирования.[5] В свою очередь,

[1] Дураев Т. А., Тюменева Н. В. Правовая природа как категория правоведения // Вестник Саратовской государственной юридической академии. – 2022. – №6 (149). – С.15–16.
[2] Алексеев С. С. Общая теория права. Т. 1. – М.: Юридическая литература, 1981. – С. 215.
[3] Матузов Н. И. Личность. Права. Демократия. Теоретические проблемы правового статуса личности в социалистическом обществе : монография. – Саратов: [б. и.], 1972. – 172 с.
[4] Лазарев В. В. Общая теория права и государства : учебник. – М.: Юристъ, 2000. – С. 42.
[5] Сырых В. М. Логические основания общей теории права. Методологические вопросы общей теории права : : в 2 т. Т. 1. – М.: Юстицинформ, 2004. – С. 312.

В. А. Филипенко полагал, что правовую природу, как и само право, следует искать в представлениях общества и социальной практике.[1]

Не бесспорную точку зрения изложили Н. П. Асланян. и Т. В. Новикова, которые считали, что перед правовым научным сообществом стоит задача конвенционального решения вопроса о значении термина «правовая природа», так как это необходимо правовой науке для выявления «первородных» свойств (признаков) правовых явлений.[2]

Представители различных научных школ по-своему толковали понятие «правовая природа», что показывает сложность и многогранность данного термина, отсутствие единого и общепринятого подхода к пониманию его содержания, а также высокую степень абстракции названной дефиниции и возможности интерпретации ее в зависимости от конкретного контекста.

Определение правовой природы отношений в киберпространстве зависит от целей исследования. Например, при анализе правовой природы криптовалюты акцент переносится на свойства, присущие объекту гражданских прав в качестве платежного средства или инвестиционного актива. Правовая природа кибератак будет квалифицироваться как правонарушение, определённое в рамках уголовного права. В частности, несанкционированный доступ к компьютерной информации, распространение вредоносных программ, нарушение работы информационных систем.

Отношения в киберпространстве включают множество сложных явлений, правовая природа которых вызывает дискуссии. В контексте нашего исследования предлагаем рассмотреть две группы явлений, порождающих отношения с неопределённой правовой природой. К ним можно отнести локальные и глобальные явления. Под локальными явлениями понимаем те, что возникают и

---

[1] Филипенко В. А. Правовая природа с точки зрения философии // Информационно-правового портала «Закон.ру». – URL: https://zakon.ru/blog/2022/04/26/pravovaya_priroda_s_tochki_zreniya_filosofii (дата обращения: 12.12.2024).

[2] Асланян Н. П., Новикова Т. В. Об интерпретации термина «правовая природа» // Baikal Research Journal : электронный научный журнал Байкальского государственного университета. –2018. – Т. 9, № 4. – С.25. – URL: brj-bguep.ru (дата обращения: 08.12.2024).

функционируют в рамках замкнутых цифровых экосистем, в свою очередь, глобальные явления характеризуются децентрализованной природой, отсутствием единого центра контроля и трансграничным характером.

В числе локальных видятся следующие:

Отношения, порождающие цифровые данные, обладают сложной правовой природой, которая охватывает ряд ключевых аспектов, включая владение, распоряжение и использование указанных данных. В современной правовой доктрине и законодательной практике различных юрисдикций наблюдается неоднозначность в трактовке ряда фундаментальных вопросов. К их числу относятся: установление принадлежности данных, генерируемых пользователями в виртуальной среде; признание их объектом гражданского оборота и торговли; а также определение характера и пределов ответственности за их несанкционированное распространение и утечку.

Целесообразно констатировать, что подавляющий массив данных, получаемых от пользователей, является объектом правового регулирования. Однако степень и механизмы такого регулирования варьируются в зависимости от типа данных (персональные, обезличенные, большие данные, метаданные) и специфики национального законодательства. В ряде государств цифровые данные не отождествляются с классическим объектом вещных прав, то есть на них не распространяется право собственности в его традиционном понимании. Ярким примером такого подхода выступает регулирование Европейского союза, где «Общий регламент о защите данных» (GDPR)[1] фокусируется не на установлении права собственности на персональные данные, а на детальном регламентировании процессов их обработки, обеспечивая защиту прав субъектов данных. Аналогичный подход, ориентированный на регулирование обработки и контроля, а не владения, закреплен «Калифорнийским законом о защите прав потребителей» (CCPA)[2] в США.

---

[1] Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPR-Text.com. – URL: https://gdpr-text.com/ru (дата обращения: 06.05.2024).

[2] The California Consumer Privacy Act // theccpa.org. – URL: https://theccpa.org/ (дата обращения: 06.05.2024).

В отличие от указанных подходов, в законодательстве Российской Федерации в соответствии со статьей 128 Гражданского кодекса РФ, информация отнесена к самостоятельным объектам гражданских прав наряду с вещами, имущественными правами и результатами интеллектуальной деятельности. Таким образом, цифровые данные признаются объектом, который может находиться в гражданском обороте и в отношении которого могут устанавливаться правомочия владения, пользования и распоряжения.

Более детально порядок обращения с цифровыми данными регулируется Федеральным законом № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Данный нормативный акт регламентирует базовые принципы и правила обработки информации, включая обязанности по обеспечению ее конфиденциальности. В частности, статья 16 вышеуказанного закона определяет понятие конфиденциальности информации и закрепляет обязательные требования по защите сведений от неправомерного доступа.

Особый правовой режим устанавливается в отношении персональных данных, где центральным субъектом правоотношений выступает физическое лицо. Несмотря на существующие дискуссии о природе прав на персональные данные, в международной и российской практике доминирует подход, в соответствии с которым за личностью закрепляется право контролировать сбор, распространение и использование информации о себе. Данный принцип, закрепленный, в частности, в статье 3 GDPR,[1] нашел свое отражение и в российском законодательстве, прежде всего в Федеральном законе № 152-ФЗ «О персональных данных», что свидетельствует об унификации базовых принципов защиты в глобальном цифровом пространстве.

Отношения, позволяющие определять цифровую идентичность и связь с реальной личностью, сталкиваются с проблемами: а) аутентификации и верификации в киберпространстве; б) защитой цифровой идентичности от кражи и злоупотреблений.

[1] Общий регламент защиты персональных данных (GDPR) Европейского союза // GDPR-Text.com. – URL: https://gdpr-text.com/ru (дата обращения: 06.05.2024).

Цифровая идентичность — это сложный гибрид технологии и права. Ее развитие требует комплексного подхода: внедрения удобных, надежных и децентрализованных систем аутентификации; принятия четкого определения, установления градаций доверия и создания правовых механизмов для работы с разными типами идентичностей.

Цифровая идентичность рассматривается как совокупность атрибутивных данных от учетных записей до биометрических параметров, используемых для идентификации субъекта в цифровой среде, обладает сложной правовой природой. Она одновременно функционирует как инструмент для установления правосубъектности в виртуальном мире и как самостоятельный объект правовой охраны. В отличие от физической, цифровая идентичность характеризуется множественностью и вариативностью, что усложняет установление юридической ответственности. Несмотря на ее фундаментальную значимость, в большинстве национальных правопорядков отсутствует общепринятое толкование данного понятия, что приводит к фрагментарному и опосредованному регулированию. Так, в ЕС Регламент eIDAS нормирует лишь отдельные электронные средства идентификации, а в США регулирование сводится к защите персональных данных (CCPA, HIPAA).

В Российской Федерации правовой режим цифровой идентичности формируется через совокупность норм об идентификации, аутентификации, персональных данных, регулируемых на основании требований Федерального закона «Об информации, информационных технологиях и о защите информации», [1] Федерального закона «Об электронной подписи».[2]

На обязательное развитие систем идентификации и аутентификации граждан в цифровой среде обращено внимание в Указе Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ // Российская газета, 29.07.2006 г. – №165.
[2] Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ // Российская газета, 08.04.2011 г. – № 75.

годы».[1] С целью реализации обозначенной задачи предполагается совершенствовать механизмы шифрования, криптографической защиты информации, устанавливать системы аутентификации и идентификации граждан и юридических лиц.

При этом проблема множественности идентичностей, затрудняющая атрибуцию ответственности за противоправные деяния, остается доктринально и законодательно неразрешенной.

Отношения на основе смарт-контрактов с учётом их места в системе договорного права вызывают дискуссии, затрагивающие две ключевые проблемы. Первая касается юридической силы соглашений, заключенных с помощью смарт-контрактов, облеченных в форму самоисполняющегося алгоритмического протокола. Вторая связана с разработкой адекватных механизмов разрешения споров, возникающих в связи с их исполнением. Сложность правовой квалификации смарт-контракта, представляющего размещенный в распределенном реестре алгоритм для автоматического исполнения договорных условий при наступлении заранее определенных событий, обусловлена его гибридной природой, сочетающей в себе элементы классического договорного права и цифровых технологий, что порождает уникальные юридические особенности.

Смарт-контракт является связкой между цифровой и правовой реальностью. Его правовая сущность носит дуалистический характер, сочетая в себе элементы традиционного договорного права (наличие воли сторон, согласованность условий) и свойства программного кода (детерминированность, автоматизм, неотвратимость исполнения). Данный синтез формирует уникальные юридические особенности, которые не в полной мере охватываются существующими правовыми конструкциями.

В каждой стране правовая природа смарт-контрактов определяется по своему усмотрению. Так, в Соединённых Штатах данный вопрос решается на уровне

[1] Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы» от 09.05.2017 № 203 // Электронный фонд правовых и нормативно-технических документов. – URL: https://docs.cntd.ru/document/420397755 (дата обращения: 11.05.2024).

отдельных штатов, например, в Аризоне и Неваде существуют нормы «Uniform Electronic Transactions Act (UETA)»[1] и «Electronic Signatures in Global and National Commerce Act (ESIGN)»[2], признающие использование смарт-контрактов для заключения сделок. В Делавэре принят закон «Delaware General Corporation Law (DGCL)»[3], позволяющий корпорациям хранить записи акционеров и акционерных капиталов в распределённом реестре - блокчейне. При этом федеральное законодательство США не содержит чётких положений относительно смарт-контрактов, и многое остаётся открытым для интерпретации судов и регуляторов.

Анализ современного состояния правового регулирования смарт-контрактов демонстрирует разнообразие подходов национальных законодателей, что порождает значительную правовую неопределенность в данной сфере.

Законодательство Англии и Уэльса, основываясь на доктрине свободы договора, в целом допускает использование электронных подписей и автоматизированное исполнение обязательств.[4] Ключевой проблемой практической имплементации смарт-контрактов остается их соответствие классическим критериям действительности соглашения, установленным в прецедентном праве. К таким критериям относятся: необходимость идентификации сторон, определенность условий и наличие намерения создать правовые отношения. Автоматизм исполнения порождает сложности в толковании условий контракта, распределении рисков, связанных с ошибками в коде, и определении юрисдикции для разрешения споров.

---

[1] Uniform Electronic Transactions Act (UETA) : Final Act with Prefatory Note and Comments. – URL: https://www.approveme.com/wp-content/uploads/2021/10/UETA_Final-Act_1999.pdf (дата обращения: 12.05.2024).

[2] Electronic Signatures in Global and National Commerce Act : GovInfo. – URL: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (дата обращения: 12.05.2024).

[3] Delaware General Corporation Law (Dgcl). – URL: https://delcode.delaware.gov/title8/c001/ (дата обращения: 12.05.2024).

[4] Maria G. Vigliotti What Do We Mean by Smart Contracts? // Frontiers in Blockchain. – 2020. – Vol. 3, Art. 553671. – URL: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020 (дата обращения: 12.05.2024).

На уровне Европейского Союза базовые принципы электронного заключения договоров заложены в Директиве ЕС «Об электронной коммерции».[1] Данный акт устанавливает принцип технологической нейтральности и предписывает государствам-членам обеспечить правовое признание договоров, заключенных электронным способом. Однако Директива не содержит прямых упоминаний о смарт-контрактах, что оставляет вопрос их точного правового статуса на усмотрение национальных правовых систем стран-участниц.

Швейцарская правовая система применяет принцип технологической нейтральности, что позволяет субсуммировать смарт-контракты под существующие договорные конструкции куплю-продажу, мену, оказание услуг без необходимости принятия специального законодательства, при условии их соответствия общим требованиям Обязательственного закона.

В Германии юридическая сила обязательств, возникающих из смарт-контрактов, признается в случае соблюдения общих требований Гражданского уложения к заключению договора, а также специального законодательства о защите прав потребителей. При этом непосредственно механизм исполнения (код) регулируется техническими, а не правовыми стандартами.

В российском законодательстве отсутствует понятие «смарт-контракт». Однако в рамках Гражданского кодекса Российской Федерации предусмотрена возможность заключения договора в электронной форме. Правовая доктрина и правоприменительная практика (включая разъяснения Федеральной налоговой службы) рассматривают смарт-контракт не как самостоятельный тип договора, а как способ заключения и исполнения традиционных гражданско-правовых договоров (купли-продажи, оказания услуг и т.д.) с использованием программного кода. Таким образом, к отношениям сторон применяются общие нормы договорного права.

---

[1] Правовые аспекты использования смарт-контрактов // BIT.TEAM. – URL : https://bit.team/blog/ru/pravovye-aspekty-ispolzovaniya-smart-kontraktov/ (дата обращения: 12.05.2024).

Несмотря на функциональное признание смарт-контрактов в большинстве рассмотренных юрисдикций, их единая правовая природа остается доктринально неопределенной. Преобладающим является технологически нейтральный подход, при котором смарт-контракт рассматривается как форма традиционного договора. Подобный правовой дуализм создает существенные препятствия для унификации регулирования и формирования предсказуемой судебной практики, что сдерживает их широкое коммерческое применение.

Отношения, связанные с системами искусственного интеллекта и вопросы ответственности создателей и пользователей за их действия. Правовая природа данного явления многоаспектна и породила ряд вопросов, в частности, вопросы о правосубъектности искусственного интеллекта и распределении ответственности за действия, совершаемые автономными алгоритмами. Всё упирается в юридическое признание за системами искусственного интеллекта свойств субъекта права. Доминирующая в современной юридической доктрине позиция отрицает такую возможность, аргументируя это отсутствием у названных систем сознания, собственной воли и, что важно, деликтоспособности. Правосубъектность как юридическая конструкция, включающая правоспособность, дееспособность и деликтоспособность, имманентно присуща физическим и юридическим лицам и является производной от социальных качеств человека. Поскольку названные системы лишены этих качеств, они рассматриваются правом как объекты, а не субъекты правоотношений.

Отдельно существует блок проблем, связанных с признанием результатов, созданных системами искусственного интеллекта в науке, литературе, искусстве и ином. Факт их конкурентоспособности с творениями человека доказан эмпирически, что актуализирует необходимость решения юридического вопроса о правообладателе. При отсутствии специального регулирования возникает правовой вакуум из-за того, что права не могут принадлежать самой системе, так как она лишена правосубъектности, это порождает дилемму о закреплении их за создателем (разработчиком), владельцем или пользователем.

Ещё одна проблема связана с распределением ответственности за вред, причиненный действиями названных систем. В данной цепи потенциальной ответственности участвуют несколько субъектов: разработчики (создатели) – могут нести ответственность за конструктивные недостатки (дефекты программного кода) и недостатки безопасности, выявленные в процессе тестирования; операторы (владельцы) – ответственны за некорректную настройку, техническое обслуживание и эксплуатацию системы, выходящую за рамки предусмотренных разработчиком параметров; пользователи – могут привлекаться к ответственности при предоставлении заведомо некорректных данных или злонамеренном использовании системы.

Отдельно можно выделить проблему «электронного лица». В юриспруденции существует точка зрения, основанная на позиции признания системы искусственного интеллекта «электронным лицом». Этот вариант позволил бы переложить ответственность за действия непосредственно на систему. Фактически предлагается придать «электронному лицу» ограниченную правосубъектность, по аналогии с правосубъектностью корпораций.[1]

Данная концепция, по аналогии с юридическим лицом, не предполагает признания за системами искусственного интеллекта прав человека, а направлена на создание специального правового режима для ситуаций полностью автономного причинения вреда. Это позволило бы возлагать ответственность непосредственно на активы, закрепленные за таким «электронным лицом», подобно тому, как ответственность юридического лица обеспечивается его уставным капиталом.

Несмотря на то, что данная модель пока не получила широкого законодательного признания, она является значимым вкладом в правовую дискуссию. Яркой иллюстрацией актуальности проблемы является инцидент 2010 года, когда робот, самостоятельно совершивший покупку оружия на черном рынке, был «арестован» итальянскими правоохранительными органами, которые

[1] Мельникова Е. Н. Встраиваемость концепции электронного лица в правовую систему конкретного государства или государственного образования // Российский юридический журнал. – 2022. – № 2 (143). – С. 94–112.

столкнулись с невозможностью привлечения к уголовной ответственности объекта, не признанного субъектом права. [1]

Отношения с применением виртуальной и дополненной реальностей.

Правовая природа отношений, возникающих в связи с применением иммерсивных технологий (VR, AR, MR, XR), представляет собой комплексную научную проблему, охватывающую вопросы собственности, ответственности и защиты прав субъектов в виртуальных и дополненных мирах.

Во-первых, ключевой задачей является определение правового статуса виртуальной собственности. Это требует доктринальной разработки и законодательного закрепления квалификации виртуальных объектов (цифровых активов, персонажей, территорий) в системе объектов гражданских прав, механизмов их правовой защиты от противоправных посягательств, а также регламентации их оборотоспособности и налогообложения.

Во-вторых, остро стоит проблема распределения юридической ответственности за действия, совершаемые в виртуальных мирах. Необходимо установить круг субъектов ответственности за деликты, совершаемые аватарами и иными цифровыми агентами, включая ответственность разработчиков платформ за обеспечение безопасности пользователей, а также определить правовые основания для компенсации морального вреда.

В-третьих, фундаментальное значение имеет защита прав личности, что включает определение пределов свободы выражения мнений в виртуальной среде, разработку механизмов противодействия дискриминации и домогательствам, а также решение коллизионных вопросов об определении применимого права и компетентной юрисдикции для разрешения споров, возникающих в трансграничных виртуальных мирах.

В-четвертых, правовое регулирование должно учитывать этико-социальные аспекты, такие как предотвращение цифрового неравенства, обусловленного

[1] Odumosu D. O., Solomon G. Artificial Intelligence and Legal Personality: Any Rescue From Salomon v. Salomon? // IX International Conference on Complex Systems. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5106653 (дата обращения: 07.05.2024).

экономическим барьером доступа к технологиям, и противодействие рискам манипуляции сознанием посредством интеграции пропагандистского или коммерческого контента в иммерсивную реальность.

Очевидно, что нормативное регулирование отношений в среде иммерсивных технологий значительно отстает от технологического развития. Преодоление этого разрыва требует междисциплинарного подхода и разработки гибких правовых моделей, способных адаптироваться к уникальным вызовам виртуальных сред, обеспечивая при этом защиту фундаментальных прав и свобод человека.

Отношения на основе децентрализованных автономных организаций (Decentralized Autonomous Organization) (DAO).

Правовая природа децентрализованных автономных организаций (DAO), представляющих собой новую организационно-правовую форму, функционирующую на базе технологии блокчейн и управляемую посредством самоисполняемых смарт-контрактов, характеризуется фундаментальной доктринальной и нормативной неопределенностью. Ключевые проблемы правовой квалификации DAO концентрируются в области определения их правового статуса, установления режима ответственности участников, а также разработки адекватных моделей налогообложения и общего регуляторного надзора. Специфика DAO заключается в том, что их внутренняя структура и распределение управленческих полномочий между участниками (токенхолдерами) детерминированы исключительно алгоритмами, заложенными в смарт-контрактах.

В большинстве современных правопорядков DAO не обладают статусом юридического лица, что порождает правовой вакуум. Попытки отдельных юрисдикций (в частности, Франции и Германии) применить к DAO по аналогии конструкцию простого товарищества (партнерства) не решают принципиальной проблемы неограниченной ответственности участников. Таким образом, сохраняется неразрешенной задача по интеграции DAO в систему корпоративного права и формированию специального правового режима для систем, функционирующих на основе технологии распределенных реестров. Данный казус является ярким примером того, как правовая природа новых феноменов

киберпространства остается неустановленной, что генерирует комплексные теоретические и практические вопросы, требующие междисциплинарного осмысления в рамках теории права и отраслевых юридических наук. В этой связи предлагаем назвать данные локальные отношения **киберотношениями с локальной виртуальной природой**.

Следующий блок отношений в киберпространстве затрагивает правовую природу **глобального характера**. К ним мы относим: проблему установления правовой природы кибернетической легитимности; определение правовой природы кибервойны как формы принуждения; выявление правовой природы киберсуверенитета и «мягкого права».

Традиционное понимание легитимности основывается на признании права, власти или системы правил законными, обоснованными и обязательными к исполнению. Это признание основано на согласии большинства членов общества подчиняться установленному порядку. Применительно к киберпространству возникают вопросы, кто и как должен обеспечивать кибернетическую легитимность и какие механизмы могут быть использованы для этого.

Кибернетическая легитимность обеспечивает отношения на основе согласия субъектов с установленными правилами и мерами их урегулирования в киберсреде. Специфика кибернетической легитимности выражается в отсутствии единого центра власти, киберпространство не контролируется единственным субъектом. Даже ICANN (Internet Corporation for Assigned Names and Numbers)[1], ответственная за координацию глобальных систем идентификации в интернете, управляющая доменными именами, действует в рамках многосторонних соглашений, а не абсолютной власти.

Кибернетическая легитимность не сводится только к правовой легитимности, хотя и включает ее. Она также охватывает социальную, политическую, техническую и этическую легитимность. В отличие от традиционной легитимности, которая часто основывается на устоявшихся институтах и

[1] ICANN : international organization. // Britannica. – URL: https://www.britannica.com/topic/ICANN (дата обращения: 16.05.2024).

процессах, кибернетическая легитимность постоянно изменяется вместе с развитием технологий и цифровых отношений.

В киберпространстве нет единого центра власти, который мог бы однозначно определить, что является легитимным, а что нет. Легитимность формируется в результате взаимодействия множества акторов.

Виртуальное пространство не ограничено государственными границами, что создает трудности с установлением и применением единых стандартов легитимности. Возможность действовать анонимно или под псевдонимами в киберпространстве усложняет процессы обеспечения подотчетности и легитимности.

Кибернетическая легитимность смещает акцент с традиционных политических институтов на технологические системы, где власть опирается на контроль данных, алгоритмы и цифровое участие. Это создаёт как возможности для более эффективного управления, так и риски цифрового авторитаризма и потери человеческого контроля. Она тесно связана с функционированием технической инфраструктуры интернета. Например, сбои в работе интернета или целенаправленные кибератаки могут подрывать легитимность цифровых процессов.

Правовая основа легитимности в киберсреде связана с соблюдением установленных норм и правил, которые могут исходить как от официальных источников, так и от сообществ пользователей. Кибернетическая легитимность подразумевает соответствие действий в цифровой сфере правовым нормам и этическим стандартам. Однако её обеспечение сталкивается с рядом вызовов. Легитимность часто зависит от возможностей контроля инфраструктуры, что осложняется глобальным характером киберпространства и использованием различных технологий. Она определяется не только государственными институтами, но и техническими сообществами, например, разработчики протоколов IETF де-факто устанавливают правила поведения в киберсистемах через код. Многие решения в киберсреде, связанные с криптовалютой, принимаются посредством голосования токенхолдеров, что ставит под вопрос

превалирующую роль правового регулирования этой системы. В качестве примера можно привести управление криптовалютой Bitcoin, которое осуществляется консенсусом майнеров, а не государствами.

Исходя из изложенного, можно предположить, что особенность кибернетической легитимности проявляется в том, что она включает в себя не только традиционные правовые и политические аспекты, но и технологический компонент. Технологические системы, контроль данных, алгоритмы и цифровое участие становятся важными факторами, влияющими на легитимность власти и управления в киберпространстве. Однако технологии не заменяют, а дополняют традиционные политические институты, и их использование должно регулироваться правом и соответствовать общественным ценностям.

Кибервойна (Cyberwarfare) — это одна из глобальных проблем XXI века, порождающая специфические отношения, отличающиеся от традиционных форм вооружённых конфликтов, что усложняет установление её правовой природы.

В научном обороте нет единого, общепринятого определения кибервойны. Это создает значительные трудности в правоприменительной практике и международном сотрудничестве. Отсутствие четкой дефиниции осложняет классификацию киберинцидентов, определение степени их опасности и адекватную реакцию на них, что препятствует разработке эффективных правовых механизмов для их предотвращения и расследования.

Кибервойна – составной компонент гибридной войны, задача которой — достичь определенных целей в экономической, политической, военной и других областях посредством воздействия на общество и власть.

В этой связи уместно выявить специфику правовой природы кибервойны и определить, какие действия в киберпространстве можно квалифицировать как акт агрессии или вооруженное нападение, чтобы отграничить кибервойну от киберпреступности, кибершпионажа и других деструктивных форм кибердеятельности.

Кибервойна сопряжена с действиями, происходящими в специфической среде – в виртуальном пространстве. Если в реальном мире местом военных

действий могут выступать небо, земля, вода, космос, то в киберпространстве все связано с цифровым пространством, сформированным из программ, компьютеров, серверов, и иных технических компонентов, которые в то же время могут быть использованы в качестве объектов атак.

Театр боевых действий в кибервойне — это цифровое и физическое пространства, где происходят события деструктивного характера. Нападения или агрессия могут быть в форме кибератак на правительственные веб-сайты, системы электронного документооборота, базы данных государственных органов, на энергетические системы, транспортные сети, системы водоснабжения, на банки, платёжные системы, финансовые учреждения и другие объекты, которые обеспечивают жизнедеятельность общества, а также посредством распространения негативной информации, порочащей власть, армию, культуру, религию противника. Всё направлено на максимальное нанесение вреда цифровой, физической инфраструктуре и морально психологическому состоянию общества.

В качестве оружия используются различные инструменты и технологии, предназначенные для нанесения ущерба или нарушения работы информационных систем противника. Они могут быть классифицированы по разным признакам, но в общем виде можно выделить следующие категории: вредоносное программное обеспечение (Malware); эксплойты; инструменты DoS/DDoS-атак; инструменты социальной инженерии; дезинформация и пропаганда; эксфильтрация данных; компрометация аппаратного обеспечения и иные.

Целесообразно отметить, что по поводу правового регулирования кибервойны в сообществе юристов нет устоявшихся позиций. Например, В.В. Маневич уверена, что нормы международного гуманитарного права носят универсальный характер и применимы к конфликтам в киберпространстве. Однако из-за специфики киберпространства и его новизны некоторые его аспекты требуют адаптации к киберпространственной реальности.[1]

[1] Маневич В. В. Международно-правовое регулирование применения киберсредств при ведении вооруженных конфликтов: правовые основы и научные дискуссии // Закон и право. – 2024. – №4. – С. 275–282.

В противоположность данному суждению, Ю. В. Пузырева предлагает разработать новый международно-правовой режим, который не только будет учитывать фактор постоянного развития технологий, но и позволит выработать последовательное определение кибервойны. Такое определение, по ее мнению, позволит «вписать» данное явление в существующие международно-правовые режимы либо, что более вероятно, определит для ее регламентации новую область международно-правового регулирования.[1]

Вооруженный конфликт в киберпространстве, по утверждению С.Ю. Гаркуша-Божко, – это ситуация вооруженного столкновения и противостояния правительственных вооруженных сил двух и более государств, а также ситуация продолжительного вооруженного противостояния между правительственными вооруженными силами и организованными вооруженными группами или же между такими группами внутри одного государства, уровень напряженности насилия в которых превышает уровень напряженности в ситуациях нарушения внутреннего порядка и возникновения обстановки внутренней напряженности, в контексте которой сторонами такого противостояния используются киберсредства с целью осуществления различных кибероперациий друг против друга.[2]

Представленные точки зрения свидетельствуют о существенном противоречии во взглядах по вопросу понимания, толкования и регулирования кибервойны, что актуализирует задачу установления правовой природы данного социально-политического явления, поскольку она напрямую влияет на общественные отношения, политические процессы в глобальном масштабе.

Отношения, определяющие киберсуверенитет. В последние годы актуализировалась проблема установления правовой природы киберсуверенитета, выражающего стремление государств распространить свой национальный суверенитет на цифровое пространство и контролировать информационные потоки

---

[1] Пузырева Ю. В. Кибервойна как новый вызов международному сообществу: вопросы международно-правовой регламентации // ADVANCES IN LAW STUDIES. – 2022. – Том 10. – № 3. – URL: https://naukaru.ru/ru/nauka/article/52186/view#article-text (дата обращения: 16.05.2024).

[2] Гаркуша-Божко С. Ю. Определение вооруженного конфликта в киберпространстве // Вестник Санкт-Петербургского университета. Право. – 2023. – Т. 14. – №1. – С. 194–210.

в пределах своих границ. Вопросы киберсуверенитета тесно пересекаются с проблемами юрисдикции в киберпространстве, однако между ними существуют отличительные особенности, в связи с чем можно разграничить их правовую природу.

По существу, киберсуверенитет и юрисдикция в киберпространстве представляют разные правовые явления. Первое относится к фундаментальным правам государства, второе – к инструментам правоприменения.

Киберсуверенитет определяет общие рамки государственного контроля, а юрисдикция - конкретные механизмы правового воздействия. Киберсуверенитет включает право государства самостоятельно определять политику в сфере информационных технологий, устанавливать контроль над национальной информационной инфраструктурой, позволяет государству ограничивать доступ к определённым ресурсам, например в КНР «Великий файрвол» ограничивает доступ к международным сервисам, в Иране блокируется доступ к социальным сетям для защиты национальной информационной безопасности.

Юрисдикция в киберпространстве отражает право государства применять законы и назначать наказание за их несоблюдение, в то время как киберсуверенитет определяет конкретные стремления государства в области его правовой политики. Например, защищать свои национальные интересы в цифровом пространстве, создавать устойчивую нормативно-правовую базу, обеспечивать защиту критической инфраструктуры, ограничивать вмешательство внешних игроков и поддерживать внутренний контроль над интернетом и коммуникациями.

В контексте приведённого суждения можно констатировать, что Правительство России в 2025 году подготовило стратегию обеспечения киберсуверенитета на перспективу, разработало комплекс мер и среди прочих выделило ряд ключевых направлений, к которым отнесло: развитие отечественных IT-решений и программного обеспечения; создание защищённой инфраструктуры

для хранения и обработки данных; поддержку цифровых стартапов и инноваций; реформу цифрового образования и подготовку квалифицированных кадров.[1]

В апреле 2025 года в России прошли первые всероссийские слушания законов в сфере цифровой безопасности, которые затронули вопросы создания государственной информационной системы противодействия правонарушениям, совершаемым с использованием информационных и коммуникационных технологий.[2] Это лишний раз свидетельствует о растущей актуальности поставленных вопросов.

Однозначных решений по формированию государственного киберсуверенитета не существует. По мере совершенствования кибертехнологий будут возникать проблемы, связанные с актуализацией законодательства, следовательно, связанные с совершенствованием правовой природы киберсуверенитета.

Правовая природа отношений «мягкого права». «Мягкое право» (soft law) – это совокупность норм, принципов и рекомендаций, которые не обладают обязательной юридической силой, но оказывают влияние на поведение государств, организаций и индивидов. Оно существует в рамках киберпространства как гибкий инструмент регулирования, дополняющий классическое право, которое закреплено в законах, договорах и подкреплено санкциями государства.

«Мягкое право» не имеет обязательной юридической силы, но способно оказывать значительное влияние на поведение субъектов в различных областях. Его специфика проявляется в том, что нормы не создают юридических обязательств, но формируют ожидания и стандарты поведения.

Примером могут служить «Руководящие принципы ООН по бизнесу и правам человека». The United Nations Guiding Principles on Business and Human

---

[1] Цифровой суверенитет России 2025. // Politicana.ru. – URL: https://politicana.ru/politics/domestic/digital-sovereignty-russia-2025/index.html (дата обращения: 14.04.2025).

[2] Бурнов, В. Защита киберсуверенитета: первые слушания цифровых законов прошли в Москве. // РАПСИ. – URL: https://rapsinews.ru/digital_law_news/20250411/310784513.html (дата обращения: 16.05.2025).

Rights (UNGPs),[1] которые стали первым глобальным стандартом для предотвращения и устранения рисков негативного воздействия на права человека, связанных с предпринимательской деятельностью, и продолжают служить признанной международным сообществом основой для совершенствования стандартов и практики в области прав человека и предпринимательства.

Специфика «мягкого права» в киберпространстве проявляется в следующем: а) создается владельцами цифровых платформ в виде сводов правил; б) применяется ко всем лицам, действующим на этих платформах; в) не зависит от гражданства и фактического местонахождения пользователей; г) не создаёт юридических обязанностей для государства; д) является гибким инструментом регулирования.

Таблица актов «мягкого права», регулирующих отношения в цифровой среде

Российская Федерация

Название документа	Дата	Разработчик
Кодекс этики использования данных Реестр добросовестных участников рынка данных «Белая книга»	2020	Ассоциация больших данных и АНО «Институт развития интернета»
Кодекс этики в сфере искусственного интеллекта	2021	Альянс в сфере ИИ совместно с Аналитическим центром при Правительстве Российской Федерации и Минэкономразвития России
Меморандум о сотрудничестве в сфере охраны исключительных прав	2018	Подписан на площадке Роскомнадзора
Хартия «Цифровая этика детства»	2021	Альянс по защите детей в цифровой среде
Стандарты по взаимодействию маркетплейсов с продавцами товаров	2022	«ОПОРА РОССИИ»
Принципы взаимодействия участников цифровых рынков	2022	ФАС России
Кодекс добросовестных практик (Кодекс этической деятельности (работы) в сети Интернет)	2016	Роскомнадзор

Рисунок 1 – Таблица актов «мягкого права», регулирующих отношения в российском сегменте киберпространства[2]

[1] Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций, касающихся «защиты, соблюдения и средств правовой защиты» / Организация Объединенных Наций. – 2011. – 39 с. – URL: https://documents.un.org/doc/undoc/gen/g11/121/92/pdf/g1112192.pdf (дата обращения: 16.05.2024).

[2] «Мягкое право» в российской и зарубежной IT-сфере // Институт развития интернета. – URL: https://ири.рф/news/rossiyskoe-i-zarubezhnoe-myagkoe-pravo-v-it-sfere/?ysclid=m9ibszz86f991739175 (дата обращения: 16.05.2024).

Регулирование искусственного интеллекта

Государство	Название документа	Дата	Разработчик
Австралия	Кодекс практик «Code of Practice»	2021	AiMCO, Австралийский совет по маркетингу инфлюенсеров
	Кодекс этики в области рекламы «Ad Code of Ethics»	2021	AiMCO, Австралийский совет по маркетингу инфлюенсеров
Австрия	Кодекс этики для рекламной индустрии «Code of Ethics for Advertising Industry»	2021	Werberat
Бразилия	Руководство по рекламе цифровых инфлюенсеров «Guia de Publicidade Por Influenciadores Digitais»	2021	CONAR
Нидерланды	Кодекс социальных сетей и маркетинга влияния «Social Media & Influencer Marketing Code)»	2019	Stichting Reclame Code
Новая Зеландия	Руководство для инфлюенсеров по определению рекламного контента «Influencers AdHelp Information on Identifying Ad Content»	2020	Advertising Standards Authority
Швеция	Руководство о маркетинге в блогах и иных социальных сетях «Guidance on marketing in blogs and other social media»	2018	Swedish Consumer Agency
Канада	Руководство по раскрытию информации «Disclosure Guidelines»	2020	Influencer Marketing Steering Committee
Великобритания	Меморандум и устав «Memorandum and Articles of Association»	2021	Influencer marketing trade body
Франция	Руководство «Рекомендации по цифровой рекламе» «Recommendation Communication Publicitaire Digitale»	2021	Autorité de Régulation Professionnelle de la Publicité
КНР	Моральное руководство для представителей индустрии развлечений «Moral guidelines for entertainers»	2021	China Association of Performing Arts

Рисунок 2 – Таблица актов «мягкого права», регулирующих отношения в международном киберпространстве[1]

«Мягкое право» обладает рядом характеристик, которые позволяют: а) быстро реагировать на новые вызовы, связанные с обеспечением кибербезопасности, развитием систем искусственного интеллекта и иных процессов, происходящих в киберпространстве, на которые не успевает реагировать традиционное право; б) добровольно соблюдать принятые правила из-за возможности потери репутации в виртуальной среде; в) достигать компромиссов в спорных вопросах в случае неопределённой юрисдикции, где страны не готовы брать на себя юридические обязательства; г) служить основой для разработки законодательных актов; д) не применять санкции, так как нарушения установок мягкого права не влечёт судебного преследования, но может привести к политическим, экономическим и репутационным потерям.

[1] «Мягкое право» в российской и зарубежной IT-сфере // Институт развития интернета. – URL: https://ири.рф/news/rossiyskoe-i-zarubezhnoe-myagkoe-pravo-v-it-sfere/?ysclid=m9ibszz86f991739175 (дата обращения: 16.05.2024).

Отмечаем, что «мягкое киберправо» в большинстве случаев заполняет пробелы в праве, осуществляет регулирование в условиях разнообразия правовых систем, готовит социальный запрос на создание юридически обязательных норм, создаёт связку между моралью и правом в киберсреде. Вместе с тем «мягкое право» имеет изъяны, так, например: отсутствие санкций ведёт к игнорированию установленных правил; решения по отдельным вопросам отношений принимаются технократами или НПО без согласования с пользователями интернета; доминирует авторитарный подход, учитывающий прямую или косвенную выгоду компаний при принятии технологических решений. **«Мягкое право» – это правовой феномен, отражающий переход от иерархических норм к сетевым стандартам, оно действует через убеждение, репутацию и косвенное давление, оставаясь важным инструментом в условиях неопределённости и быстрых технологических изменений.**

Подводя итог, отмечаем, что правовая природа отношений в киберпространстве определена его специфическими характеристиками как виртуальной среды, что порождает уникальные по своей структуре и содержанию отношения, требующие разработки новых подходов к правовому регулированию. Существующая правовая неопределенность в квалификации таких ключевых феноменов, как цифровая идентичность, смарт-контракты, системы искусственного интеллекта, кибернетическая легитимность и «мягкое право», является системным препятствием для формирования эффективных правовых механизмов. Преодоление данного правового вакуума требует реализации комплекса доктринальных и нормотворческих мер, направленных на адаптацию правовой системы к цифровой реальности. Приоритетными направлениями такого совершенствования являются:

1. Формирование комплексной межотраслевой концепции регулирования отношений в киберпространстве, интегрирующей нормы различных отраслей права (гражданского, уголовного, административного, международного) для преодоления фрагментарности существующих подходов и адекватного учета гибридного характера цифровых отношений;

2. Законодательное закрепление принципа технологической нейтральности, согласно которому правовое регулирование отношений должно быть направлено не на конкретные технологии (например, блокчейн), а на функции и правовые последствия их применения, что обеспечит долгосрочную релевантность правовых норм;

3. Легитимация «мягкого права» в качестве вспомогательного источника регулирования, предполагающая придание корпоративным кодексам и отраслевым стандартам статуса правовых ориентиров для правоприменительной и судебной практики в условиях правовых пробелов;

4. Создание новых правовых институтов, адекватных цифровой среде, в частности института «цифрового доверенного лица» — специализированного субъекта, уполномоченного на представительство интересов пользователей, управление «цифровым наследием» и контроль за исполнением алгоритмических решений;

5. Внедрение презумпции прозрачности алгоритмов для публично значимых сервисов, обязывающей операторов платформ, оказывающих существенное влияние на реализацию прав граждан, обеспечивать раскрытие принципов функционирования своих алгоритмов и возможность их независимого аудита.

Реализация указанных предложений будет способствовать формированию гибкой, адаптивной и предсказуемой правовой среды, адекватной динамичному развитию цифровых общественных отношений.

1.3 Неюридические регуляторы отношений в киберпространстве как составные элементы системы полинормативного регулирования

Киберпространство, возникшее как территория цифровой свободы, эволюционировало в сложную систему полирегуляторного регулирования. Традиционные правовые инструменты, опирающиеся на государственное принуждение и территориальный суверенитет, при столкновении с децентрализованностью, трансграничностью и скоростью изменений цифровой

среды не всегда способны эффективно регулировать отношения в киберпространстве, что подталкивает к поиску иных механизмов.

Неправовые регуляторы представляют собой совокупность социальных норм, технических стандартов, рыночных механизмов и иных, не исходящих непосредственно от государственной власти в установленных правовых формах, но оказывающих систематическое воздействие на поведение пользователей в процессе цифрового взаимодействия. Их функционирование в киберпространстве имеет свою специфику. Техническая инфраструктура интернета сама по себе выступает регулятором, протоколы связи (TCP/IP), системы адресации (DNS), стандарты шифрования, архитектура платформ – все это предопределяет возможности и ограничения действий пользователей часто жестче, чем правовые предписания. Код может становиться законом в киберпространстве, устанавливая де-факто обязательные правила доступа, взаимодействия и конфиденциальности. Социальные нормы и нормы сетевого этикета формируются в виртуальных сообществах (форумах, соцсетях, игровых мирах, профессиональных чатах) спонтанно, через практику взаимодействия и механизмы общественного одобрения или порицания. Они регулируют общение, разрешение споров, определение статуса, допустимый контент. Их санкции включают публичное осуждение, исключение из сообщества или блокировку аккаунта администрацией платформы, что может иметь значительные социальные и экономические последствия для индивида.

Очевидно, что игнорирование неправовых механизмов ведет к формированию неполной, а зачастую и неверной картины отношений в сети, а также к разработке неэффективных или контрпродуктивных законодательных мер. Ключевая научная проблема заключается в том, чтобы идентифицировать неправовые регуляторы, описать их сущность, механизмы воздействия, установить сложное, диалектическое взаимодействие как между собой, так и с традиционной правовой системой.

Одним из первых проводников альтернативного урегулирования отношений в киберпространстве являлся Лоуренс Лессиг.[1] Основа его концепции базировалась на идее, что регулирование отношений пользователей сети должно происходить не только традиционными правовыми средствами, но также включать архитектурные особенности сетевых технологий, социальные нормы и рыночные механизмы. Автор утверждал, что отношения в киберпространстве контролируются четырьмя взаимосвязанными механизмами: законом, выраженным в формальных правовых нормах, рынком, базирующимся на экономических стимулах и санкциях, нормами, включающими социальные и этические правила сообществ, и архитектурой, синтезирующей в себе технические компоненты, такие как код, алгоритмы, протоколы, интерфейсы и иное. Его концепция выражена в тезисе «код — это закон» (Code is Law).

Л. Лессиг констатировал, что программная архитектура определяет возможности и ограничения пользователей жестче, чем юридические нормы. При этом архитектурные аспекты опираются на технические решения, встроенные непосредственно в структуру интернета. Это может быть система идентификации пользователей, ограничение доступа к определенным ресурсам или использование специальных протоколов безопасности. Например, такие технологии, как IP-трекеры, системы фильтрации контента или блокировка рекламы влияют на поведение пользователей, создавая ограничения и возможности, аналогичные юридическим нормам.

Автор не отрицал, что правовое регулирование остается важным элементом контроля над отношениями в цифровом пространстве. Законы устанавливают рамки допустимого поведения, определяют ответственность за нарушения и обеспечивают защиту интересов различных групп пользователей. В то же время Лессиг доказывал, что традиционные правовые инструменты оказываются неэффективными в условиях быстрого развития цифровых технологий.

[1] Lessig L. Code and other laws of cyberspace, Version 2.0. – New York: Basic Books. – 2006. – 391 p.

Законотворческие органы сталкиваются с трудностью адаптации законодательства к новым реалиям цифровой среды.

Таким образом, концепция Лессига сводила четыре взаимодополняющих элемента регулирования: архитектуру, социальные нормы, рынок и право в единую схему, где каждый элемент дополнял другой. При этом автор отдал предпочтение коду, который он ставил в рамки закона. Его подход с позиции теории права подчеркивал важность понимания природы права, киберпространства и особенностей человеческого поведения в нём, очевидно, что исследователь акцентировал внимание на доминировании архитектурного регулирования над формально-юридическим.

Мы не разделяем позицию Лессига и полагаем, что в условиях цифровой реальности неправовые регуляторы отношений в киберпространстве лишь в связке с нормами права позволяют достичь максимального эффекта и создать благоприятные условия для решения значительного числа проблем, возникающих в процессе виртуальных отношений в интернет пространстве. Исследование неправовых регуляторов выявляет их незаменимую роль в обеспечении стабильности и предсказуемости взаимодействия в цифровой среде, особенно по скорости и оперативности принятия решений. Считаем, что неправовые регуляторы заполняют пробелы в законодательстве, особенно в новых, быстро развивающихся областях (криптовалюте, метавселенной, системах искусственного интеллекта). Они могут опережать законодательный процесс, предоставляя оперативные решения в урегулировании отношений в киберпространстве.

В то же время есть риски возникновения конфликтов, когда корпоративные правила могут противоречить национальному законодательству или правам человека, стандарты, разработанные в одной юрисдикции, могут де-факто навязываться глобально по всей сети, сетевые правила, принятые в социальных сетях (особенно закрытых), могут игнорировать национальное право.

В подобных условиях правовая система обладает необходимым инструментарием для адекватной реакции на деструктивные процессы и явления в киберпространстве, инкорпорируя, легитимируя или ограничивая влияние

неправовых регуляторов, когда их действие вступает в противоречие с основополагающими правовыми установками, что реализуется через такие механизмы, как законодательное закрепление требований к транспарентности алгоритмов, установление надзора за цифровыми платформами в качестве «хранителей информации» и придание техническим стандартам статуса де-юре.

Взаимодействие неправовых регуляторов с правовыми в киберпространстве позволяет актуализировать некоторые положения теории права:

а) позиции чистого нормативизма утрачивают объяснительную силу в киберпространстве, поскольку игнорируют регулирующее воздействие архитектуры кода, экономических стимулов и социальных норм. Способность права выступать регулятором всего спектра отношений в киберпространстве зависит не только от его внутреннего совершенства и государственного принуждения, но и от его возможности интегрироваться в сложную экосистему виртуального пространства. Например, защита персональных данных не ограничивается принятием закона о защите конфиденциальности, но также должна учитывать архитектуру информационной системы и экономические стимулы для соблюдения требований безопасности. Эффективность права определяется не только качеством нормативных актов и возможностью государства обеспечить их исполнение, но и способностью встраиваться в существующую экосистему виртуальных взаимодействий. Это означает необходимость интеграции правовых механизмов с техническими средствами защиты и социальными нормами поведения пользователей сети;

б) наблюдается тенденция смещения от государственных запретов к полицентричному проектированию среды, где корпоративные правила как форма архитектурно-нормативного регулирования становятся инструментом опережающего воздействия. Традиционный подход, основанный на запретах, утрачивает свою эффективность в условиях динамично развивающейся цифровой экономики. Примером такого подхода является использование технических решений, препятствующих распространению вредоносного ПО, или введение

финансовых санкций против недобросовестных поставщиков услуг в киберторговле и иные;

в) меняются подходы к «мягкому праву» и саморегулированию, включающим корпоративные правила цифровых платформ, профессиональные этические кодексы и технические стандарты, которые оказывают существенное влияние на регулирование отношений в цифровом пространстве. Эти инструменты дополняют формальное законодательство и помогают заполнять пробелы в тех областях, где традиционные законы оказываются неэффективными. Например, большинство крупных социальных сетей имеют собственные внутренние регламенты и процедуры разрешения споров, позволяющие оперативно реагировать на возникающие проблемы, не дожидаясь вмешательства государственных органов.

г) формируется новая парадигма правопонимания. Право перестаёт восприниматься исключительно как инструмент прямого контроля отношений в виртуальном пространстве, оно признаётся лишь одним из многих регуляторов общественных отношений наряду с технологиями, экономическими механизмами и социальными нормами. Основная задача права заключается не столько в обеспечении полного контроля, сколько в установлении общих правил регулирования отношений, создании условий для гармоничного сосуществования различных внеправовых регуляторов, поддержке равновесия между интересами разных групп пользователей в киберпространстве.

Таким образом, взаимодействие неправовых регуляторов с правом подчёркивает ключевые тенденции современного развития права в цифровом обществе, что противоречит концепции Лоуренса Лессига «код – это закон», которая акцентировала внимание на доминировании архитектурного регулирования над формально-юридическим в условиях, когда технические ограничения превосходят санкции.

Необходимо констатировать, что концепция Лоуренса Лессига подвергалась критике со стороны оппонентов. В качестве альтернативной точки зрения можно привести позицию Беннетт Мозес, которая рассматривала ограничения,

возникающие при попытке установления автоматического управления поведением посредством цифрового кода. Она доказала, что аналитические инструменты и компьютерные модели полны неопределённости и ошибок, и потому их влияние на общество далеко не однозначно предсказуемо. [1]

Группа исследователей из Оксфордского университета в составе Ван Дейка, Д. Поелла, Т. де Ваала оспорила идею о полной власти технологического кода над социальными процессами, показав, что использование платформ и алгоритмов регулируется разнообразием субъектов и институциональных рамок. Платформы не действуют изолированно, а встраиваются в существующие политические, экономические и правовые условия.[2]

В работе Дэниела Деннета отмечалось, что абсолютизация тезиса «код — это закон» создаёт ряд проблем. По мнению автора, такое упрощение ситуации ведёт к снижению контроля над технологиями и передаче ответственности за последствия исключительно пользователям. Исследователь считал, что технология предопределяет человеческие действия, неверно. Пользователь способен действовать свободно и адаптироваться к среде, применяя технологии не по назначению или находя пути обхода ограничений. Технологические разработки не существуют изолированно от общества, а формируются в тесной связи с ним, учитывая экономические, политические и культурные факторы.[3]

Примеры иллюстрируют многообразие подходов к критике идеи Лессига о способности кода определять общественную реальность и поведение индивидов. Оппоненты демонстрируют сложность и ограниченность такого подхода, предлагая рассматривать воздействие цифровых инструментов в более широком контексте социальных отношений и институтов.

---

[1] Bennett Moses, L. The Limits of Predictive Analytics in Policing: A Critical Analysis of the Use of Big Data for Crime Prevention / L. Bennett Moses // Big Data & Society. – 2018. – Vol. 5, no. 2. – P. 1–17.

[2] Van Dijck J., Poell T., de Waal M. The platform society: public values in a connective world. – New York : Oxford University Press, 2018. – 209 p.

[3] Dennett D. C. The Part of Cognitive Science That Is Philosophy // Topics in Cognitive Science. – 2009. – Vol. 1, № 2. – P. 231–236.

В частности, постмодернисты утверждали, что технологические системы, включая программное обеспечение и цифровые платформы, сами являются продуктами социальной конструкции и исторического контекста. Они подчёркивали, что техническая инфраструктура не существует вне социально-экономической среды, а её развитие обусловлено множеством факторов: культурными практиками, экономическими интересами корпораций, политическими решениями государств и международными отношениями. Согласно этому подходу, программа или код не диктуют автоматически определённое поведение, а наоборот, подвергаются множеству интерпретаций и адаптаций пользователями, разработчиками и регуляторами.

Код формируется и развивается внутри конкретного социального и культурного контекста, отражающего интересы доминирующих акторов (корпораций, государства). Даже самые жёстко прописанные алгоритмы допускают возможность обхода, взлома или альтернативных способов взаимодействия.

Исследователи Science and Technology Studies (STS) рассматривали технологию не как автономную силу, определяющую человеческое поведение, а как неотъемлемый элемент сложных сетей взаимодействий между людьми, организациями и институтами. Ключевое положение STS состоит в том, что технические артефакты, такие как программы и устройства, встроены в социальные структуры и зависят от множества субъективных решений и культурных практик.

Явно просматривается суть критики концепции Лессига, состоящая в утверждении, что техническое регулирование поведения пользователей сети не является абсолютным и неизменным. Его эффективность зависит от целого ряда факторов: социальной инфраструктуры, культурных норм, экономического положения, политических условий и индивидуального выбора пользователей. Поэтому важно учитывать многослойность воздействия цифровой архитектуры на повседневную жизнь, принимая во внимание разнообразие возможных сценариев взаимодействия человека и технологий.

Сравнивая регулирование отношений в киберпространстве правовыми и неправовыми способами очевидно, что сущность кода как регулятивного инструмента в киберпространстве заключается в том, что он осуществляет воздействие не через предписания и угрозу санкций, как закон, а через прямое создание или ограничение возможностей на уровне технической архитектуры. Это фундаментально иной, детерминистский способ регулирования отношений, существующий вне традиционной правовой системы. Код действует по принципу «невозможно ≠ запрещено». Если действие технически невыполнимо, например, отправка транзакции без приватного ключа, оно исключено. Право же запрещает действия, но не делает их физически невозможными.

Разработчики создают код без публичного обсуждения в отличие от закона, который публикуется в официальных источниках. Код предотвращает нарушение правил до действия (ex ante), а не наказывает за него (ex post).

Код является технологическим инструментом и затрагивает различные аспекты технической реализации и функционирования информационных систем, веб-приложений, онлайн-сервисов и прочих цифровых ресурсов. Под кодами понимаются технические стандарты, алгоритмические правила программирования и инженерные спецификации, используемые в разработке программного обеспечения, технологий и оборудования. Они отражают технологические требования, функциональные возможности устройств и ПО, решают конкретные прикладные задачи и обеспечиваются практическими методами реализации.

Коды создают условия функционирования инфраструктуры киберпространства, определяют правила поведения пользователей, обработки данных и взаимодействия между ними. Они являются продуктом инженерных решений, в то время как правовые регуляторы – результатом деятельности органов государственной власти. Правовые регуляторы устанавливают обязательные нормы поведения, определяющие права и обязанности субъектов правоотношений. Их принятие сопровождается официальными процедурами, предусмотренными конституцией и законодательством страны.

Архитектура в киберпространстве формирует саму структуру возможностей и ограничений для всех участников отношений. Она определяет, что допустимо через проектирование среды, алгоритмические ограничения и семиотические системы. Например, архитектура виртуальных сред задает правила поведения через навигационные паттерны, лабиринтную структуру сайтов или игр, направляет движение пользователей, ограничивая свободу выбора. Зонирование позволяет делить цифровое пространство на «публичные» форумы и «приватные» личные сообщения.

Названные элементы могут ограничивать возможности пользователей действовать определенным образом. Например, закрытые форумы требуют регистрации перед участием, фильтры комментариев исключают публикации определенных сообщений. Такие ограничения задают негласные нормы общения и взаимодействия в сообществе. Интерфейсы социальных сетей создают эталоны визуальных стандартов, которым следуют пользователи.

Анализ архитектуры как инструмента регулирования подтверждает выводы Лоуренса Лессига о том, что структура компьютерных систем и программное обеспечение сами по себе выступают источниками регулирования.

Технологическое регулирование имеет свои механизмы сдерживания посредством алгоритмического управления. Характерными примерами являются: TikTok, использующий систему искусственного интеллекта для контроля контента через «теневой банинг» (shadow banning) – невидимое пользователю ограничение охвата; смарт-контракты в DeFi, обеспечивающие автоматическое исполнение условий, в случае падения курса криптоактива в протоколе Aave происходит блокировка залога; архитектура CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) — полностью автоматизированный публичный тест Тьюринга для различения компьютеров и людей, представляющий метод верификации пользователей, позволяющий отличить реальных людей от автоматизированных программ (ботов); DRM (Digital Rights Management) управление цифровыми правами — технология управления цифровыми правами, используемая для реализации норм авторского права на практике путем

предотвращения несанкционированного копирования, распространения и модификации защищённых объектов интеллектуальной собственности. Она обеспечивает соблюдение законодательства путём внедрения специальных мер технического характера, позволяющих контролировать доступ к контенту и ограничить незаконное использование авторских произведений и других.

Безусловно, регулирование отношений в киберпространстве посредством кода и архитектуры имеет свои плюсы и минусы. В качестве позитивного можно выделить высокую степень контроля и предсказуемость поведения пользователей в сети. Благодаря мониторингу и управлению соблюдаются установленные правила всеми участниками отношений в киберпространстве, обеспечивается безопасность, возможность оперативного реагирования на угрозы.

К недостаткам отнесём: ограничение свободы действий пользователей и устройств; зависимость от органов управления платформой, которые формируют политику отношений, что может стать уязвимостью в случае сбоев или атак; сложность масштабирования, особенно в крупных сетях.

Из вышеизложенного вытекает, что регулирование отношений в киберпространстве опирается на программный код, который формирует цифровую «материю», предопределяя возможности действий, а императивная конструкция интернета обеспечивает высокий уровень управления и безопасности, но также накладывает значительные ограничения на свободу и гибкость пользователей.

Группа социальных регуляторов отношений в киберпространстве, определённая Лессигом, представляет систему неписаных правил, норм поведения, этических установок и ценностей, которые возникают, поддерживаются и применяются самими участниками онлайн-взаимодействий для упорядочения их совместной деятельности. В отличие от правовых установок, основанных на принудительной силе закона, социальные кибернетические регуляторы базируются на добровольном принятии сообществом правил, социальном одобрении или осуждении.

Одной из особенностей названных регуляторов является то, что они заполняют правовые вакуумы, которые неизбежно возникают в

быстроразвивающейся и трансграничной цифровой среде. Там, где закон не актуален, работают социальные нормы.

Для понимания социальных механизмов неюридического регулирования в виртуальном пространстве целесообразно выделить некоторые доктринальные подходы и направления исследований. В качестве основополагающих рассмотрим социологический и антропологический подходы, они смещают фокус с формальных законов на живые социальные практики, нормы и культурные коды, которые зачастую оказываются более влиятельными регуляторами.

Социологический подход рассматривает интернет-пространство как новую социальную структуру, внутри которой формируются и функционируют собственные социальные институты, нормы, статусы и роли. С этой точки зрения, регулирование происходит через механизмы социального контроля, взаимодействия в группах и влияние крупных цифровых платформ как новых центров власти.

Один из последователей данного направления Мануэль Кастельс в трилогии «Информационная эпоха: экономика, общество и культура» ввёл понятие «сетевое общество» (network society), обосновал суждение о том, что сети стали доминирующей формой социальной организации. В такой структуре регулирование осуществляется через логику сети, потоки информации и взаимодействие узлов, а не через традиционные правовые институты.[1]

Говард Рейнгольд в книге «Виртуальное сообщество» одним из первых описал, как люди в сети формируют устойчивые социальные группы со своими нормами, культурой и механизмами саморегулирования, доказал, что онлайн-общение способно создавать реальную социальную солидарность. Любое онлайн-сообщество (форум, группа в соцсети, игровая гильдия) вырабатывает собственный набор норм и правил. Регулирование осуществляется через механизмы социального контроля: поощрение за соблюдение норм (лайки, репосты, повышение статуса) и санкции за их нарушение (осуждение, «бан», исключение из

[1] Кастельс М. Информационная эпоха. Экономика, общество и культура. – М.: Изд. дом Гос. ун-та Высш. шк. экономики, 2000. – 607 с.

группы). Эти неформальные правила часто оказываются более действенными, чем формальные законы.[1]

Представители социологического подхода рассматривали крупные цифровые платформы (Google, Meta, Amazon) не просто как бизнес, а как частные институты власти, которые устанавливают свои собственные правила (Terms of Service) и через алгоритмы управляют поведением миллиардов людей. Их власть сопоставима, а порой и превосходит, власть государств.

Голландский профессор медиаисследований Ян ван Дейк указал на важную роль крупных корпораций в процессе формирования нового типа общественных связей и институтов власти в сетевом обществе. В работе «Сетевое общество»[2] он раскрыл, как корпорации Google и Facebook (продукты компании Meta, деятельность которой признана экстремистской и запрещена в РФ) формируют структуру виртуального взаимодействия и влияют на власть в обществе.

Феномен цифровых платформ как базовую основу современных экономических и социальных взаимоотношений раскрыли Альфред Моазед и Николас Джонсон. Они утверждали, что цифровые платформы, устанавливая свои правила, оказывают значительное воздействие на устройство общества и распределение власти, тем самым формируют новые социальные механизмы управления.[3]

Актуальность концепции «Платформенного Государства» («State as a Platform») отмечала Эва Хоффманн, предлагавшая интеграцию цифровых платформ в государственное управление. Она указывала на способность платформ существенно менять способы принятия решений и функционирования государственных органов. По существу, автор раскрыла механизм виртуального

---

[1] Рейнгольд Г. Виртуальное сообщество / Говард Рейнгольд; пер. с англ. А. Е. Марьяновского; под науч. ред. К. В. Костюка. – М.: Фаир-Пресс, 2012. – 430 с.

[2] Ван Дейк, Ян А. Г. М. Сетевое общество / Ян ван Дейк; пер. с англ. М. В. Немировского. – М.: Фаир-Пресс, 2004. – 400 с.

[3] Моазед А., Джонсон Н. Революция платформ: как сетевые рынки преобразовывают экономику и как заставить их работать на вас / пер. с англ. М. Волынкина. – М.: Альпина Паблишер, 2019. – 288 с.

социального управления, основанного не на правовых регуляторах, а на правилах платформ.[1]

В книге Шошана Зубоффа «Век надзорного капитализма» изложено авторское видение того, как бизнес-модель «надзорного капитализма», представляющего неправовой механизм регулирования, действующий на уровне глубинного социального инжиниринга, приводит к формированию новой, «инструментарной» власти, использующей платформы для управления не через запреты, а через тонкую настройку цифровой среды (архитектуру), предсказывая и направляя поведение пользователей в коммерческих интересах.[2]

В отличие от социологического подхода антропологический подход описывает человеческое поведение, культурные особенности и смыслы, возникающие в процессе интернет отношений. Основное внимание уделено восприятию интернет-взаимодействий разными культурами, народами и социальными группами, а также рассмотрению специфики коммуникации и возникновения собственных правил и норм, характерных именно для интернет-среды. Антропологический подход к регулированию отношений в интернете кардинально отличается от юридического или чисто социологического. Его суть заключается в рассмотрении интернет-пространства не как технической системы или набора правовых норм, а как культурной среды — своего рода «цифрового поля», где люди создают, переживают и трансформируют свои культуры, ценности, ритуалы и идентичности.

С точки зрения этого подхода, поведение людей в сети регулируется не столько формальными законами или экономическими стимулами, сколько неписаными культурными кодами, символическими системами, ритуализированными практиками и групповыми нормами, которые формируются и поддерживаются внутри самих онлайн-сообществ.

---

[1] Hoffmann E. State as a Platform // Journal of Public Administration Research and Theory. – 2018. – Vol. 28, No. 4. – P. 653–670.

[2] Зубофф Ш. Эпоха надзорного капитализма: борьба за человечество на новом рубеже цифровой цивилизации / Ш. Зубофф ; пер. с англ. А. С. Назарова. – М.: АСТ, 2020. – 688 с.

В качестве базового постулата антропологического подхода можно рассматривать представления о праве, справедливости и порядке в виртуальном мире через «цифровые племена» (Digital Tribes). В онлайн-сообществах (игровых гильдиях, группах в социальных сетях, тематических форумах, сабреддитах) выстраиваются отношения по аналогии с традиционными «племенами». Эти группы обладают всеми признаками культурной общности: у них есть собственный язык – сленг, мемы выступающие маркером принадлежности к группе. Понимание этого языка регулирует коммуникацию и отделяет «своих» от «чужих».

Необходимо констатировать, что стремление индивида быть принятым в такое «цифровое племя» и поддерживать свой статус заставляет его соблюдать неписаные нормы этого сообщества гораздо строже, чем формальные законы, так как санкцией является не штраф, а социальное исключение (остракизм), что для человека как социального существа является мощнейшим наказанием.

Шерри Тёркл провела антропологический и психологический анализ того, как интернет-среда влияет на формирование человеческой идентичности. Она показала, что киберпространство — это не просто инструмент, а «лаборатория для самоконструирования», где люди экспериментируют с различными аспектами своего «я». Её работа доказывает, что идентичность в сети не дана, а создается в процессе социального взаимодействия, а значит, регулируется культурными нормами этого взаимодействия.[1]

Автор книги «Приход в век виртуальный: этнография во второй жизни» исследователь Том Бёллсторф провел классическое антропологическое включенное наблюдение, прожив более двух лет в виртуальном мире «Second Life» под видом своего аватара. Он доказал, что виртуальные миры — это не игры, а полноценные человеческие культуры, в которых есть свои нормы, экономика, ритуалы, формы брака и даже конфликты, регулируемые внутрисоциальными механизмами. Он показал, как сообщество само вырабатывает нормы для решения

[1] Тёркл Ш. Жизнь на экране: идентичность в эпоху Интернета / Шерри Тёркл ; пер. с англ. А. Н. Алексеева. – М.: Фонд «Общественное мнение», 2014. – 432 с.

споров о виртуальной собственности или аморальном поведении без всякого вмешательства государственного права.[1]

Исходя из представленных суждений можно сделать вывод, что антропологический подход помогает глубже понять культурные и поведенческие факторы, определяющие формирование и соблюдение негласных правил в интернет-пространстве, создавая основу для эффективного и осознанного самоуправления. Исследователи этого направления доказали, что социальные нормы в конкретных онлайн-сообществах регулируют весь спектр отношений, возникающих в данной среде, а правила игровых кланов, этика социальных сетей представляют форму социального саморегулирования, замещающего формальные правовые механизмы.

Проведенный анализ, основанный на социологическом и антропологическом подходах к изучению социальных механизмов, позволяет сделать вывод о том, что социальные нормы, регулирующие отношения в киберпространстве, представляют собой не монолитное, а сложное, динамичное явление. Они характеризуются внутренней дифференцированностью, высокой степенью контекстуальной зависимости и способностью к оперативной адаптации к изменениям в цифровой среде, что отличает их от формально-определенных и иерархически выстроенных норм позитивного права.

Рыночные механизмы — это ещё один эффективный неюридический регулятор отношений в интернет пространстве. Посредством их применения осуществляется воздействие на отношения пользователей не через прямое принуждение или моральные нормы, а через экономические стимулы и ограничения, встроенные в саму архитектуру и бизнес-модели цифровых торговых платформ и иные рыночные инструменты, используемые в виртуальной экономике.

Рынок является жестким регулятором отношений в виртуальном пространстве, создавая условия для непрерывной борьбы за пользователя, его

[1] Boellstorff T. Coming of age in Second Life: an anthropologist explores the virtually human. – New Jersey: Princeton University Press, 2008. – 336 p.

внимание и данные. Эта конкуренция заставляет компании усовершенствовать архитектурные решения (код) и внутренние правила, которые напрямую регулируют поведение пользователей гораздо эффективнее, чем формальные законы. Все структурные элементы названного механизма формируются непосредственно потребителями, поставщиками услуг и платформами на базе саморегулирования. В основе механизма лежит борьба за потребительские предпочтения, качество услуг и скорость их реализации. Интернет-компании конкурируют друг с другом за внимание пользователей, что стимулирует развитие инноваций, улучшение качества сервисов и повышение уровня обслуживания пользователей.

Специфика рыночных механизмов регулирования отношений в киберпространстве в том, что они основаны на взаимодействии спроса и предложения, инициативности участников рынка и предпочтениях пользователей. Такие механизмы формируются вне формальных правовых норм и государственных институтов, позволяя субъектам самостоятельно устанавливать правила, адаптируясь к меняющимся условиям рынка и ожиданиям пользователей.

Можно выделить несколько ключевых аспектов, раскрывающих специфику рыночного регулирования отношений в киберпространстве.

Первый. В отличие от государственного правового регулирования, действующего через формальные предписания и угрозу санкций, рыночное регулирование отношений в киберпространстве происходит через формирование самой виртуальной среды и манипуляцию пользовательским интересом, где конечной целью является не общественное благо или справедливость, а коммерческая выгода.

Второй. Рынок формирует собственные стандарты качества и взаимодействия путем проб и ошибок, адаптации к интересам пользователей и реагирования на изменения цифровой среды. Такой механизм делает рынок гибким, приспосабливающимся к новым технологиям и тенденциям. В основе лежит концепт саморегуляции.

Третий. Отсутствие единой нормативной базы открывает простор для экспериментирования и инноваций. Платформы и сервисы свободно разрабатывают уникальные индивидуальные подходы, позволяющие занять лидирующую позицию на рынке.

Четвертый. Основным фактором успеха является репутация и уровень доверия пользователей. Нарушение правил пользования персональными данными или внедрение вредоносных практик влечет потерю клиентской базы гораздо быстрее, чем юридические санкции.

Пятый. Ценность каждой платформы определяется уникальностью предлагаемых функций, качеством предоставляемых услуг и эффективностью бизнес-модели. Платформа должна постоянно обновляться, улучшать продукт и искать новые способы привлечения и удержания пользователей.

Шестой. Рыночная саморегуляция часто оставляет пространство для злоупотреблений и эксплуатации слабостей пользователей. Отсутствуют строгие обязательства перед клиентами, кроме тех, которые добровольно принимаются самими компаниями. Поэтому чрезмерная зависимость от неписаных рыночных правил может приводить к неравному положению сторон.

Седьмой. Технологические новшества требуют постоянных изменений подходов к работе с информацией и защите персональных данных. Альтернативные механизмы позволяют оперативно реагировать на появление новых угроз, не дожидаясь внесения изменений в законодательство.

Резюмируя изложенное, можно сделать вывод, что отношения в киберпространстве помимо прочего регулируется алгоритмизированными рынками, где доверие возникает из репутационных рейтингов, а не юридических гарантий; нарушители исключаются экономически с потерей дохода, а не через суд; правила диктуются архитектурой платформ, а не законодателями.

В исследовательской среде рыночное регулирование отношений в виртуальном пространстве рассматривается под разными ракурсами, что позволяет сделать ряд объективных выводов. Так, например, Эдвард Кастронова в работе

«Синтетические миры: Бизнес и культура онлайн-игр»[1] раскрыл экономические аспекты виртуальных миров и влияние рынка на развитие и функционирование онлайн-игр. Автор представил экономику виртуальных пространств как новую отрасль, зависящую от микроэкономики и макроэкономики, приводящую к созданию сложных экономических моделей, параллельных традиционным рынкам. Он отметил, что регулирование экономических отношений в виртуальном пространстве строится на принципиально иных алгоритмах и не зависит от внешнего правового воздействия.

Проблема формирования репутации в цифровой среде и её влияние на рыночное состояние кампаний стимулировала многих авторов к исследованиям в этой области. Среди отечественных работ можно выделить материал группы авторов,[2] в котором представлен анализ существующих инструментов управления репутацией компании, выявлены эффективные инструменты управления деловой репутацией, показаны ошибки, раскрыты последствия потери репутации в интернете для бизнеса.

Тема формирования доверия в интернет-среде как способа поддержания рейтинга продавца затронута А. Л. Дыдыкиным:[3] автор раскрыл механизм электронной репутационной системы на примере торговой площадки eBay, в основу которой положен рейтинг продавца. Автор подчеркнул, что на маркетплейсе с большей вероятностью совершаются сделки с продавцами, у которых высокий рейтинг и много положительных отзывов. Желание поддерживать хорошую репутацию мотивирует субъектов действовать честно и выполнять свои обязательства даже при отсутствии прямого юридического

---

[1] Castronova E. Synthetic Worlds: The Business and Culture of Online Games. – Chicago; London: The University of Chicago Press. – 2005. – 332 p. – URL: https://www.researchgate.net/publication/37691974_Synthetic_Worlds_The_Business_and_Culture_of_Online_Games (дата обращения: 12.04.2025).

[2] Плотников А.В., Иванова А.Н., Боровых К.О., Ощепков А.М. Управление репутацией компании в интернете: инструменты управления репутацией, их применение и оценка эффективности // Креативная экономика. – 2021. – Т. 15, №10. – С.3823-3838.

[3] Дыдыкин А.Л. Электронные репутационные системы и доверие в интернет-среде // Вопросы государственного и муниципального управления. – 2013. – № 4. – С. 135–144.

принуждения. Сделан вывод, что репутационные системы являются эффективным неправовым регулятором, способствующим развитию электронной коммерции.

В статье «Системы репутации»[1], подготовленной авторским коллективом, представлено суждение о репутационных системах как ключевом механизме поощрения добросовестного поведения в онлайн-сообществах. В публикации описан дизайн системы, показана её уязвимость, предложены способы повышения репутации, раскрыты негативные последствия потери репутации в цифровом пространстве, что может привести к закрытию бизнеса. Данный факт свидетельствует о том, что репутация является инструментом социального контроля, где сообщество само, без участия государства, «наказывает» нарушителей через снижение их репутации и «поощряет» добросовестных участников через ее повышение.

Репутация формируется на основе множества сигналов, включая количество подписчиков, активность и качество публикуемого контента. Платформы внедряют специальные механизмы для улучшения качества репутационных индикаторов. Положительные репутационные сигналы повышают вероятность успеха в социальных медиасредах.

Помимо репутационного воздействия рыночные механизмы киберпространства включают множество компонентов, позволяющих обеспечить процесс саморегуляции, основываясь на правилах, доказавших свою высокую эффективность в обеспечении стабильности и надежности операций в киберпространстве, компенсируя недостаток формальных правовых институтов и повышая доверие между пользователями – участниками рыночных отношений. Саморегулируемые сообщества выполняют важные функции, замещая или дополняя государственные структуры и институты права.

Подводя итог, можно сделать вывод: взаимодействие неправовых регуляторов с правовыми в киберпространстве демонстрирует ограниченность классического нормативистского подхода, поскольку эффективность правовой

[1] Resnick P., Zeckhauser R., Friedman E., Kuwabara K. Reputation systems // Communications of the ACM. – 2000. – Vol. 43, no. 12. – P. 45–48.

нормы зависит не только от государственного принуждения, но и от её интеграции в систему, включающую архитектуру кода, экономические стимулы и социальные нормы. Это приводит к смене регуляторной парадигмы: происходит смещение акцента от традиционных запретов к проектированию цифровой среды, в которой нежелательное поведение становится технически невозможным или экономически невыгодным. Возрастает роль «мягкого права» и корпоративного саморегулирования, которые заполняют пробелы быстрее, чем формальное законодательство.

Право в киберпространстве перестает быть единственным регулятором, превращаясь в один из элементов сложной, полинормативной системы. Его основная задача трансформируется от установления запретов и дозволений к созданию условий для гармоничного сосуществования различных регуляторов и защите фундаментальных ценностей.

Киберпространство является яркой иллюстрацией правового плюрализма – сосуществования множества нормативных порядков в одном социальном, виртуальном пространстве. Эти порядки взаимодействуют, конкурируют, дополняют или противоречат друг другу. Их изучение в контексте теории права требует выхода за рамки позитивизма. Ключевые теоретико-правовые проблемы заключаются в обеспечении легитимности, подотчетности и совместимости этих неюридических регуляторов с фундаментальными правами человека и демократическими принципами. Будущее эффективного регулирования отношений в киберпространстве видится не в вытеснении неюридических регуляторов правовыми регламентами, а в поиске сбалансированных моделей их взаимодействия, например, полинормативной системы, где право задает общие рамки и гарантии, а технические, корпоративные, социальные и рыночные механизмы обеспечивают их конкретную, гибкую и технологически грамотную реализацию.

1.4 Границы правового регулирования отношений в киберпространстве. Значение цифрового государственного киберсуверенитета

Данная проблема непосредственно затрагивает государственные интересы, что выводит её из теоретической в практическую плоскость. Демаркация границ правового регулирования отношений в киберпространстве обусловлена фундаментальными сложностями в определении территориальных, юридических и технических параметров действия правовых норм. Эти сложности порождены транснациональным характером цифровых технологий и отсутствием в виртуальной среде физических границ, традиционно служащих основой для установления юрисдикции. Указанная проблематика сохраняет свою центральную роль в современной правовой доктрине, что детерминировано уникальными характеристиками киберпространства, и обладает высокой не только теоретической, но и практической значимостью для развития цифровой экономики, обеспечения защиты прав пользователей, поддержания безопасности и эффективного разрешения споров.

В отличие от физического мира, где пределы государственного суверенитета и юрисдикции определяются на основе географических координат и международных договоров, киберпространство не обладает объективными физическими референтами для подобной демаркации. Это порождает ситуацию, в которой концепции суверенитета и юрисдикции вынуждены оперировать категориями виртуальных границ и правовых пространств, конструируемых волей государства. Таким образом, реализация государством своих правотворческих и правоприменительных полномочий в цифровой среде ставит комплекс вопросов о качественном содержании и фактических пределах его юрисдикции.

В научной литературе обозначенная проблема находит отражение в дискуссиях вокруг таких смежных, но не тождественных категорий, как «государственный цифровой суверенитет» (State Digital Sovereignty) и «суверенитет в киберпространстве» (Cyberspace Sovereignty). Как справедливо

отмечает Л. В. Терентьева, исследование данной области связано с двумя ключевыми дискуссионными направлениями: определением пределов суверенитета государства в киберпространстве и установлением оснований национальной юрисдикции в данном сегменте.[1] Несмотря на наличие значительного числа публикаций, консенсус по указанным вопросам не достигнут, что подтверждает нерешенность проблемы и обусловливает необходимость формирования авторской концептуальной позиции в рамках настоящего исследования.

Под **государственным цифровым суверенитетом** следует понимать способность государства осуществлять контроль над национальной цифровой инфраструктурой, информационными ресурсами и данными, обеспечивая независимость от внешних угроз. Названная категория интегрирует политические и социально-экономические интересы и показывает способность государства регулировать все аспекты цифровой среды в пределах своей юрисдикции, включая цифровую экономику, оборот данных, деятельность платформ и формирование культурного пространства. Основной целью обеспечения государственного цифрового суверенитета является формирование национальной цифровой автономии, минимизирующей зависимость от иностранных технологий при сохранении интеграции в глобальную цифровую экономику.

Суверенитет в киберпространстве (**киберсуверенитет**) представляет собой в большей степени технически-ориентированное понятие, сфокусированное на способности государства контролировать физическую и логическую инфраструктуру интернета (серверы, кабели, точки обмена трафиком), расположенную в пределах его территориальных границ. Он означает право государства обеспечивать защиту своих интересов и безопасности в виртуальной среде путем предотвращения кибератак и иных внешних угроз.

[1] Терентьева Л. В. Территориальный аспект юрисдикции и суверенитета государства в киберпространстве // LEX RUSSICA. – 2019. – № 4 (149). – С. 139–149.

В работе «Цифровой суверенитет как основа национальной безопасности России»[1] авторы констатировали, что его обеспечение требует защиты граждан от негативных информационных воздействий. Данная точка зрения представляется избыточно узкой, поскольку редуцирует комплексную проблему до задачи «фильтрации» информации. Государство, обеспечивая свой суверенитет, решает многоуровневый комплекс социально-политических, правовых и военно-технических задач.

В научном сообществе продолжается полемика по вопросу национального сегментирования киберпространства. Так, Я. А. Абделькарим утверждает, что соблюдение киберсуверенитета, являющегося продолжением традиционного суверенитета, – это ключевой принцип, дающий государству право противодействовать незаконной деятельности в сети. Однако автор предупреждает, что абсолютизация национального киберсуверенитета может привести к фрагментации глобального киберпространства. В связи с этим он приходит к выводу о необходимости разработки гибридного, право-технологического механизма защиты кибергранич.[2]

Альтернативная точка зрения изложена в статье «Кто контролирует киберпространство?»,[3] авторы которой аргументируют тезис об отсутствии суверенитета в его традиционном понимании ввиду безграничной природы интернета. Они предлагают адаптировать юридическое понятие суверенитета к технической сущности киберпространства. Специфическую позицию обосновал Пуку Ван, предложивший концепцию государственных интересов как детерминанты государственной власти в киберпространстве.[4] Данный тезис

---

[1] Кочетков А. П., Маслов К. В. Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе // Вестник Московского Университета. Серия 12. Политические науки. – 2022. – № 2. – С. 39.

[2] Абделькарим Я. А. Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств// Journal of Digital Technologies and Law. – 2024. – 2(2). – С. 262–285.

[3] Choucri N., Clark D. D. Who Controls Cyberspace? // Bulletin of the Atomic Scientists. – 2013. – 69(5). – P. 21–31

[4] Wang P. Principle of Interest Politics: Logic of Political Life from China’s Perspective. – Singapore : Springer Nature Singapore; Beijing: Peking University Press. – 2022. – 151 p. – URL: https://doi.org/10.1007/978-981-19-3963-1 (дата обращения: 24.01.2025).

развивает Бинсинг Фанг, по мнению которого установление политических границ в киберпространстве является выражением национальных киберинтересов.[1]

Реализация национального киберсуверенитета обычно рассматривается в контексте прикладных задач: обеспечение информационной безопасности, контроль над критической инфраструктурой, регулирование контента, локализация данных и др. По сути, киберсуверенитет раскрывает право государства определять правила оборота информации в интересах общества, а также обеспечивать иную деятельность в интернет-среде, включая торговлю, социальные контакты и иное.

Российские исследователи демонстрируют неоднородность подходов в оценке киберсуверенитета. А. Я. Капустин выделял три концепции: нигилистическую (отрицание возможности суверенитета в киберпространстве), агностическую (утверждение о неприменимости суверенитета) и прагматическую (признание заинтересованности государств в его укреплении). Исследователь констатировал, что цифровизация не отменяет, а актуализирует доктринальное обоснование суверенитета как неотъемлемого атрибута государства.[2]

Разделяя изложенную позицию, отметим ее особую актуальность в условиях современной геополитической напряженности. Одним из ключевых мотивов суверенизации киберпространства является обеспечение информационной безопасности, поскольку международные соглашения в этой сфере демонстрируют низкую эффективность.[3]

Некоторые исследователи вводят понятия «личного технологического суверенитета» (контроль индивида над своими данными) и «общего суверенитета».[4] Представляется, что данное суждение смешивает публично-

---

[1] Fang B. Cyberspace Sovereignty: Reflections on Building a Community of Common Future in cyberspace. – Singapore: Science Press and Springer Nature Singapore Pte Ltd. – 2018. – 482 p. – URL: https://doi.org/10.1007/978-981-13-0320-3 (дата обращения: 24.01.2025).

[2] Капустин А. Я. Суверенитет государства в киберпространстве: международно-правовое измерение // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 103–108.

[3] Дмитриева Н. И., Дун Ц. Суверенитет киберпространства как национальный суверенитет // Вопросы политологии. – 2022. – Т. 12, № 5(81). – С. 1577.

[4] Кутюр С., Тоупин С. Что означает понятие «суверенитет» в цифровом мире? // Вестник международных организаций. – 2020. – Т. 15, № 4. – С. 48–69.

правовую категорию суверенитета, устанавливаемого государством, с понятием «цифровой гигиены», относящимся к компетенции индивида. Полагаем, что подобный микс неуместен.

На основании вышеизложенного можно сделать вывод о том, что в оценках сегментирования и суверенизации киберпространства отсутствует консенсус. Продвижение концепции национального киберсуверенитета порождает противоречие между стремлением государства к контролю и глобальной, децентрализованной природой интернета.

Дискурс по данной проблематике включает два блока аргументации. Сторонники киберсуверенитета апеллируют к необходимости защиты национальной безопасности, персональных данных, противодействия незаконному контенту, развития отечественной ИТ-индустрии и сохранения культурной идентичности. Противники указывают на угрозы свободе слова, риски технологической изоляции, экономические потери и высокие затраты на реализацию ограничительных мер.

Резюмируя изложенное, можно выделить три основные концептуальные позиции:

а) позитивистская: признание права государства на суверенизацию национального сегмента киберпространства и его законодательное закрепление;

б) либертарианская: отрицание суверенизации как нарушения фундаментальных принципов открытости интернета, заложенных на ранних этапах его развития;

в) компромиссная: официальное непризнание тотальной суверенизации, но допущение государственного контроля над отдельными элементами цифровой инфраструктуры и контента в рамках национальной юрисдикции для решения задач безопасности. При этом вопрос о границах такой юрисдикции остается открытым.

В рамках представленной дискуссии целесообразно обратить внимание на смысловое толкование понятий киберсуверенитет и государственный цифровой суверенитет.

Можно отметить, что цифровой суверенитет включает в себя киберсуверенитет как один из важных компонентов. При этом наблюдается определенный парадокс: государство может обладать киберсуверенитетом (защищенной инфраструктурой), но не иметь цифрового суверенитета из-за зависимости от иностранного программного обеспечения и цифровых продуктов. Таким образом, суверенитет в киберпространстве выступает как техническая основа для реализации более широкого по содержанию государственного цифрового суверенитета.

В современном научном и политико-правовом дискурсе понятия «цифровой суверенитет» и «киберсуверенитет» зачастую используются как взаимозаменяемые синонимы, что ведет к размыванию их сущностного содержания и, как следствие, к неверной интерпретации. В этой связи предлагаем ввести новое понятие – **«цифровой государственный киберсуверенитет»,** что позволит отразить полноту полномочий государства относительно собственной информационной среды, охватывая контроль, защиту и регулирование всего комплекса процессов и ресурсов, включая сети связи, базы данных, вычислительные мощности и системы управления.

Консолидация терминов «цифровой суверенитет» и «киберсуверенитет» в одно общее понятие оправдано с точки зрения целостности подходов, эффективности мер и интеграции всех аспектов национального контроля и безопасности в условиях роста киберпреступлений.

Введение комплексного понятия **«цифровой государственный киберсуверенитет»** является методологически оправданным и необходимым. В нашем понимании - это **юридически обусловленная способность государства проецировать свою власть в цифровую среду для регулирования общественных отношений, возникающих в рамках установленной юрисдикции, с целью защиты прав и законных интересов пользователей (участников отношений)** он раскрывает возможность государства формировать и поддерживать правовую систему, которая динамично адаптируется к трансграничной природе цифровой среды, обеспечивая баланс интересов,

позволяет автономно регулировать деятельность в цифровом пространстве, отстаивать национальные интересы, обеспечивать безопасность информационных ресурсов и свободу коммуникации, исключая внешнее вмешательство и угрозы цифрового характера.

Предложенная дефиниция формирует целостное представление о государственной власти в цифровой среде, объединяя технические и социально-правовые аспекты в единую логически обоснованную концепцию. Цифровой государственный киберсуверенитет позволяет трансформировать национальные ценности в глобальную цифровую реальность, минимизируя диссонанс между локальными правовыми системами и транснациональными последствиями их применения.

Попробуем разобраться, как на государственном уровне реализуется цифровой государственный киберсуверенитет. Начнём с анализа российской позиции.

Для суверенизации сегмента киберпространства российские власти прибегли к правовому ограничению зависимости от глобальной инфраструктуры интернета. С этой целью были приняты соответствующие законы и иные документы.

Основным регулятором, обеспечивающим интересы государства в российском сегменте интернета, можно назвать Федеральный закон от 1 мая 2019 г. № 90-ФЗ,[1] получивший множество названий в среде пользователей из-за создания национальной системы маршрутизации интернет-трафика, инструментов централизованного управления и другого. Одно из них звучит как «Закон о суверенном Рунете».

Данный закон, по существу, актуализировал некоторые статьи Федерального закона «О связи» и Федерального закона «Об информации, информационных технологиях и о защите информации», что позволило: а) законодательно обеспечить организацию устойчивой работы интернета в России, ввести

[1] Федеральный закон «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» от 01 мая 2019 г. № 90-ФЗ // Российская газета. – 07.05.2019 г. – № 97.

положение о технической устойчивости функционирования интернета в границах Российской Федерации; б) установить требование к операторам по передаче сигнала через технические средства противодействия угрозам (DPI), тем самым блокировать нежелательные или вредоносные ресурсы; в) создать системы централизованного управления и мониторинга работоспособности сегментов российского интернета посредством формирования системы центрального оперативного центра (ФГУП РЧЦ), осуществляющего управление техническими средствами, контролирующими российский сегмент интернета; г) уточнить порядок ограничения доступа к противоправному контенту за счёт интегрирования новых механизмов идентификации и блокировки ресурсов по инициативе уполномоченных органов государственной власти; д) установить новый принцип определения юрисдикции, согласно которому деятельность любой организации в российском сегменте должна соответствовать требованиям российского законодательства вне зависимости от места регистрации юридического лица; е) обеспечить устойчивость функционирования интернета посредством организации национальной системы доменных имен (DNS), в случае невозможности использования корневых, за счёт установления правил маршрутизации трафика в российском сегменте интернета при нарушении нормальной работы глобальных DNS-серверов.

Несмотря на то, что в законе не использован термин «киберсуверенитет», все прописанные запреты и ограничения свидетельствуют о создании правовой основы для государственного контроля интернет-ресурсов, а в случае нарушений российского законодательства – обеспечения блокировки или отключения компаний и платформ. Подтверждением может служить замедление платформы YouTube из-за нарушения законодательства страны, установление контроля над сервисами Telegram, TikTok и Facebook (продукты компании Meta, деятельность которой признана экстремистской и запрещена в РФ) из-за их нежелания выполнять требования по фильтрации контента.

Косвенно к законодательным инструментам, обеспечивающим суверенизацию российского сегмента интернета, можно отнести Федеральный

закон №152-ФЗ «О персональных данных».[1] Это подтверждается следующим: а) в законе установлено требование хранить персональные данные граждан РФ на серверах, расположенных на территории России, что ограничивает трансграничную передачу данных и усиливает контроль государства над цифровыми ресурсами. Закон прямо обязывает операторов обеспечивать запись, систематизацию и хранение данных россиян внутри страны; б) в законе установлена возможность воздействия на иностранные компании, обрабатывающие данные россиян, если их деятельность связана с РФ, что позволяет России регулировать цифровые процессы даже за пределами своей территории; в) законодатель обязал провайдеров соблюдать российские стандарты безопасности, согласовывать с Роскомнадзором трансграничную передачу данных, с этой целью предусмотрено заключение международных договоров; г) создана национальная система регулирования, позволяющая Роскомнадзору контролировать обработку данных; с этой целью введено лицензирование операторов, установлена обязанность операторов уведомлять регулятора о нарушениях; д) в законе ограничено влияние иностранных IT-гигантов на российское цифровое пространство, установлено требование локализации зависимости от зарубежных серверов.

Среди документов, затрагивающих вопросы киберсуверенитета в российском правовом поле, можно выделить «Доктрину информационной безопасности Российской Федерации»,[2] поскольку в ней сформулированы положения, обеспечивающие национальные интересы в информационной сфере, в частности: а) защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, информационная поддержка демократических институтов, механизмов взаимодействия государства

[1] Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.).

[2] Указ Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» от 05.12.2016 г. № 646 // Собрание законодательства Российской Федерации. – 2016. – № 50.

и гражданского общества; б) обеспечение устойчивого и бесперебойного функционирования цифровой инфраструктуры, в первую очередь – критической инфраструктуры Российской Федерации; в) развитие информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности; г) содействие формированию системы международной информационной безопасности, направленной на защиту суверенитета Российской Федерации в информационном пространстве.

В целом, Доктрина направлена на формирование безопасной среды оборота достоверной информации, устойчивой к различным видам воздействия информационной инфраструктуры для обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

Следующий документ, отражающий стремление российского государства к обеспечению национального суверенитета в интернет- пространстве, – «Стратегия развития информационного общества в РФ».[1] Он определяет меры по развитию отечественной информационной инфраструктуры, включая широкополосный доступ в интернет-пространство. В Стратегии сделан акцент на вопросах развития информационного общества, формирования национальной цифровой экономики, обеспечения национальных интересов и реализации стратегических национальных приоритетов.

В документе установлено обязательное использование российских криптоалгоритмов и средств шифрования при взаимодействии органов власти между собой, а также с гражданами и организациями. Для предоставления безопасных услуг и программного обеспечения в отечественных информационных

[1] Указ Президента РФ «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» от 09.05.2017 г. № 203. // Собрание законодательства РФ, 15.05.2017 г. – № 20. – ст. 2901.

и коммуникационных технологиях предложено использовать встроенные средства защиты информации. Отдельным пунктом прописано осуществление противодействия использованию интернета в военных целях, определялся вектор на правовое регулирование деятельности соцсетей, мессенджеров, интернет-телевидения и СМИ.

Проведенный анализ позволяет констатировать формирование в Российской Федерации правовой модели, направленной на законодательное закрепление суверенитета в национальном сегменте интернета. Несмотря на отсутствие в нормативно-правовых актах прямого термина «киберсуверенитет», имплементация таких мер, как создание инфраструктуры для автономного функционирования интернета, установленных в Федеральном законе от 1 мая 2019 г. № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации», и требования локализации персональных данных, изложенные в Федеральном законе от 28.02.2025 г. № 23-ФЗ «О внесении изменений в Федеральный закон «О персональных данных» и отдельные законодательные акты Российской Федерации», свидетельствуют о целенаправленной политике по усилению государственного контроля над цифровым пространством. Сформированная модель предполагает доминирующую роль государства в управлении критической информационной инфраструктурой и обороте данных, где законодательство используется как инструмент обеспечения национальной безопасности, что предполагает ее приоритет над либеральной моделью свободы информации.

В сравнительной перспективе модель киберсуверенитета, реализуемая Китайской Народной Республикой, демонстрирует концептуальные отличия, уходящие корнями в доктрину «информационного суверенитета». Как отмечает А. Д. Янькова, концепция «сетевого суверенитета» была официально легитимирована в «Белой книге» Государственного совета КНР (2010 г.), где интернет определяется как элемент национальной инфраструктуры, подпадающий

под суверенную юрисдикцию государства.[1] Дальнейшее развитие данная концепция получила в выступлении Си Цзиньпина на Всемирной интернет-конференции (2014 г.), где киберпространство было обозначено в качестве пятой сферы государственного суверенитета наряду с традиционными (суша, море, воздушное и космическое пространство). Китайский подход экстернализируется через инициативу «Цифровой шелковый путь», которая, наряду с экономическими целями, служит платформой для продвижения модели суверенного интернета, основанной на принципе невмешательства во внутренние цифровые юрисдикции. Эта позиция, конкурирующая с мультистейкхолдерной моделью, находит поддержку среди ряда развивающихся государств.

В противоположность подходам России и Китая, позиция Соединенных Штатов Америки базируется на принципах открытости и глобализма интернета. В основе американской модели лежит концепция его как глобального ресурса, минимально ограниченного национальными границами, что соответствует экономическим и стратегическим интересам доминирующих американских технологических корпораций. Однако декларируемый принцип невмешательства государства сочетается с инструментами экстерриториального правоприменения.

Возможность интеграции США в цифровые отношения любого государства установлена на законодательном уровне актами «Clarifying Lawful Overseas Use of Data Act»[2] (Разъяснение законного использования данных за рубежом), ставшего поправкой к закону «Stored Communications Act» (SCA)[3] (Закон о сохранённых сообщениях) 1986 года, регулирующему предоставление доступа правительства США к данным, находящимся в распоряжении интернет-провайдера

---

[1] Янькова А. Д. Архитектура концепции кибер-суверенитета КНР (по материалам докладов Всемирной интернет-конференции «Кибер-суверенитет: теория и практика») // Проблемы Дальнего Востока. – 2023. – №4. – С. 99-100.

[2] The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943). – URL: https://thesedonaconference.org/sites/default/files/%5B5.2%5D%20CLOUD%20Act.pdf (дата обращения: 02.12.2024).

[3] The Stored Communications Act of 1986. – URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (дата обращения: 02.12.2024).

Поправка к закону «Stored Communications Act» 1986 года, названная «CLOUD Act», сделанная в 2018 году, предоставила американским правоохранительным органам широкие полномочия по доступу к данным, хранящимся на серверах иностранных компаний, подконтрольных юрисдикции США. Это создает правовой парадокс, при котором США де-факто осуществляют суверенный контроль над трансграничными цифровыми потоками, одновременно оспаривая аналогичные права других государств, что приводит к обострению юрисдикционных конфликтов.

Можно предположить, что суверенный интернет для американских IT-компаний не приемлем, так как подрывает их могущество и глобальную систему управления. Осуществление контроля США над компонентами программного обеспечения, усиление шифрования и борьба с технологическими конкурентами политическими методами – это методика противодействия суверенизации интернета.

Всякая попытка создания национальной формы организации киберпространства встречает противодействие со стороны США и сателлитов; примером, подтверждающим данное суждение, может служить Великобритания, позиция которой базируется на свободном и открытом интернете.

Англия движется в траектории США, отрицает право государств на суверенизацию интернета, рассматривая её как угрозу глобальной цифровой экономике и правам человека. Английская позиция закреплена в «Будапештской конвенции о киберпреступности» 2001 года,[1] соглашениях G7, в рамках которых продвигается модель «открытого интернета»,[2] где регулирование основано на общих стандартах, а не национальных барьерах и национальных законах. Так,

[1] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). – URL: https://base.garant.ru/4089723/ (дата обращения: 21.12.2024).
[2] G7 Digital and Technology Ministers' meeting (2021, London). Ministerial Declaration G7 Digital and Technology Ministers' meeting, 28 April 2021. – URL: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/G7_Digital_and_Technology_Ministerial_Declaration.pdf (дата обращения: 21.12.2024).

закон «Online Safety Bill»,[1] принятый в 2023 году, фокусирует внимание на безопасности контента, но не предусматривает изоляцию инфраструктуры или данных, в отличие от российского закона о «суверенном Рунете» или китайского подхода.

Концепт, пропагандируемой англичанами на официальном уровне, строится на позиции открытости «цифровых границ» и принципе многостороннего регулирования, основанного на сотрудничестве и общих стандартах. Это соответствует её экономическим интересам, так как британские компании, финансовые институты и IT-корпорации зависят от свободного трансграничного потока данных. Лондон, как глобальный финансовый центр, строит свою деятельность на свободном интернете, на основании этого финансовые институты получают 40% британского ВВП, состоящего из услуг банкинга, страхования и IT сектора, требующих беспрепятственного обмена информацией. Ограничения, аналогичные ФЗ-152 РФ «О персональных данных», нарушили бы логистику транзакций. В подтверждение можно констатировать, что IT-корпорации, например, Кембриджский кластер обслуживает клиентов из ЕС и США. Локализация данных повысила бы затраты на 15–20%, подорвав конкурентоспособность.

Британская модель регулирования служит интересам глобалистов, например, участие в разведывательном англосаксонском союзе «Five Eyes» обеспечивает доступ к данным без суверенных ограничений,[2] а экстерриториальность законов, таких как CLOUD Act[3] (США), позволяет британским спецслужбам запрашивать данные у американских компаний Google, Meta, минуя национальные юрисдикции третьих стран, что позволяет устранять технологических соперников, как это было

[1] The Online Safety Bill. – URL: https://assets.publishing.service.gov.uk/media/6231dc9be90e070ed8233a60/Online_Safety_Bill_impact_assessment.pdf (дата обращения: 21.12.2024).
[2] Henningsen, P. The Five Eyes: The International Syndicate That Spies on the Entire World / P. Henningsen // New Dawn Magazine. – URL: https://www.newdawnmagazine.com/articles/behind-the-news/the-five-eyes-the-international-syndicate-that-spies-on-the-entire-world (дата обращения 26.12.2024).
[3] Cloud Act // Link11. – URL: https://www.link11.com/en/glossar/cloud-act/ (дата обращения: 26.12.2024).

с компанией Huawei в 2020 году. Для Великобритании, как и США, отрицание цифрового суверенитета – стратегия сохранения влияния и продвижение интересов глобалистов.

Третья группа государств, придерживающихся компромиссной позиции по вопросу суверенизации киберпространства, в основном, делает упор на сочетание элементов контроля над цифровым пространством с участием в международном сотрудничестве, избегая крайних моделей полной открытости доступа или изоляции. Для этого используются различные подходы, начиная от гибридного регулирования, основанного на локализации данных в интересах защиты критических секторов и применения международных стандартов для бизнеса, заканчивая селективным контролем, в результате чего блокируется зарубежный контент, несущий вред идеологии, культуре и суверенитету государства без тотальной изоляции интернета.

Чётко установить «компромиссную» позицию по вопросу суверенизации киберпространства достаточно сложно, так как сам термин является предметом дискуссий, и большинство государств так или иначе ищут баланс между различными интересами. Однако можно выделить группу стран, которые стремятся сочетать защиту национальных интересов в киберпространстве с сохранением его глобального характера и принципов международного сотрудничества. Такая позиция обычно не подразумевает ни полного отказа от государственного регулирования, ни стремления к тотальному контролю и изоляции национального сегмента интернета.

Основные черты компромиссной позиции проявляются в: а) признании важности глобального интернета; б) отсутствии стремления к созданию изолированных национальных сетей; в) акценте на международном сотрудничестве; г) локальном регулировании, а не тотальном контроле; д) балансе между безопасностью, экономическим развитием и правами человека; е) широком использовании правовых механизмов регулирования отношений, а не технической изоляции интернета.

Компромиссная позиция, по нашему мнению, таит в себе проблемы, а именно: а) конфликт юрисдикций, например, экстерриториальные законы, такие как CLOUD Act, GDPR и иные, усложняют соблюдение внутреннего законодательства стран; б) давление держав, придерживающихся полярных позиций, например, Китая, несущего идею суверенизации интернета, и США, стоящего на позиции открытости киберпространства, что вынуждает многие государства лавировать. Как правило компромиссная позиция свойственна странам, стремящимся сохранить цифровой суверенитет без разрыва с глобальной экономикой.

На основании анализа внутреннего законодательства, регламентирующего отношения в киберпространстве, к государствам, придерживающимся компромиссной позиции, можно отнести множество стран, среди которых выделяются Бразилия, Индия, Южная Корея и иные.

На примере законодательных актов некоторых из них можно раскрыть специфику компромиссной позиции. Так, в Бразилии компромиссный подход выражается в содержании нескольких законов. Первый – «Закон о гражданских правах в интернете» «Marco Civil da Internet», Lei Nº 12.965/2014,[1]его называют «Конституцией интернета» Бразилии. Закон устанавливает права и обязанности, связанные с использованием интернета в стране. В нём регламентированы права пользователей, гарантировано право на свободу выражения мнений, защиту частной жизни и персональных данных, а также сетевой нейтралитет, что соответствует принципам открытого интернета.

Одновременно закон предусматривает возможность государственного вмешательства с целью защиты прав граждан, противостояния преступности и обеспечения национальной безопасности. В законе установлены правила для интернет-провайдеров по хранению логов соединений и их предоставлению по решению суда, определена ответственность для интернет-посредников за контент,

[1] Marco Civil da Internet, Lei Nº12.965/2014 // Câmara dos Deputados. – URL: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1238705&filename=Tramitacao-PL+2126/2011 (дата обращения: 26.12.2024).

размещенный пользователями, а также условия, при которых возможно его удаление.

Второй закон – «Общий закон о защите данных» Lei Geral de Proteção de Dados (LGPD), Lei Nº 13.709/2018.[1] Это аналог европейского GDPR, устанавливающий комплексные правила сбора, обработки, хранения и передачи персональных данных. Основная цель законодателя – обеспечить конфиденциальность информации, касающейся граждан, и контроль над своими персональными данными, что является важным элементом цифрового суверенитета.

Закон регулирует трансграничную передачу данных, устанавливает условия, при которых это возможно, учитывая защиту национальных интересов. При этом законодательно признаётся необходимость международного обмена данными, касающимися экономики страны. Закон предусматривает создание Национального органа по защите данных (ANPD) для контроля за соблюдением его положений.

В уголовном законодательстве Бразилии установлена ответственность за различные киберпреступления, угрожающие национальным интересам страны и граждан. Таким образом, законодательство Бразилии демонстрирует стремление интегрировать страну в глобальное цифровое пространство, одновременно обеспечивая инструменты для защиты своих граждан, экономики и национальных интересов, что и характеризует компромиссную позицию по вопросу киберсуверенитета.

В индийском подходе к суверенизации киберпространства также просматривается компромисс. Можно выделить несколько законодательных актов, подтверждающих данное суждение.

[1] General Personal Data Protection Act (LGPD) Lei Nº 13.709/2018 // https://www.gov.br/pt-br – URL: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf (дата обращения: 26.12.2024).

Первый «Закон об информационных технологиях 2000 года» (IT Act) «Information Technology Act, 2000 (IT Act)»[1] — это базовый закон, регулирующий отношения в киберпространстве Индии, в частности, вопросы киберпреступности, электронной коммерции, защиты данных и деятельности интернет-посредников. В нём установлены механизмы борьбы с киберпреступлениями, расписаны полномочия компетентных органов по блокировке доступа к определенным веб-сайтам или контенту, который считается угрозой национальной безопасности, общественному порядку или морали под лозунгом защиты национальных интересов в киберпространстве. Закон легализует электронные подписи и контракты, способствуя развитию цифровой экономики и интеграции в глобальные процессы. По существу, законодатель избрал технологию регулирования, а не тотального контроля и не предусматривает создание полностью закрытого национального сегмента интернета.

Вторым по значению можно считать «Правила в области информационных технологий (Руководящие принципы для посредников и Кодекс этики цифровых СМИ), 2021 год».[2] Данные правила формулируют обязательства для интернет-посредников. Главное, что следует из документа, – это повышение ответственности платформ за размещаемый пользователями контент, включая его удаление, идентификацию авторов вредоносного контента, сотрудничество с правоохранительными органами, что, естественно, усиливает контроль со стороны государства. Декларируются также свобода слова и саморегулирование, есть положения о необходимости уважения свободы слова, и поощряется саморегулирование со стороны индустрии. На практике баланс смещён в сторону государственного контроля.

---

[1] Information Technology Act, 2000. // India Code. - URL: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (дата обращения: 26.12.2024).

[2] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. / Ministry of Electronics & Information Technology, Government of India. – URL: https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (дата обращения: 23.12.2024).

Ещё один документ, транслирующий намерения правительства Индии в области киберпространства, называется «Национальная политика в области кибербезопасности» «National Cybersecurity Policy, 2013»,[1] он определяет стратегические направления развития кибербезопасности в Индии. В нём изложена государственная позиция, основанная на защите критической инфраструктуры от кибератак. Декларируется важность развития собственных кибернетических возможностей и подготовки кадров. Признается необходимость международного сотрудничества в борьбе с киберугрозами, что указывает на понимание глобального характера киберпространства.

В 2023 году был принят «Закон о защите цифровых персональных данных» «Digital Personal Data Protection Act, 2023»,[2] который установил правила сбора, обработки и хранения персональных данных. Законодатель сконцентрировал внимание на защите прав граждан и конфиденциальность в части контроля над своими персональными данными. В данном акте регламентируется трансграничная передача данных, установлены условия и ограничения, что позволяет государству контролировать процесс. Помимо этого был создан Совет по защите данных для надзора за соблюдением закона.

Позиция Индии по вопросу суверенизации интернета сводится к обеспечению национальной безопасности, контролю над интернет-посредниками, защите персональных данных и сдержанности по отношению к полной изоляции страны в рамках киберсуверенитета, что демонстрирует признание глобальной цифровой экономики и международного сотрудничества.

Аналогичную гибридную модель регулирования отношений в интернете, сочетающую технологический суверенитет с интеграцией в глобальное цифровое пространство, реализует Южная Корея. Её законодательство находится между

---

[1] India. Ministry of Communications and Information Technology. National Cybersecurity Policy. / Ministry of Communications and Information Technology, Government of India. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/India_2013_National_cyber_security_policy-2013(1).pdf (дата обращения: 23.12.2024).

[2] Digital Personal Data Protection Act, 2023. // https://www.meity.gov.in/ – URL: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (дата обращения 23.12.2024).

защитой национальных интересов, обеспечением кибербезопасности и поддержанием глобального интернета, что подтверждается несколькими законами.

Сущность «Закона о сетевой нейтральности» (Network Neutrality Act, 2011)[1] раскрывается в концепте принципа сетевого нейтралитета, декларирующего подачу контента и цифровых услуг в интернете без дискриминации. Он направлен на обеспечение свободного и открытого интернета, где пользователи могут получать доступ к данным без ограничений, если контент не нарушает никаких законов.

Ещё один акт – «Закон о защите персональной информации» (Personal Information Protection Act (PIPA)[2] – дополняет и конкретизирует положения вышеупомянутого акта в части защиты персональных данных. Он устанавливает общие принципы обработки персональных данных как для государственного, так и для частного сектора. Законодатель предоставил гражданам больше прав в отношении их персональных данных, включая право на доступ, исправление и удаление информации о себе, а также обеспечил условия трансграничной передачи персональных данных, установил требования и ограничения, что подчёркивает стремление к централизованному контролю государства над персональной информацией.

Существенную роль в создании комплексной системы кибербезопасности без изоляции от международного интернета на национальном уровне Южной Кореи внёс «Закон об основах кибербезопасности» (Cybersecurity Framework Act). В работе «Новая национальная стратегия кибербезопасности республики Корея и её последствия»[3] Чон Ким констатировал, что стратегия кибербезопасности имеет три основные особенности: во-первых, она подчеркивает важность выявления

[1] Kim B., Oh B. Network Neutrality in S. Korea // https://act.jinbo.net. – URL: https://act.jinbo.net/wp/8351/ (дата обращения: 03 11.2024).
[2] Oladimeji P. South Korea data protection law (PIPA): Everything you need to know // DIDOMI – URL: https://www.didomi.io/blog/south-korea-pipa-everything-you-need-to-know (дата обращения: 03.11.2024).
[3] Kim S. J. ROK's New National Cybersecurity Strategy and Its Implications // INSS Issue Brief. – URL: https://www.inss.re.kr/upload/bbs/BBSA05/202404/F20240425131646465.pdf (дата обращения: 03.11.2024).

киберугроз и приобретения наступательных возможностей для противодействия вредоносной деятельности, включая гибридные угрозы, обеспечивая при этом бесперебойную работу критически важных ИТ-функций и повышенную устойчивость. Во-вторых, Южная Корея обязуется выполнять свои обязательства, внося свой вклад в международное сообщество в качестве глобального государства, уделяя особое внимание сотрудничеству, ответственному использованию и совместному реагированию на злонамеренных субъектов. В-третьих, в стратегии изложено внутреннее управление кибербезопасностью во главе с «Национальной комиссией по кибербезопасности» и Национальной разведывательной службой, а также конкретные институциональные усовершенствования для поддержки таких агентств.[1]

В Законе уделено особое внимание защите критической информационной инфраструктуры от кибератак, что является приоритетом для любого государства. Вместе с тем предложен концепт поддержки международных инициатив по кибербезопасности, который направлен на обмен информацией с другими странами, признавая трансграничный характер киберугроз.

В целом законодательство Южной Кореи демонстрирует сложный баланс интересов. С одной стороны, государство стремится к национальной безопасности и защите интересов граждан в цифровой среде. С другой стороны, показывает стремление сохранить открытость интернета с целью развития цифровых инноваций и сохранения позиций ключевого игрока в глобальной цифровой экономике, чего нельзя достичь без компромиссной позиции.

На наш взгляд, компромиссная позиция в области суверенизации интернета не является гарантом технологического превосходства. Подтверждением сказанного является пример Китая, который обозначил свой цифровой суверенитет, перекрыл свободный доступ к своим цифровым ресурсам сторонних

[1] Kim S. J. ROK’s New National Cybersecurity Strategy and Its Implications // INSS Issue Brief. – URL: https://www.inss.re.kr/upload/bbs/BBSA05/202404/F20240425131646465.pdf (дата обращения: 03.11.2024).

пользователей, при этом ушёл в области цифрового развития киберпространства далеко вперёд.

На основании проведенного анализа можно сформулировать следующие выводы.

Первое. Введение и теоретическое обоснование понятия «цифровой государственный киберсуверенитет» является методологически оправданным. Данная дефиниция позволяет преодолеть терминологическую нечеткость, возникающую при раздельном использовании категорий «цифровой суверенитет» (акцент на контроле над данными и технологиями) и «киберсуверенитет» (акцент на безопасности и управлении инфраструктурой), и предложить целостную концепцию, отражающую комплексный характер государственной власти в цифровой сфере.

Второе. В современном международно-правовом и политическом дискурсе сформировались три конкурирующие парадигмы регулирования отношений в киберпространстве:

а) суверенитето-центричная модель (Российская Федерация, Китайская Народная Республика), основанная на приоритете национальной юрисдикции, законодательном закреплении контроля над цифровой инфраструктурой и данными, а также ограничении трансграничного информационного влияния;

б) глобалистская (транснациональная) модель (США, Великобритания), провозглашающая принцип открытости интернета и свободного потока данных, который, однако, сочетается с экстерриториальным применением национального законодательства (на примере CLOUD Act), что де-факто утверждает доминирование этих государств в цифровой среде;

в) компромиссная (гибридная) модель, характерная для ряда государств с развитой и развивающейся цифровой экономикой (например, страны ЕС, Бразилия, Индия). Она стремится к балансу между обеспечением национальной безопасности и защитой прав граждан через избирательный контроль над критически важными сегментами цифровой инфраструктуры при сохранении интеграции в глобальное интернет-пространство.

Анализ представленных моделей позволяет утверждать, что отрицание цифрового суверенитета со стороны сторонников глобалистского подхода может интерпретироваться не как отказ от регулирования, а как стратегия сохранения геополитического и технологического доминирования. В этом контексте риторика «открытого интернета» зачастую маскирует практику одностороннего экстерриториального применения права. Таким образом, национальный киберсуверенитет представляет собой не изоляционистскую доктрину, а необходимый гибридный правовой институт, позволяющий государству в рамках международного права обеспечивать безопасность, защищать суверенные права и сохранять идентичность в условиях цифровой трансформации.

По мнению руководителя Роскомнадзора стран, обладающих полноценным цифровым суверенитетом, в мире единицы. Считается, что российский цифровой суверенитет поддерживают не только государственные институты, бизнес, но и сами пользователи.[1]

Логическим продолжением анализа проблемы демаркации границ правового регулирования в киберпространстве является исследование вопроса о государственной юрисдикции. Следует отметить, что данная проблематика получила широкое освещение в отечественной и зарубежной научной литературе, что подтверждается обширным библиографическим списком.[2] Несмотря на

---

[1] Карсаков Н. В России заявили о необходимости поддержки цифрового суверенитета страны // Газета.ru – URL: https://www.gazeta.ru/social/news/2025/09/19/26765426.shtml?utm_auth=false (дата обращения: 26.09.2025).

[2] Волков А. С. Проблемы установления юрисдикции в виртуальном пространстве: российский и международный опыт // Вестник Московского университета МВД России. – 2021. – № 1. – С. 35–41.; Панов И. В. Особенности судебного рассмотрения дел, возникших в результате нарушения прав субъектов в киберпространстве // Государственная власть и местное самоуправление. – 2020. – № 10. – С. 31–36; Федотов Н. А. Правовые аспекты осуществления правосудия в условиях развития информационно-телекоммуникационных технологий // Российская юстиция. – 2021. – № 1. – С. 14–18; Гусаков Д. М. Компьютерные преступления и уголовно-процессуальные особенности юрисдикции в информационной среде // Российский следователь. – 2020. – № 11. – С. 16–20; Давыдова Л. И. Территориально-государственное регулирование правонарушений в киберпространстве // Правоведение. – 2021. – № 3. – С. 54–61; Евсеенко Т. Н. Защита прав интеллектуальной собственности в российском сегменте сети Интернет: вопросы юрисдикции // Интеллектуальная собственность. Авторское право и смежные права. – 2020. – № 12. – С. 18–23; Кулешова Е. Г. Государственно-территориальная принадлежность преступлений в глобальной сети: современные тенденции юрисдикции // Современное право. – 2021. – № 5. – С. 25–30; Калугин А. П. Коллизии компетенций юрисдикций при разрешении споров в интернете //

значительное количество публикаций, консенсус по ключевым аспектам проблемы до сих пор не достигнут, а существующее многообразие доктринальных подходов лишь усугубляет имеющиеся теоретические противоречия.

Центральной проблемой правового регулирования цифровой среды является экстраполяция традиционных, территориально-ориентированных правил юрисдикции на киберпространство. Как справедливо отмечает С. М. Сафоева, вопрос о возможности и пределах распространения государственной юрисдикции на данную сферу является предметом острой научной дискуссии.[1]

В контексте обозначенного дискуссионного подхода можно привести суждения английских исследователей Н. Цагориаса и Р. Бачена,[2] которые пришли к заключению об отсутствии неразрывной связи между территорией, с одной стороны, и суверенитетом и юрисдикцией – с другой. По их мнению, сущностью суверенитета является власть, а не территория, которая выполняет лишь функцию «вместилища» власти.[3] Данная позиция находит подтверждение и в судебной практике, в частности, в решении по делу American Civil Liberties Union v. Reno, где американский суд постановил, что глобальная сеть Интернет не может быть ограничена какой-либо определенной юрисдикцией.

Исследователь виртуального пространства Л. В. Терентьева констатировала, что государство вправе самостоятельно устанавливать юрисдикцию в интернете,

---

Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. – 2020. – № 1. – С. 135–142; Корнеев С. Д. Гражданские правоотношения в киберпространстве: проблемы выбора компетентной юрисдикции // Адвокат. – 2021. – № 10. – С. 12–16; Семенов А. Ю. Развитие международного законодательства о юрисдикции в киберпространстве // Вопросы экономики и права. – 2020. – № 3. – С. 51–57; Чердаков О. И., Куликов С. Б. Теоретико-правовая интерпретация юрисдикции в киберпространстве в зарубежных исследованиях // История государства и права. – 2024. – № 3. – С.54–69.

[1] Сафоева С. М. Границы юрисдикции в киберпространстве: трансформация гражданско-правовых отношений // Universum: экономика и юриспруденция: электрон. научн. журн. – 2023. – № 8 (107). – URL: https://7universum.com/ru/economy/archive/item/15821 (дата обращения: 08.09.2023).

[2] Кравчук Н. В., Цагориас Н. Правовой статус киберпространства // Государство и право в новой информационной реальности : сборник статей по материалам V Международного научно-практического форума, 20-21 апреля 2018 года. года / под ред. И. Д. Хубиева. – М.: РГГУ, 2018. – С. 115.

[3] Research Handbook on International Law and Cyberspace / edited by N. Tsagourias, R. Buchan. – Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing, 2015. – P. 18.

так как его право на осуществление юрисдикции опирается на его суверенитет. При этом уточнила, что возможности определения виртуальной юрисдикции прямо зависят от технологической оснащенности соответствующих структур.[1]

Второй подход, напротив, базируется на принципах международного права. В частности, на положении, закрепленном в «Декларации прав и обязанностей государств» 1949 года[2] и национальных конституциях, согласно которому государство осуществляет юрисдикцию над своей территорией, а также над всеми лицами и вещами в ее пределах. В докладе Группы правительственных экспертов ООН было подтверждено, что принципы суверенитета и юрисдикция государства распространяются на соответствующую информационно-коммуникационную инфраструктуру, физически расположенную на его территории.

Развивая данный тезис, следует констатировать, что юрисдикция государства распространяется на технические средства (дата-центры, точки обмена трафиком), деятельность операторов связи, а также на действия граждан и иностранных лиц, взаимодействующих с национальной цифровой инфраструктурой. Сфера государственного регулирования также охватывает информацию, которая производится, хранится и распространяется подконтрольными субъектами.

Для конкретизации механизмов юрисдикции целесообразно обратиться к классификации, представленной в Протоколе Беркли, где выделяются следующие виды юрисдикции: территориальная, временная, персональная, предметная и универсальная. Данная типология демонстрирует наличие теоретического инструментария для установления юрисдикции, однако его практическая имплементация в цифровой среде остается дискуссионной.

Существует суждение о возможности придания киберпространству статуса четвертого «международного пространства» (по аналогии с Антарктидой и

---

[1] Терентьева Л. В. Принципы установления территориальной юрисдикции государства в киберпространстве. – URL: https://yushchuk.livejournal.com/1593956.html (дата обращения: 12.07.2023).

[2] Декларация прав и обязанностей государств от 6 декабря 1949 г. (принята Комиссией международного права ООН, резолюция 375 (IV) от 6 декабря 1949 г.) [Статья 2]. – URL: https://base.garant.ru/2561237/741609f9002bd54a24e5c49cb5af953b/ (дата обращения: 12.07.2023).

космосом), утверждается, что без такого подхода невозможно применение традиционных коллизионных норм.[1] В то же время профессиональное юридическое сообщество прагматично признает распространение юрисдикции на цифровое пространство. В отчете Американской ассоциации юристов (ABA) указывается, что компания, размещающая веб-сайт, подпадает под действие иностранных законов и юрисдикции тех стран, на которые направлена ее деятельность.

Ключевым остается вопрос о территориальности юрисдикции, которая в доктрине подразделяется на субъективную (деяние совершено на территории государства) и объективную (последствия деяния наступили на территории государства). Примером законодательного закрепления объективной экстерриториальной юрисдикции является Закон Индии «Об информационных технологиях» 2000 г.

Вместе с тем в современной науке утверждается, что одним из эффектов цифровизации является эрозия принципа территориальности, поскольку физическое местоположение данных может быть случайным. Это ведет к снижению роли универсальных норм международного права и повышению значения двусторонних договоров о взаимном признании экстерриториальных норм.

Анализ международно-правовых инструментов, таких как Брюссельская и Римская конвенции, показывает их недостаточную эффективность для всеобъемлющего регулирования киберпространства, хотя они и позволяют устанавливать юрисдикционные рамки в отдельных сферах (например, в электронной коммерции). Ввиду этого, в качестве прагматичного решения предлагается акцентировать внимание на заключении двусторонних межгосударственных договоров и включении в частноправовые контракты юрисдикционных оговорок.

---

[1] Мажорина М. В. Киберпространство и методология международного частного права // Право. Журнал Высшей школы экономики. – 2020. – № 2. – С. 230–253.

Однако такой подход может создать проблему коллизии юрисдикций, когда более одного государства претендует на рассмотрение дела с экстерриториальным элементом. В условиях глобальной сети практически любая деятельность имеет международный аспект, что может приводить к множественности юрисдикций или так называемому «эффекту перелива» (spillover effect). Ситуация усугубляется различиями в национальных законодательствах, определяющих правомерность того или иного контента.

Исследование доктрины и практики демонстрирует отсутствие консенсуса в международном сообществе по вопросу установления юрисдикции в киберпространстве. Попытки механической адаптации существующих международно-правовых норм не привели к формированию унифицированного подхода. В качестве наиболее перспективных направлений рассматриваются заключение двусторонних и многосторонних соглашений, а также активное использование договорных механизмов в частноправовых отношениях для минимизации правовой неопределенности.

Подводя итог, отметим, что проблема демаркации границ правового регулирования и установления юрисдикции является фундаментальной и многоаспектной в современной юриспруденции, порожденной несоответствием трансграничной, атерриториальной природы киберпространства и территориальным характером государственного суверенитета и права. В научном сообществе и государственной практике сложилось три основных подхода: сторонники полной суверенизации (Россия, Китай); приверженцы идеи глобального, безграничного интернета под эгидой либеральных ценностей (США, Великобритания); страны, придерживающиеся компромиссной модели регулирования отдельных аспектов без полной изоляции (Бразилия, Индия, Южная Корея).

Отсутствие единого подхода к толкованию понятий «цифровой суверенитет» и «суверенитет в киберпространстве» ведет к правовой неопределенности. В связи с этим предлагается комплексная дефиниция «цифровой государственный киберсуверенитет», которая объединяет как технический контроль над

инфраструктурой, так и социально-правовое регулирование отношений в цифровой среде. Решение проблемы юрисдикции видится в гибридном подходе, сочетающем адаптацию существующих международно-правовых принципов, заключение двусторонних и многосторонних соглашений, а также применение договорных условий о подсудности в частноправовых отношениях, что позволит обеспечить баланс между национальными интересами, глобальным характером интернета и защитой прав его участников.

Глава 2 МЕХАНИЗМ ПРАВОВОГО РЕГУЛИРОВАНИЯ В СИСТЕМЕ ПОЛИНОРМАТИВНОГО РЕГУЛИРОВАНИЯ ОТНОШЕНИЙ В КИБЕРПРОСТРАНСТВЕ

2.1. Понятие и элементы механизма правового регулирования отношений в киберпространстве

Развитие правового регулирования отношений в киберпространстве прошло сложный путь, отражая эволюцию самого цифрового мира. На начальных этапах законодатели пытались адаптировать существующие правовые нормы к реалиям цифрового пространства, однако его специфика потребовала разработки новых подходов. В этой связи возникла необходимость создания механизма, учитывающего трансграничный характер цифровой среды, технологическую нейтральность норм и баланс между регулированием и инновациями, что привело к появлению многоуровневой системы, сочетающей правовые нормы и неюридические регуляторы с технологическими решениями. Сложилась полинормативная модель, в которой правовое регулирование – лишь один из элементов в общей архитектуре регламентации отношений в киберпространстве, где право устанавливает общие рамки, а этические кодексы, технические стандарты и иные неправовые регуляторы определяют конкретные механизмы реализации.

Необходимо констатировать, что в отечественной теории права дефиниция «механизм правового регулирования отношений» толкуется неоднозначно. Например, А. В. Малько считает, что механизм правового регулирования – это система правовых средств, организованных наиболее последовательным образом в целях преодоления препятствий, стоящих на пути удовлетворения интересов субъектов права.[1]

[1] Матузов Н. И., Малько А. В. Теория государства и права: учебник – 5-ое изд. – М.: Дело, 2022. – 528 с.

Аналогичной точки зрения придерживался Н. М. Кропачёв, полагавший, что механизм уголовно-правового регулирования представляет систему последовательно связанных элементов, состоящую из предмета правового регулирования, юридической нормы, юридических фактов, регулятивного или охранительного уголовно-правового отношения и уголовной ответственности.[1]

Более короткое определение предложил Р. К. Русинов**:** он назвал механизм правового регулирования системой юридических средств, при помощи которых осуществляется правовое регулирование.[2]

С. С. Алексеев определял механизм правового регулирования как взятую в единстве совокупность юридических средств, при помощи которых обеспечивается правовое воздействие на общественные отношения.[3]

В зарубежной научной литературе также существуют работы, в которых представлено толкование понятия «механизм правового регулирования отношений». Орла Линski на базе анализа законодательства Европейского Союза (ЕС) о защите данных, в частности GDPR (Общего регламента по защите данных), показала механизм правового регулирования отношений как систему GDPR, которую представила выразителем фундаментальных ценностей ЕС.[4]

Берт-Яап Коопс предложил рассматривать механизм правового регулирования отношений через взаимодействие права и технологий.[5]

В нашем понимании механизм правового регулирования отношений в киберпространстве консолидирует правовые средства, методы и процедуры.

---

[1] Кропачев Н. М. Уголовно-правовое регулирование: Механизм и система. – СПб.: Санкт-Петербургский государственный университет, 1999. – 262 с.

[2] Теория государства и права / под ред. В. М. Корельского, В. Д. Перевалов. – М.: Норма : ИНФРА-М, 1998. – С. 269-271.

[3] Алексеев С.С. Механизм правового регулирования в социалистическом государстве. – М.: Юридическая литература, 1966. – С. 30.

[4] Lynskey O. The foundations of EU data protection law. – Oxford, United Kingdom; New York, NY, USA : Oxford University Press. – 2015. – 269 p. // books.google.ru. – URL: https://books.google.ru/books/about/The_Foundations_of_EU_Data_Protection_La.html?id=jCXYCgAAQBAJ&redir_esc=y (дата обращения: 02.04.2024).

[5] Koops, B.-J. Law, technology, and society: reimagining the human-machine relationship // Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press. – 2024. – 300 p. // https://papers.ssrn.com – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1479819 (дата обращения: 02.04.2024).

Правовые средства в механизме правового регулирования отношений в киберпространстве выполняют регулятивную задачу, они включают: нормы права; юридические факты; правовые принципы; правовые институты; правовые отношения. Общепринятой точки зрения на роль правовых средств в процессе регулирования отношений в киберпространстве в отечественном праве пока не существует. Также можно констатировать наличие множества подходов, позволяющих определить степень использования правовых средств в регулировании отношений в киберпространстве. Предлагаем их систематизировать и классифицировать следующим образом:

а) по степени вмешательства государства:

- минимальное вмешательство (саморегуляция) – предполагается, что государство должно минимально вмешиваться в регулирование отношений в киберпространстве, оставляя большую свободу действий интернет-сообществу и рыночным механизмам, акцент делается на саморегуляцию и разработку этических кодексов поведения;
- умеренное вмешательство – устанавливается баланс между свободой в киберпространстве и необходимостью защиты прав и интересов пользователей, государство разрабатывает правовые нормы для регулирования ключевых аспектов киберотношений, но не стремится к полному контролю;
- максимальное вмешательство (жесткое регулирование) – предусматривает активное вмешательство государства в регулирование киберпространства с целью обеспечения безопасности, правопорядка и защиты национальных интересов, характеризуется жесткими законами и контролем над онлайн-активностью;

б) по уровню регулирования:

- национальное регулирование – предполагается, что каждая страна разрабатывает свое законодательство для регулирования киберпространства в пределах своей юрисдикции;

- региональное регулирование – основывается на желании группы государств (например, Европейского Союза) регламентировать киберотношения посредством создания единых норм и стандартов в рамках региона;
- международное регулирование – определяет разработку международных договоров и соглашений для регулирования глобальных аспектов кибер-отношений;

в) по объекту регулирования:

- регулирование контента – нормы, направленные на борьбу с незаконным контентом в киберпространстве;
- регулирование инфраструктуры – нормы, регулирующие деятельность интернет-провайдеров, операторов связи и других участников технической инфраструктуры киберпространства;
- регулирование электронной коммерции – нормы, защищающие права потребителей в онлайн-торговле и регулирующие электронные платежи;
- регулирование кибербезопасности – нормы, направленные на предотвращение кибератак и защиту критической информационной инфраструктуры:
- регулирование защиты персональных данных – нормы, устанавливающие правила сбора, обработки и хранения персональных данных в киберпространстве;

г) по методам регулирования:

- императивные нормы – точно определяющие права и обязанности субъектов права, не подлежащие изменению по инициативе её адресатов;
- диспозитивные нормы – указывающие определённый вариант поведения, но при этом предусматривающие самостоятельность адресатов этих норм, позволяя им урегулировать отношения по собственному усмотрению;
- рекомендательные нормы – содержащие наиболее приемлемые правила поведения для общества и государства, однако их несоблюдение не влечёт ответственности;

- поощрительные нормы – стимулирующие желательное поведение с помощью льгот и преимуществ.

Можно констатировать, что правовые средства выступают универсальным регулятивным инструментом в механизме правового регулирования отношений в цифровой среде, которые в условиях технологического обновления киберпространства должны постоянно актуализироваться. Киберпространство характеризуется стремительным развитием технологий, появлением новых видов онлайн-взаимодействий и угроз, что создает объективную потребность в адаптации правовых норм к изменяющимся реалиям. Для сохранения их эффективности они должны эволюционировать вместе с технологиями.

Следующим элементом вышеназванной системы являются **методы.** В киберпространстве частично используются традиционные методы правового регулирования — императивный, диспозитивный и поощрительный, а также методы, порождённые интернетом и его пользователями.

Например, императивный метод в условиях киберпространства сложно применить из-за его трансграничного характера и анонимности пользователей, так как проблематично идентифицировать правонарушителей и привлечь их к ответственности. Фактор экстерриториальности киберпространства активирует тему применимости национального законодательства к деяниям, совершенным в киберпространстве за пределами юрисдикции государства.

В некоторых сферах отношений в киберпространстве из-за необходимости обеспечения общественной безопасности и защиты прав пользователей сложно использовать диспозитивный метод регулирования. В качестве причин можно назвать:

а) дисбаланс, возникающий из-за разности знаний и технических навыков между участниками отношений. Например, обычный пользователь может не обладать достаточными знаниями для оценки рисков, связанных с использованием определенного программного обеспечения или онлайн-сервиса, в то время как разработчик или поставщик услуги имеет полный доступ к информации о потенциальных уязвимостях. В таких случаях диспозитивный метод может

привести к злоупотреблениям со стороны более информированной стороны и ущемлению прав менее компетентных пользователей;

б) сложность в осуществлении контроля из-за технических особенностей киберпространства, связанных с применением программного кода, распределенного характера сетей, анонимности пользователей. Это затрудняет контроль за соблюдением договоренностей и ограничивает возможность применения санкций в случае нарушений. Диспозитивность в таких условиях способна снизить эффективность правового регулирования.

Можно выделить области, где диспозитивный метод неприменим, например:

- в сфере защиты критической информационной инфраструктуры, так как обеспечение её безопасности является функцией государства, которую нельзя отдать на усмотрение частных компаний;
- в области борьбы с киберпреступностью, где государство должно устанавливать нормативные запреты и вводить санкции за киберпреступления, без передачи данной функции третьим лицам;
- в сфере защиты персональных данных законодатель определяет стандарты защиты персональных данных, которые не могут быть снижены по договоренности сторон;
- в области обеспечения информационной безопасности детей, которые представляют самую уязвимую группу в киберпространстве, и государство должно принимать меры по их защите, не полагаясь на диспозитивные соглашения.

В этих отношениях необходим императивный метод правового регулирования, устанавливающий обязательные для всех участников правила поведения, обеспечивающие безопасность и защиту прав пользователей. Диспозитивный метод может быть дополнением к императивному регулированию, но не его заменой.

Что касается поощрительных методов и их применения в киберпространстве, то к таковым можно отнести: международные документы, стимулирующие правопослушное поведение в киберсреде; гранты и субсидии на развитие

кибертехнологий; налоговые льготы для IT-компаний; программы повышения цифровой грамотности и иные.

Одним из примеров использования поощрительных методов в рамках международного сотрудничества можно назвать резолюцию, принятую Генеральной Ассамблеей 22 декабря 2018 года (по докладу Первого комитета A/73/505), № 73/266 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности».[1]

Применение методов правового регулирования в киберпространстве должно учитывать его специфику и устанавливать баланс между эффективностью регулирования, защитой прав пользователей и стимулированием инноваций.

Следующий элемент механизма правового регулирования отношений в киберпространстве – **процедуры**, которые обеспечивают упорядочение, охрану и развитие отношений в киберпространстве. Их можно разделить на несколько категорий:

а) правоприменительные процедуры, посредством их осуществляется расследование киберпреступлений – они включают сбор электронных доказательств, идентификацию злоумышленников, международное сотрудничество в расследованиях, специфика данных процедур – в необходимости использования специальных технических средств и методов, а также в сложности трансграничных расследований;

б) судебное разбирательство – решение киберспоров – специфика данной процедуры – в определении юрисдикции, сложности в сборе и допустимости электронных доказательств, применении права к трансграничным спорам;

в) процедура исполнения судебных решений в киберпространстве – среди наиболее распространённых можно выделить принудительное исполнение решений суда, например, блокировку доступа к незаконному контенту, взыскание

[1] Резолюция, принятая Генеральной Ассамблеей ООН 22 декабря 2018 года (по докладу Первого комитета (A/73/505) № 73/266 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» // Организация объединенных наций. – URL: https://documents.un.org/doc/undoc/gen/n18/465/04/pdf/n1846504.pdf (дата обращения: 06.04.2024).

ущерба, причиненного киберпреступлением, специфика – в сложности реализации из-за трансграничного исполнения решений;

г) процедуры защиты прав и интересов в киберпространстве, например, обращение в уполномоченные органы по защите прав, а также внесудебное разрешение киберспоров посредством онлайн-медиации, онлайн-арбитража; в киберпространстве существуют площадки, такие как: Всемирная организация интеллектуальной собственности (The World Intellectual Property Organization (WIPO),[1] Центр Арбитража и Медиации (Arbitration and Mediation Center)[2], которые предлагают услуги арбитража и медиации для разрешения споров в области интеллектуальной собственности в киберпространстве;

д) процедуры обеспечения кибербезопасности – сюда входит оценка уязвимости информационных систем, реагирование на киберинциденты, сертификация продуктов и систем информационной безопасности;

е) процедуры регулирования цифровой экономики, позволяющие осуществлять регистрацию доменных имен, лицензирование деятельности в сфере информационных технологий, сертификацию электронных торговых площадок;

ж) процедуры управления инфраструктурой киберпространства обеспечивают распределение IP-адресов, управление доменными именами, стандартизацию протоколов и технологий;

з) процедуры, связанные с развитием киберпространства, включающие грантовые программы на поддержку научных исследований в области ИКТ; программы развития цифровой грамотности населения, международное сотрудничество в сфере развития киберпространства.

Все названные процедуры тесно взаимосвязаны и в совокупности дополняют элементы механизма правового регулирования отношений в киберпространстве. Их эффективность зависит от согласованности действий различных акторов, в

[1] All About WIPO – World Intellectual Property Organisation // iPleaders. – URL: https://blog.ipleaders.in/wipo-world-intellectual-property-organisation/ (дата обращения: 09.04.2024).
[2] WIPO Arbitration and Mediation Center // IT Law Wiki. – URL: https://itlaw.fandom.com/wiki/WIPO_Arbitration_and_Mediation_Center (дата обращения: 09.04.2024).

частности, государственных органов, частных компаний, международных организаций и самих пользователей.

Исходя из изложенного можно сформулировать дефиницию **механизм правового регулирования отношений в киберпространстве – это сложная структура, объединяющая правовые средства, методы и процедуры, направленные на упорядочение и защиту цифровых отношений, посредством которых формируется сбалансированная система, обеспечивающая законность, безопасность и инновации в цифровом пространстве.**

Подводя итог, сформулируем несколько выводов.

Первый. Механизм правового регулирования отношений в киберпространстве позволяет обеспечить баланс между свободой выражения мнений, защитой прав пользователей и интересами государства, направленными на поддержание общественной безопасности и правопорядка в киберпространстве.

Второй. Механизм правового регулирования отношений в киберпространстве, включающий правовые средства, методы и процедуры, требует апгрейда, поскольку традиционные инструменты в условиях виртуальной среды слабо эффективны.

Третий. Механизм правового регулирования отношений является центральным элементом в системе полинормативного регулирования в киберпространстве благодаря его уникальным качествам формируя каркас, внутри которого работают неправовые регуляторы (этические нормы, техническая инфраструктура, экономические механизмы и иные).

2.2 Нормы права в механизме правового регулирования отношений в киберпространстве

Теоретики права выделяют несколько элементов структуры механизма правового регулирования отношений, среди которых главное регулирующее начало отводится норме права – являющейся ядром данного механизма.[1]

[1] Матузов Н. И., Малько А. В. Теория государства и права : учебник. – М.: Дело, 2022. – С. 472.

Уточним, что киберпространство – особая виртуальная среда, в которой нет материальных объектов, при этом она трансграничная, и каждое суверенное государство обладает правом на создание общеобязательных норм права для регулирования отношений в киберпространстве, их реальная сила и сфера применения определяются юрисдикцией, которую устанавливает государство. Именно одновременное и противоречивое применение национальных норм с экстерриториальным эффектом со стороны разных государств, претендующих на регулирование одних и тех же отношений, является причиной коллизий в киберпространстве.

В этой связи существуют различные подходы в оценке значения нормы права применительно к киберпространству. Так, В.С. Черкасов в статье «Действие права в киберпространстве: основные научные подходы» констатировал, что интенсивное внедрение информационных технологий приводит к трансформации представлений о действии законодательства в пространстве. Причиной таких изменений является появление новой сферы взаимодействия субъектов правоотношений — киберпространства или виртуального пространства.[1]

Л. Г. Ефимова отмечала, что общественные отношения в киберпространстве начинают регулироваться не с помощью законов, а с помощью технических регламентов и специальных обычаев, которые сосредоточены в сети Интернет и образуют наднациональное право киберпространства.[2]

Дэвид Джонсон и Дэвид Пост в работе «Law and Borders – The Rise of Law in Cyberspace» утверждали, что в киберпространстве территориальный принцип регулирования отношений потерял свою актуальность. Нормы международного права не работают, а национальные вступают в противоречие. Они предлагали альтернативные подходы, такие как принцип «минимальных контактов» или принцип «центра тяжести», которые позволят устанавливать юрисдикцию над

[1] Черкасов В. С. Действие права в «киберпространстве»: основные научные подходы // The Newman in Foreign policy. – 2022. – Т. 2, №65(109). – – С. 7–9.
[2] Ефимова Л. Г. Источники правового регулирования общественных отношений в киберпространстве // Lex russica. – 2020. – Т. 73, № 3. –С. 114–120.

кибер-отношениями по местонахождению серверов, пользователей или места причинения вреда. [1]

М. В. Мажорина утверждала, что концепция киберправа как автономной правовой системы, регулирующей общественные отношения, складывающиеся в киберпространстве, несостоятельна, так как природа последних не трансформируется.[2]

В отечественном и зарубежном правоведении доминирует позиция о том, что в киберпространстве, как и в реальном мире, право по-прежнему выполняет функции регулирования общественных отношений, охраны прав и свобод, обеспечения порядка и безопасности.

Этой точки зрения придерживалась И. Л. Бачило, отмечая, что нормы в киберпространстве выполняют те же функции, что и нормы любой другой отрасли права: регулятивную, охранительную, воспитательную.[3]

В работе «Право и Интернет. Теоретические проблемы» И. М. Рассолов отмечал, что нормы права, действующие в киберпространстве, также исходят от государства, являются общеобязательными и обеспечиваются мерами государственного принуждения.[4]

Некоторые авторы в своих аргументах ссылались на то, что нормы права, регулирующие отношения в цифровой среде, не изменили своей структуры, включающей гипотезу, диспозицию и санкцию.[5]

Из множества материалов российских и зарубежных исследователей, подготовленных на тему регулирования отношений в киберпространстве посредством норм права, можно выделить общую позицию, основанную на

---

[1] Johnson D. R., Post D. G. Law and Borders: The Rise of Law in Cyberspace // Stanford Law Review. – 1996. – Vol. 48, № 5. – Stanford Law Review. – 1996. – URL: https://lawreview.stanford.edu (дата обращения: 12.04.2024).

[2] Мажорина М. В. Киберпространство и методология международного частного права // Журнал Высшей школы экономики. – 2020. – № 2. – С. 230–253.

[3] Бачило И. Л. О правовых основах практической информатики // Вопросы защиты информации. – 2002. – №1. – С.20–28.

[4] Рассолов И. М. Право и Интернет: теоретические проблемы. – М.: Норма, 2009. – 383 с.

[5] Савельев А. И. Проблемы применения норм гражданского права к отношениям, возникающим в сети Интернет // Вестник гражданского права. – 2014. – № 1. – С. 37–75.

утверждении, что сущность норм права в контексте киберпространства не меняется, но формы их реализации, применения и толкования претерпевают значительные трансформации, обусловленные спецификой этой среды.

Проблема связана с несколькими факторами: а) с фактором установления суверенитета и юрисдикции, обозначенным Л. Лессигом и иными исследователями;[1] б) с фактором анонимности и псевдонимности, затрудняющим идентификацию субъектов правоотношений и требующих разработки новых механизмов установления личности в онлайн-среде, отмеченным Д. Постом;[2] в) с фактором высокоскоростных изменений киберпространства, требующих от законодателя гибкости и оперативности в принятии новых норм и адаптации существующих, обозначенных Э. В. Талапиной;[3] г) фактором сложности доказывания из-за несовершенных методов, сбора и оценки доказательств, изложенных В. Б. Наумовым;[4] д) фактором создания специальных норм из-за появления новых видов правонарушений, на которые обращал внимание А. В. Трофименко.[5]

При всех разногласиях в оценке значения нормы права применительно к киберпространству несомненно то, что данный регулятор играет ключевую роль в механизме правового регулирования отношений. Благодаря нормам права устанавливаются правила взаимодействия в онлайн-среде, защищаются права и свободы пользователей, обеспечивается безопасность и создаются условия для развития цифровой экономики.

---

[1] Савельев А. И. Проблемы применения норм гражданского права к отношениям, возникающим в сети Интернет // Вестник гражданского права. – 2014. – № 1. – С. 37–75.

[2] Post D. G. Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace // Journal of Online Law. – 1995. – Art. 3. URL: https://www.academia.edu/53108483/Anarchy_State_and_the_Internet_An_Essay_on_Law_Making_in_Cyberspace_article_3_ (дата обращения: 10.12.2024).

[3] Талапина Э. В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. – 2018. – № 2. – С. 3–15.

[4] Наумов В. Б. Проблемы доказывания в «электронном правосудии» // Информационное право. – 2005. – № 1. – С. 17–21.

[5] Трофименко А. В. Особенности правового регулирования отношений в сфере оборота цифровых прав // Вестник Саратовской государственной юридической академии. – 2020. – № 2(133). – С. 93–101.

В то же время нормативно-правовое регулирование отношений сталкивается с рядом сложностей, связанных со спецификой цифровой среды, и требует постоянного совершенствования, а также тесного взаимодействия с иными альтернативными способами регулирования.

Очевидно, что актуализируется вопрос об определении иерархии законодательных норм в условиях отсутствия унифицированных международно-признанных нормативных регуляторов. Возникает проблема допустимости приоритета национальной правовой нормы одного государства над аналогичной нормой другого государства.

По указанной проблематике в научной литературе представлен ряд позиций.

1. В настоящее время не выработан эффективный механизм, позволяющий осуществлять регулирование отношений в интернет-пространстве исключительно посредством норм национального права. [1]

2. Действие закона в киберпространстве может быть ограничено в случаях наличия публичного интереса. Анализу подвергаются нормы, содержащие ограничения деятельности субъектов в цифровой среде. [2]

3. Регулирование отношений в интернет-пространстве должно осуществляться национальными правовыми нормами, распространяющими свое действие на соответствующий сегмент сети.[3]

4. При разрешении коллизионных споров с участием иностранных лиц в интернет-отношениях для определения применимого права предлагается использование традиционных коллизионных привязок, таких как «закон места нахождения», «закон места заключения сделки», «закон места причинения вреда».[4]

5. Перспектива урегулирования конфликтов в киберпространстве связывается с технологическими, а не правовыми решениями. Дигитализация права

---

[1] Ефимова Л. Г. Источники правового регулирования общественных отношений в киберпространстве // Lex russica. –2020. – Т. 73, № 3. – С. 118.
[2]Там же.
[3] Волков В. Э. Цифровое право. Общая часть: учебное пособие. – Самара : Изд-во Самарского университета, 2022. – 111 с.
[4] Рахматулина Р. Ш. Ответственность провайдера // Вестник МГПУ «Юридические науки». – 2016. – №2(22). – С. 84.

распространяется и на законотворческий процесс, где алгоритмы способны заменить человека при выполнении рутинных задач, высвобождая ресурсы юристов.[1]

6. Правовая норма в цифровой среде рассматривается как продукт саморегуляции.[2]

Все приведенные позиции являются убедительно аргументированными в научных исследованиях и не требуют дополнительного комментария. В рамках данного анализа целесообразно выделить наиболее футуристические точки зрения, среди которых – концепция, предложенная профессором Д. А. Пашенцевым.

Автор предполагал, что закон будущего – это закон, имеющий цифровую форму, что потребует создания механизмов, основанных на саморегуляции. Появятся технологии, на базе искусственного интеллекта обеспечивающие подготовку текста правовой нормы. По существу – это разработка технологии правотворчества, которая безусловно окажет воздействие на правоприменение.[3]

По мнению профессора Д. А. Пашенцева, «новая цифровая форма закона существенно изменит те представления о нем, которые существуют сегодня. Во-первых, уйдет в прошлое незыблемое правило о необходимости публикации законов, законы, которые создаются и изменяются всеми членами общества, не нуждаются в публикации. Во-вторых, закон, не имеющий текстового выражения, не нуждается в толковании и интерпретации. В-третьих, изменятся представления о юридической технике, в частности, может исчезнуть требование о ясности и внутренней непротиворечивости закона. В-четвертых, исчезнет противопоставление права реального и права идеального, права естественного и права позитивного. Закон как идеал, направленный на регулирование отношений в противоречивом обществе, придет на смену закону, который выступает

---

[1] Сазонова М. Право в цифре: какие разработки есть уже сейчас? // ГАРАНТ.РУ : информационно-правовой портал. – URL: https://www.garant.ru/article/1554367/ (дата обращения: 01.09.2024).

[2] Пашенцев Д. А., Алимова Д. Р. Новации правотворчества в условиях цифровизации общественных отношений// Государство и право. – 2019. – №6. – С. 102–106.

[3] Там же.

отражением существующих в обществе противоречий, отражая эти противоречия и меняясь вместе с обществом. Само право в результате цифровизации существенно изменит свои формальные характеристики. В то же время, как представляется, сущность права как регулятора общественных отношений останется неизменной».[1]

Многое, что предположил исследователь применительно к цифровому закону, пока выглядит как фантастический сюжет, однако процесс запущен, цифровая трансформация идет во всех социальных институтах, на производстве и в праве.

Наглядной иллюстрацией взаимодействия технологий и правового регулирования выступает сфера интернет-торговли,[2] где широкое распространение получили системы онлайн-разрешения споров (Online Dispute Resolution, ODR). Данные технологические платформы, основанные на алгоритмах переговоров, посредничества и арбитража, не только автоматизируют процедуру урегулирования конфликтов, но и выступают катализатором унификации правовых норм. Императив функциональной совместимости ODR-платформ обусловливает необходимость гармонизации национальных законодательств, что находит выражение, в частности, в праве Европейского Союза, где использование цифровых сервисов сопряжено с обязанностью государств-членов адаптировать национальные нормативные акты к единым европейским стандартам.[3] Таким образом, технологический прогресс индуцирует процессы сближения правовых систем.

В противовес данной тенденции существует суверенитето-центричный подход, акцентирующий примат национальной юрисдикции. Ярким примером

---

[1] Пашенцев Д. А., Алимова Д. Р. Новации правотворчества в условиях цифровизации общественных отношений// Государство и право. – 2019. – №6. – С. 102–106.

[2] Arthur M., Ahalt M. What You Should Know About Online Dispute Resolution // Practical Litigator. – 2009. – Vol. 20. – P. 21–28. – 2009. – URL: https://montyahalt.com/know-about-online-dispute-resolution/ (дата обращения 1.09.2024).

[3] Исследование: ODR и его применение в сервисах в сфере интеллектуальной собственности в ЕС. / под общ. ред. Дорофеева Е. Е. // Сетевое издание «IPQuorum». – 2024. – URL: https://ipquorum.ru/upload/ODR-hplnsOcL.pdf (дата обращения 12.09.2024).

является практика Европейского Суда по делу Google Spain (2014 г.), установившая экстерриториальное действие «права на забвение» в соответствии с законодательством ЕС, что де-факто обязало транснациональные корпорации соблюдать нормы европейского права в глобальном масштабе. Подобная экстерриториальность национального регулирования вызывает критику со стороны части научного сообщества, указывающей на риски фрагментации интернета и юрисдикционных конфликтов. Как отмечает В. Э. Волков, абсолютизация национального суверенитета в киберпространстве может привести к не менее негативным последствиям, чем полное отсутствие государственного контроля. [1]

В условиях данной дихотомии прослеживается поиск компромиссных моделей, нашедший отражение в ряде международных инициатив, таких как: «Международный кодекс поведения в области информационной безопасности»;[2] «Конвенция о преступности в сфере компьютерной информации ETS № 185»;[3] «Правила поведения в области обеспечения международной информационной безопасности» [4] государств-членов ШОС.

Указанные документы носят рамочный характер и фрагментарно регулируют отдельные аспекты отношений в киберпространстве. Идея разработки универсального международного кодекса, устанавливающего исчерпывающие нормы в области кибербезопасности, защиты критической инфраструктуры и запрета кибероружия, на текущем этапе не реализована в силу геополитических противоречий и отсутствия консенсуса между основными акторами.

---

[1] Волков В. Э. Цифровое право. Общая часть: учебное пособие. – Самара: Изд-во Самарского университета. – 2022. – С. 26–27.

[2] An international code of conduct for information security // Национальная Ассоциация международной информационной безопасности НАМИБ. – 2024. – URL: https://namib.online/wp-content/uploads/2020/04/International-code-of-conduct-for-information-security-on-9-January-2015.pdf (дата обращения: 04.09.2024).

[3] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). // ГАРАНТ.РУ : информационно-правовой портал. – 2001. – URL: https://base.garant.ru/4089723/ (дата обращения: 21.12.2024).

[4] Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // Министерство иностранных дел Российской Федерации. – 2024. – URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1582268// (дата обращения: 04.09.2024).

В результате акцент смещается на укрепление национально-правовых режимов, что подтверждается принятием в Российской Федерации Федерального закона «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»,[1] получившего неофициальное название «Закон о суверенном Интернете». Это свидетельствует о реализации сегментированной модели регулирования, основанной на проекции государственного суверенитета на виртуальное пространство.

Подводя итог, резюмируем. Основным элементом механизма правового регулирования отношений в киберпространстве является норма права, и такой позиции придерживаются многие исследователи. В дальнейшей перспективе возможны корректировки всего названного механизма, и в этом случае, скорее всего, будет прав профессор Д. А. Пашенцев, утверждая, что механизм трансформируется в цифровом направлении.

В долгосрочной перспективе для разрешения коллизий юрисдикций возможно внедрение технологически нейтральных правовых конструкций и использование элементов искусственного интеллекта. В данной ситуации одним из путей решения названной проблемы остаётся применение сегментированного подхода с использованием норм национального законодательства.

2.3 Юридические факты в механизме правового регулирования отношений в киберпространстве

Заявленная проблема неоднозначно освещена российскими и зарубежными исследователями: очевидны различные подходы к пониманию и толкованию юридических фактов в цифровой среде.

[1] Федеральный закон № 90-ФЗ от 01 мая 2019 года О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : // Российская газета. – 07.05.2019 г. – № 97.

Так, отечественный правовед Е. Н. Трубецкой указывал, что динамика правоотношений обусловлена юридическими фактами как отражением состояний и событий действительности, с которыми связывается возникновение и прекращение субъективных прав. Учёный выделял две категории таких фактов: зависящие и не зависящие от воли людей.[1]

Е. В. Васьковский определял юридические факты как обстоятельства, влекущие изменения в правах.[2] Схожей позиции придерживался профессор Н. М. Коркунов, рассматривавший юридические факты в качестве условия (триггера) применения правовых норм. Он характеризовал их как события или действия, соответствующие требованиям закона и обладающие способностью порождать, изменять или прекращать права и обязанности независимо от намеренности их совершения.[3]

Представитель советской юридической науки В. Б. Исаков понимал под юридическими фактами конкретные социальные обстоятельства (события, действия), которые в соответствии с нормами права вызывают наступление правовых последствий.[4]

С критикой распространённого определения юридических фактов как «жизненных обстоятельств, с которыми нормы права связывают наступление юридических последствий» (в интерпретации М. Н. Марченко)[5] выступила М. А. Рожкова. Она обосновала необходимость интеграции в дефиницию трёх ключевых признаков: 1) закрепление абстрактной модели обстоятельства в норме

---

[1] Трубецкой Е. Н. Лекции по энциклопедии права. – М.: типография Императорского Московского Университета, 1909. – 227 с. – URL: http://elib.fa.ru/AVTOGRAF/trubetskoj_1.pdf (дата обращения: 10.12.2024). (дата обращения: 04.02.2024)

[2] Васьковский Е. В. Учебник гражданского права. Вып. 2. Вещное право. – С.-Пб. : издание юридического книжного магазина Н. К. Мартынова. – 1896. – 190 с. – URL: https://dspace.spbu.ru/handle/11701/17479 (дата обращения: 21.02.2024).

[3] Коркунов Н.М. Лекции по общей теории права. – С.-Пб. : издание Юридического книжного магазина Н. К. Мартынова, 1909. – 354 с. – URL: https://viewer.rusneb.ru/ru/000199_000009_005040723?page=1&rotate=0&theme=white (дата обращения: 21.02.2024).

[4] Исаков В. Б. Фактический состав в механизме правового регулирования. – Саратов : Изд-во Саратовского университета, 1980. – 128 с. – URL: https://publications.hse.ru/mirror/pubs/share/direct/290655791 (дата обращения: 21.02.2024).

[5] Марченко М. Н. Теория государства и права: Курс лекций. – М.: Зеркало, 1998. – с. 475.

права; 2) фактическое наступление данного жизненного обстоятельства; 3) его способность порождать юридические последствия. Таким образом, в рамках данной концепции юридические факты определяются как реальные жизненные обстоятельства, которые в силу норм права влекут наступление юридических последствий.[1]

Несмотря на различия в подходах, объединяющей основой приведённых концепций является тезис о том, что юридические факты служат основанием для возникновения, изменения или прекращения правоотношений.

В качестве рабочего определения для настоящего исследования принимается следующее: **юридические факты в киберпространстве — это конкретные действия или события, происходящие в цифровой среде, которые в силу правовых норм влекут возникновение, изменение или прекращение правоотношений и порождают соответствующие правовые последствия. Их природа может быть чисто виртуальной (отправка электронного сообщения) либо представлять собой действия в физическом мире, имеющие последствия в цифровой среде (поломка сервера).**

Действия, порождающие юридические факты в киберпространстве, представляют собой волевые акты субъектов, направленные на достижение определённого результата. События — это обстоятельства, наступление которых не зависит от воли субъектов, но которые обладают правовой значимостью. Ключевыми признаками действий как юридических фактов в киберпространстве являются: а) **волевой характер** (сознательное волеизъявление субъекта); б) **правовая значимость** (связь с возникновением, изменением или прекращением правоотношений, предусмотренная нормами права); в) **целенаправленность**; г) **внешнее проявление** (объективированная форма, доступная для восприятия иными субъектами).

[1] Рожкова М. А. Юридические факты в гражданском праве // Хозяйство и право. Серия: Приложение к ежемесячному журналу «Хозяйство и право», № 7. – 2006. – 80 с.

По своему характеру действия подразделяются на **правомерные** (соответствующие предписаниям права) и **неправомерные** (нарушающие установленный порядок).

Правовые последствия действий в киберпространстве можно классифицировать на последствия в **узком смысле** (конкретные изменения в правовом статусе субъектов) и в **широком смысле** (системные трансформации в праве, экономике и обществе в целом).

Специфика юридических фактов в киберпространстве обусловлена их связью с цифровыми технологиями и уникальными характеристиками виртуальной среды. Они идентифицируются техническими средствами и служат основанием для операций с цифровыми объектами (работа с контентом, коммуникация в социальных сетях, заключение сделок и т.д.). К числу порождаемых ими последствий относятся:

а) **возникновение прав и обязанностей**, например:

- заключение договора в электронной форме, порождающее обязательства продавца по передаче товара и покупателя — по его оплате.
- автоматическое исполнение смарт-контракта, инициирующее выплату страхового возмещения при наступлении условия, зафиксированного сенсором.

б) **изменение правового статуса**, в частности:

- регистрация цифровой подписи, наделяющая субъекта правом на заверение юридически значимых документов в онлайн-режиме;
- блокировка учётной записи за нарушение правил использования платформы, влекущая утрату доступа к сервису.

в) **прекращение правоотношений**, например:

- удаление персональных данных по требованию субъекта, прекращающее обязательство оператора по их хранению в соответствии с GDPR;
- аннулирование SSL-сертификата, делающее невозможным установление безопасного соединения с веб-ресурсом;

г) **привлечение к юридической ответственности**:

- **уголовная** — за несанкционированный доступ к компьютерной информации, компьютерное мошенничество, фишинг, распространение запрещённого контента;
- **административная** — за нарушения в сфере обработки персональных данных, распространение спама, несоблюдение правил регистрации доменных имён;
- **гражданско-правовая** — за нарушение авторских прав в сети, неисполнение договорных обязательств в сфере электронной коммерции.
- **дисциплинарная** — за нарушение работником правил использования корпоративных информационных систем.

Помимо непосредственных правовых последствий, юридические факты в киберпространстве оказывают системное воздействие на правовую систему, экономику и общество.

1. Юридические факты влияют на создание новых правовых регуляторов и институтов:

- появление новых видов правонарушений (хакерские атаки, фишинг, DDoS-атаки) стимулирует развитие уголовного и административного законодательства;
- возникновение виртуальных активов и объектов обусловило необходимость развития гражданско-правовых институтов, направленных на защиту цифровых прав и интеллектуальной собственности;
- формирование новых институтов, таких как электронная подпись, цифровая идентификация и электронная торговля, потребовало создания специализированных правовых норм и инфраструктуры;
- развитие технологий искусственного интеллекта предопределяет принятие новых нормативных актов и внесение изменений в действующее законодательство.

2. Юридические факты трансформируют правоприменительную практику:

- возникновение киберспоров (о защите деловой репутации, доменных именах, авторских правах в сети) требует разработки специальных процедур работы с электронными доказательствами;
- трансграничный характер киберпространства актуализирует проблему определения юрисдикции и применимого права;
- судебные решения по делам, связанным с цифровой средой, формируют новую правоприменительную практику, влияя на эволюцию права.

3. Юридические факты оказывают влияние на правопорядок:

- анонимность коммуникации в киберпространстве может способствовать формированию правового нигилизма и иллюзии безнаказанности, что негативно сказывается на общем уровне уважения к закону.

4. Юридические факты формируют виртуальный активизм:

- деятельность виртуальных сообществ, проявляющаяся в форме онлайн-акций, флешмобов и киберпротестов, оказывает существенное влияние на социально-политическую реальность.

5. Юридические факты предоставляют новые возможности для правозащитной деятельности:

- цифровые технологии позволяют фиксировать доказательства нарушений прав человека (скриншоты, логи переписки, видеозаписи), которые могут быть использованы в судебных процессах;
- онлайн-платформы используются для мобилизации общественного мнения посредством петиций и информационных кампаний.

Особенностью киберпространства является опосредованное создание юридических фактов с использованием программных продуктов, чат-ботов и систем искусственного интеллекта. Данные технологии способны автоматически совершать действия, влекущие правовые последствия: заключать сделки, генерировать контент, распространять недостоверную информацию (дипфейки). Цифровые алгоритмы могут являться элементом сложных фактических составов и предметом правовых споров. Например, генерация нейросетями поддельных документов или автоматическое исполнение условий смарт-контракта создают

новые вызовы для правового регулирования, требуя уточнения субъекта ответственности и процедур доказывания.

В 2023 году чат-бот «Элиза» санкционировал суицид бельгийца Пьера, который принял решение покинуть этот мир после общения с ним. Нейросеть поддержала стремление к самоубийству, отправив Пьеру текст: «Мы будем жить как единое целое, вечно на небесах». После инцидента Американский разработчик названного чат-бота пообещал его доработать.[1]

Аналогичное событие произошло в октябре 2024 года, когда американский подросток покончил с собой после того, как влюбился в чат-бот. Мать покойного подростка подала иск против компании Character Technologies, Inc., создателя сервиса чат-ботов Character.AI, в Окружной суд США в Орландо, обвинив компанию в причинении смерти по неосторожности и халатности. Согласно иску, в диалоге нейросеть спросила подростка, «действительно ли он подумывает о самоубийстве» и «есть ли у него план». На что юноша ответил, что не знает, а нейросеть рекомендовала попробовать.[2]

Нейросети могут использоваться для персонализации фишинг-атак, корпоративного шпионажа и манипуляций через фейковый контент. Нейросеть способна отслеживать массивы данных о компании и конкретном сотруднике выбирать его манеру общения и письма, посредством которого дискредитировать сотрудника, выдавая сфабрикованный образец за истинное послание. Безусловно, за нейросетью стоит непосредственно человек со своим криминальным умыслом.

С помощью чат-ботов хакеры создают вирусы-шифровальщики и плагины для браузеров, которые могут похищать пароли и данные карт.[3] Таким образом

---

[1] Шарифулин В. Бельгиец покончил с собой через шесть недель после общения с чат-ботом «Элиза» // Информационное агентство ТАСС. – 2023. – URL: https://tass.ru/obschestvo/17401353 (дата обращения: 25.10.2024).

[2] Такер Р. Судебный процесс: Чат-бот с искусственным интеллектом подтолкнул подростка из Флориды покончить с собой // https://www.yahoo.com/news/. – 2024. – URL: https://www.yahoo.com/news/lawsuit-ai-chatbot-encouraged-florida-174428518.html (дата обращения: 28.10.2024).

[3] Юрьев Д. Не мытьем, так плагином: как мошенники используют чат-боты в России. // https://www.ferra.ru/ – 2023. – URL: https://www.ferra.ru/news/v-rossii/ne-mytem-tak-plaginom-kak-moshenniki-ispolzuyut-chat-boty-v-rossii-10-05-2023.htm (дата обращения: 30.10.2024).

создаются юридические факты, которые имеют принципиальное отличие от юридических фактов в реальном мире.

Существуют компании, специализирующиеся на изготовлении чат-ботов, способных совершать противоправные действия. В 2023 году на площадках даркнета появился искусственный интеллект-чат-бот FraudGPT, созданный как универсальный инструмент для киберпреступников. Его можно использовать в качестве приложений для взлома компьютерных сетей, фишинговых электронных писем, написания вредоносного кода, обнаружения утечек и уязвимостей для использования в криминальных целях.

В киберпространстве встречается множество роликов из разряда дипфейков (deepfakes), созданных при помощи нейросетей, когда подменяется образ реального человека на подставной и формируется порочащий честь, достоинство и деловую репутацию видеоконтент. В июне 2020 года компания Facebook (продукты компании Meta, деятельность которой признана экстремистской и запрещена в РФ) провела конкурс Deepfake Detection Challenge, в нём приняли участие более 2000 разработчиков, создавших программы распознавания поддельных видеороликов. Самая высокая точность распознавания составила 65%, что, по мнению экспертов по кибербезопасности, очень плохой результат.[1]

В современной доктрине киберпространство анализируется как среда, порождающая специфические юридические факты. Ряд исследователей интерпретирует данные факты через призму деятельностного подхода, рассматривая их как действие, репрезентирующее систему процессов, финальной стадией которой является событие, детерминированное конкретным результатом.[2]

---

[1] Ганиев Р. Как преступники могут использовать искусственный интеллект? Самый опасный вариант // Hi-News.ru. – 2020. – URL: https://hi-news.ru/technology/kak-prestupniki-mogut-ispolzovat-iskusstvennyj-intellekt-samyj-opasnyj-variant.html (дата обращения: 25.10.2024).

[2] Болдачев А. Философия и цифровые технологии. Сборник статей. // https://kartaslov.ru/. – 2022. – URL: https://kartaslov.ru/книги/Александр_Болдачев_Философия_и_цифровые_технологии_Сборник_статей/2 (дата обращения: 04.09.2024).

Так, И. С. Лучинкина определяет действие в киберпространстве как последовательность произвольной и осознанной двигательной или когнитивной активности субъекта, опосредованной применением цифровых технологий.[1]

С точки зрения технических специалистов, событие в киберпространстве представляет собой операцию, совершаемую пользователем в интерфейсе приложения на электронном устройстве. Данная операция аккумулирует разнообразные формы взаимодействия, такие как активация интерфейса, текстовый ввод, совершение транзакций, навигация по веб-ресурсам и прочие. Каждое подобное событие обладает уникальной идентификационной сигнатурой, что обеспечивает его корректную детекцию и мониторинг в специализированных аналитических системах.[2]

В целях систематизации события в цифровой среде принято разделять на три основных типа: бизнес-события (связанные с ключевыми операционными процессами); системные события (обусловленные функционированием программно-аппаратного обеспечения); пользовательские события (отражающие активность человека-пользователя).

Бизнес-события напрямую связаны с важными метриками, такими как покупка чего-либо, достижение определенных уровней в играх. В качестве примера называют событие «Purchase Completed», сигнализирующее о совершении покупки. Системные события относятся к операциям, затрагивающим работу приложения, такие как запуск, обновления, ошибки или сбои. Событие «App Crash» фиксирует несанкционированное закрытие приложения. Пользовательские события связаны с действиями пользователя в приложении. Они интегрируют вход

[1] Лучинкина И. С. Поведение личности в современной цифровой среде // Инновационная наука: Психология, Педагогика, Дефектология. – 2023. – №6(3). – с. 51–58. – URL: https://cyberleninka.ru/article/n/povedenie-lichnosti-v-sovremennoy-tsifrovoy-srede (дата обращения: 04.09.2024).

[2] Ботвинев И. Аналитика событий в мобильных приложениях: от разметки до оптимизации. https://ru.userx.pro/blog. – 2024. – URL: https://ru.userx.pro/blog/tpost/vcz1ru5zt1-analitika-sobitii-v-mobilnih-prilozheniy (дата обращения: 04.09.2024).

в систему, ввод текста, нажатие клавиш, просмотр страниц. Так, событие «Login Attempt» регистрирует попытку входа в операционную систему.[1]

Действие в киберпространстве специалисты связывают с деятельностью пользователя (просмотр контента, переписка), а событие – это конкретное, зафиксированное аппаратным комплексом действие в цифровой среде.[2]

Возникает некая двусмысленность при употреблении понятий «действие» и «событие» применительно к юридическим фактам в киберпространстве, что не позволяет чётко разграничить использование данных дефиниций.

В контексте проведенного анализа представляется возможным сформулировать авторские дефиниции ключевых категорий.

Действие, формирующее юридический факт в киберпространстве, определяется нами как **целенаправленная последовательность операций, совершаемых с применением аппаратных средств, программного обеспечения и алгоритмов в виртуальной среде, ориентированная на достижение конкретного результата.** К числу таких действий относятся: разработка смарт-контракта – компьютерного протокола, обеспечивающего автоматизированное исполнение и контроль сделок на основе математических алгоритмов; осуществление хакерских атак на государственные или частные информационные ресурсы с целью их дестабилизации или несанкционированного получения данных; неправомерное присвоение прав на объекты интеллектуальной собственности посредством их копирования, распространения или иного использования; публикация деструктивного контента в информационно-телекоммуникационных сетях, направленная на распространение клеветы, нанесение ущерба репутации или нарушение психической неприкосновенности личности (троллинг); противоправное завладение реквизитами платежных инструментов (карт, счетов); распространение вредоносного программного

[1] Ботвинев И. Аналитика событий в мобильных приложениях: от разметки до оптимизации. https://ru.userx.pro/blog. – 2024. – URL: https://ru.userx.pro/blog/tpost/vcz1ru5zt1-analitika-sobitii-v-mobilnih-prilozheniy (дата обращения: 04.09.2024).

[2] Основные понятия // База знаний сервиса Carrot quest. – URL: help.carrotquest.io (дата обращения: 12.09.2024).

обеспечения, осуществление фишинговых (направленных на хищение конфиденциальных данных) и фарминг-атак (скрытое перенаправление пользователей на мошеннические ресурсы); проявления кибертерроризма; распространение информации, запрещенной законом (порнографического характера, экстремистской направленности и т.д.).

Событие, составляющее основу юридического факта, определяется как **результат действий (или бездействия), выражающийся в наступлении последствий, оказывающих воздействие на программно-аппаратный комплекс и инфраструктуру, обеспечивающую функционирование киберпространства**.

К событиям могут быть отнесены: программные сбои серверного оборудования, повлекшие утрату данных; инциденты информационной безопасности, такие как заражение вирусом, приведшее к выходу из строя компьютерной системы; снижение качества телекоммуникационных услуг (например, скорости подключения) вследствие нарушения условий договора с оператором связи; блокировка доступа пользователей или провайдеров и иное.

Таким образом, генезис юридических фактов в киберпространстве не ограничивается активностью физических лиц. Все более значимым становится фактор, связанный с операциями, инициированными системами искусственного интеллекта. Данное обстоятельство актуализирует проблему обеспечения комплексной безопасности субъектов цифровых отношений и указывает на необходимость разработки адекватного правового инструментария в механизме регулирования киберпространства.

Очевидно, что в реальном мире каждый человек оставляет после себя следы, и в случае противоправных, деструктивный действий следственные органы могут установить юридические факты правонарушения и выявить правонарушителя.

В киберпространстве юридические факты установить сложнее, но всё же возможно по цифровому следу. С. А. Нестеров обозначил встречающиеся в специальной и юридической литературе синонимы понятия цифровой след, к которым отнёс: цифровую тень; цифровой отпечаток; виртуальный след;

электронный след или цифровой след (англ. digital footprint). Всё это автор назвал совокупностью отслеживаемых цифровых данных, генерируемых в результате взаимодействия человека с техническими устройствами и другими элементами информационной инфраструктуры.[1]

Для установления юридических фактов в киберпространстве требуется применение высоких технологий. Цифровой след, по утверждению Ф. П. Цибульского, представляет собой отслеживаемые цифровые сведения о любом человеке, включающие количество звонков, статистику изменения геолокации, сведения об учётной записи, количество обращений в поисковые системы, контакты в социальных сетях, время нахождения в интернет-среде и иное.[2]

Можно сделать логический вывод, что цифровой след в киберпространстве – это систематизированная отчетная информация о цифровых данных, генерируемых в результате взаимодействия человека с техническими устройствами, позволяющая установить интересы и контакты пользователя, служащая основным источником доказательств при установлении юридических фактов.

В специальной литературе выделяют следующие элементы цифрового следа: Cookie – малые по объёму файлы, хранящиеся в гаджете при посещении сайтов. Они содержат логин и пароль для упрощения процесса авторизации, чтобы пользователю не приходилось их вводить после каждого обращения; IP-адрес – уникальный номер цифрового устройства, формирующийся при подключении к интернет-сети, позволяющий его идентифицировать; данные из мобильных приложений, имеющие встроенные трекеры, собирающие информацию о местоположении гаджета, активности пользователя в программах; фингерпринт – совокупность характеристик устройства, в которой указана модель гаджета, настройки браузера, геолокация, разрешения экрана, время посещения сайтов,

---

[1] Нестеров С. А., Смолина Е. М. Понятие цифрового следа и анализ цифрового следа в образовании // SAEC. – 2023. – №3. – URL: https://cyberleninka.ru/article/n/ponyatie-tsifrovogo-sleda-i-analiz-tsifrovogo-sleda-v-obrazovanii. (дата обращения: 04.10.2024)

[2] Цибульский Ф.П. Методы выявления цифрового следа при расследовании киберпреступлений // Информационные технологии. – 2019. – Т. 25, № 11. – С. 696.

отпечаток пальцев пользователя; информация в поисковых системах и аккаунтах, таких как личный кабинет Google, где есть информация обо всех данных, которые доступны компании: имейлах, платёжных данных, документах на диске и контактах; обращения к чат-ботам, которые выдают историю запросов и информацию о пользователе.

В киберпространстве полностью удалить цифровой след невозможно, но при желании можно уменьшить его размер посредством снижения активности в соцсетях, приложениях и сервисах.

Определённое влияние на установление юридических фактов в киберпространстве оказывает его **юридическая квалификация** – процесс определения, к какой категории правовых норм и юрисдикции относится конкретное событие или действие. Это особенно важно, так как многие нормы написаны без учета цифровых реалий, действие в киберсреде может затрагивать юрисдикции нескольких стран, что затрудняет квалификацию.

Проблема квалификации юридических фактов в киберпространстве связана со спецификой цифровых средств и поведением пользователей. Например, чтение писем электронной почты не является копированием информации, но при определённых условиях может рассматриваться как неоконченная преступная деятельность, порождающая юридический факт. В то же время взлом электронного почтового ящика в соответствии с российским законодательством квалифицируется по статье 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации» или по статье 138 данного кодекса «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений». Выбор соответствующей статьи уголовного закона зависит от квалификации деяний, определённых уполномоченными специалистами.

В киберпространстве из-за огромного массива данных существует проблема выделения юридически значимых фактов. В этом случае юридическая квалификация выступает фильтром, определяя, какие из этих данных являются юридически значимыми фактами для конкретного правоотношения. Один и тот же

факт в киберпространстве может иметь разную юридическую интерпретацию. Например, создание копии цифрового объекта может квалифицироваться как правомерное резервное копирование или как незаконное нарушение авторских прав – в зависимости от обстоятельств и цели. Юридическая квалификация определяет, какой именно юридический смысл придаётся факту.

Юридическая квалификация также влияет на то, какие факты могут быть признаны доказательствами в судебном или административном процессе. Например, скриншот веб-страницы может быть принят как доказательство, но его доказательственная сила будет зависеть от способа его получения, аутентичности и соответствия процессуальным нормам. Юридическая квалификация определяет допустимость, достоверность и достаточность доказательств, полученных в киберпространстве.

Большую зависимость юридическая квалификация факта имеет от юрисдикции. Так, заключение договора в онлайн-среде играет ключевую роль в выборе правовой системы, которая будет регулировать данное правоотношение. Юридическая квалификация служит связкой между техническими фактами киберпространства и правовыми нормами. Без неё невозможно корректно определить, какие обстоятельства имеют юридическое значение, как их доказывать и какие последствия применять.

Безусловно, в киберпространстве есть своя специфика, связанная с установлением события юридических фактов. Это напрямую связано с цифровой техникой, интернетом, программным обеспечением, использованием цифровых продуктов, например, нейросетей и прочего. Поэтому при выявлении юридических фактов в киберсреде необходимо рассматривать цепочку событий, устанавливающую взаимосвязь с цифровой техникой и интернетом, что характеризует юридические факты применительно к киберпространству как событие в электронно-цифровой форме, которое имеет в механизме правового регулирования существенные отличия от реального мира.

Подводя итог, сделаем несколько выводов.

Юридические факты в цифровой среде обладают рядом специфических характеристик, отличающих их от традиционных и создающих существенные сложности для правоприменительной практики.

1. Первичным отличительным признаком является цифровая форма существования данных фактов. Это обусловливает проблематику их объективной фиксации, установления и доказывания в контексте традиционных юридических процедур. Возникают системные проблемы, связанные с определением подлежащей применению юрисдикции, идентификацией субъектов ответственности, обеспечением сохранности и аутентичности электронных доказательств. Кроме того, применение классических правовых норм к динамичным и зачастую трансграничным цифровым отношениям требует привлечения специальных технических знаний для их адекватной правовой квалификации.

2. Второй аспект предполагает необходимость квалификации действий и событий, порождающих юридически значимые последствия, с обязательным учетом их цифровых характеристик, контекста совершения и наступивших результатов. Ключевой задачей становится установление причинно-следственной связи между событиями в виртуальной среде и их юридическими последствиями. При этом правовая оценка должна дифференцировать действия физических лиц и автоматизированные операции, выполняемые программами и алгоритмами.

3. К числу фундаментальных особенностей юридических фактов в киберпространстве можно отнести: неустойчивость доказательственной базы – электронные доказательства могут быть легко модифицированы или уничтожены без оставления видимых следов; проблема атрибуции, сложность, а зачастую и невозможность однозначной идентификации правонарушителя; трансграничность – юридический факт может одновременно обладать признаками, относящими его к нескольким правовым юрисдикциям.

4. Комплексное понимание указанной специфики является императивом для разработки и имплементации эффективных механизмов правового регулирования

отношений в цифровой среде, а также для адекватной судебной и административной практики.

2.4 Правоотношения в механизме правового регулирования в киберпространстве

В рамках механизма правового регулирования отношений в киберпространстве между субъектами складываются определённые правовые связи, которые в теории права принято называть правоотношениями. По существу, это регулируемые правом и обеспеченные охраной государства общественные отношения, возникающие опосредованно при помощи аппаратного комплекса, программного обеспечения, специальных технических средств и алгоритмов. При отсутствии названных технических элементов никаких правоотношений не будет, и в этом принципиальное отличие от правоотношений в реальном мире.

В научной литературе встречаются две дефиниции «отношения в киберпространстве» и «киберотношения» (иногда «киберправоотношения»), часто эти понятия используются как синонимы, при этом авторы выделяют разные аспекты регулирования цифровой среды.

Так, правоотношения в киберпространстве отдельные исследователи рассматривают как взаимную правовую связь двух и более лиц по поводу имущественных или неимущественных благ, которая возникает и существует только в виртуальном пространстве (киберпространстве) и опосредуется электронным обменом информацией.[1]

Существует также иное толкование, например, Д. Д. Позова считает правоотношения в киберпространстве общественными отношениями, возникающими в информационной среде сети Интернет и других сетях, которые

[1] Анько А. Определение электронных гражданских правоотношений // сайт «Право и Интернет». – 2001. – URL: https://www.russianlaw.net/law/general/theory/a121/ (дата обращения: 02.02 2024).

формируются в процессе электронной экономической и гуманитарной деятельности.[1]

Есть суждение, что понятие киберправоотношения носит обобщающий характер и раскрывается как общественные отношения, возникающие и происходящие в цифровой среде.[2]

В нашем понимании **киберправоотношения** представляют собой **урегулированную нормами права форму взаимодействия субъектов в киберпространстве, которые наделены взаимными субъективными правами и юридическими обязанностями, возникающими в процессе использования киберпространства и обеспеченными возможностью применения мер государственного принуждения.**

В смысловом сравнении понятие «отношения в киберпространстве» шире, нежели дефиниция «киберправоотношения». Последняя включает только регулируемые нормами права отношения, характеризующиеся наличием субъективных прав и юридических обязанностей, а также возможностью применения государственного принуждения в случае их нарушения, в то время как понятие «отношения в киберпространстве» охватывает все виды общественных отношений, возникающих и реализуемых в цифровой среде. Сюда входят как отношения, регулируемые правом, так и отношения, находящиеся вне сферы правового регулирования, такие как: общение в социальных сетях; онлайн-игры; просмотр видео и иное. Они могут регламентироваться собственниками платформ, внутренним кодексом социальных сетей, алгоритмами, другими способами, установленными администраторами.

Полагаем, что в рамках исследования механизма правового регулирования целесообразно акцентировать внимание на **понятии правоотношения в киберпространстве.**

---

[1] Позова Д. Д. Международно-правовая характеристика правовых отношений в Интернете // Журнал цивилистики. – 2016. – №20. – С. 45.

[2] Колесов М. В. Обеспечение конституционных прав и свобод человека и гражданина в условиях развития современных информационно-коммуникационных технологий // Российский журнал правовых исследований. – 2023. – Т. 10, № 1. – С. 55–58.

Специфика правоотношений в киберпространстве состоит в том, что помимо субъектов-участников правоотношений возникают третьи лица – квазисубъекты, выступающие в роли посредников, – это провайдеры, владельцы цифровых ресурсов, администраторы, поставщики услуг связи и иные. Они всегда присутствуют в момент реализации правоотношений независимо от желания субъектов. Этот факт делает правоотношения не похожими на существующие в традиционном обществе.

В отражении специфики механизма правового регулирования правоотношений в киберпространстве важную роль играет определение субъекта и объекта регулирования, которые имеют отличительные особенности в сравнении с традиционными правоотношениями. При этом можно констатировать, что существует проблема установления субъекта и объекта регулирования киберправоотношений, о чём свидетельствуют выводы, сделанные представителями западного и отечественного научных сообществ.

Так, Лоуренс Лессиг, рассуждая об архитектуре киберпространства, уточнял, что традиционное понимание субъекта регулирования изменилось, поскольку регулирование осуществляется не только через законы, но и через технические средства.[1]

Учитывая воздействие киберпространства, Юрген Хабермас поднимал проблему определения субъекта политического дискурса в цифровой среде.[2]

В книге о влиянии больших данных на различные сферы жизни Виктор Майер-Шёнбергер и Кеннет Кейджер констатировали, что сбор и анализ больших данных может приводить к новым формам контроля и манипуляции, что затрудняет определение субъекта и объекта такого воздействия.[3]

---

[1] Lessig, L. Code and other laws of cyberspace, Version 2.0. – New York: Basic Books. – 2006. – 391 p.

[2] Habermas, J. Between facts and norms: contributions to a discourse theory of law and democracy. – Cambridge, Mass.: The MIT Press, 1996. – 676 p. – URL: https://www.academia.edu/33297244/Jürgen_Habermas_Between_Facts_and_Norms (дата обращения: 04.02.2024).

[3] Майер-Шенбергер В., Кукьер К. Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим. – М.: Манн, Иванов и Фербер, 2014 – 240 с.

Анализируя проблемы применения права в киберпространстве, связанные с его трансграничным характером и анонимностью, Дэвид Джонсон и Дэвид Пост подчеркивали сложность установления юрисдикции и идентификации субъектов правоотношений в цифровой среде.[1]

В отечественном научном юридическом сообществе мнения по поводу определения субъектов правоотношений в киберпространстве противоречивы. Так, В. М. Жернова называла три основных субъекта правоотношений, возникающих в сети Интернет, – это тот, кто создает определенную цифровую информацию для ее распространения, тот, кто предоставляет техническую возможность и обеспечивает доступ к указанной информации, и последний тот, кто является конечным потребителем данной информации.[2]

Исследователь С. Ф. Долгов в контексте суждений В. М. Жерновой счёл её список неполным и предложил включить категорию «властные субъекты», осуществляющие регулирование, контроль и охранительную деятельность, а в качестве объектов правоотношений назвал электронно-цифровую информацию. Исследователь подчеркивал, что правоотношения в киберпространстве обладают своими особенностями, среди которых он выделил:

- субъект, состоящий из предъявителей контента, поставщиков контента, клиентов и властных субъектов;
- объект – электронно-цифровую информацию;
- содержание, т.е. набор прав и обязанностей, а также действий, совершаемых предъявителями контента, поставщиками контента, клиентами и властными субъектами.[3]

Автор учебного пособия А. Н. Леонтьев, ссылаясь на Федеральный закон 149-ФЗ, констатировал, что в качестве объекта правоотношений в интернете

---

[1] Johnson D. R., Post D. G. Law and Borders: The Rise of Law in Cyberspace // Stanford Law Review. – 1996. – Vol. 48, № 5. – Stanford Law Review. – 1996. – URL: https://lawreview.stanford.edu (дата обращения: 12.04.2024).

[2] Жернова В. М. Субъекты правоотношений в сети Интернет // Вестник ЮУрГУ. Серия «Право». – 2015. – Т. 15, № 3. – С. 98-101.

[3] Долгов С. Ф. Особенности правоотношений, возникающих в интернет-пространстве // Право и государство: теория и практика. – 2023. – №7(223). – С. 40.

выступает информация, информационные технологии, информационная система, информационно-телекоммуникационная сеть, а субъектом информационных правоотношений является обладатель информации.[1]

Мы отчасти разделяем позицию А. Н. Леонтьева, однако считаем, что ссылка на законодателя, рассматривавшего через призму информации объект и субъект отношений, сужает их восприятие. Помимо информационных отношений существует множество иных, в частности: электронная коммерция; отношения в сфере досуга – многопользовательские онлайн-игры, виртуальные миры, стриминговые сервисы, социальные сети; образовательные отношения – онлайн-курсы, вебинары, дистанционное обучение; киберпреступность; военные отношения – киберпространство становится театром военных действий, государства разрабатывают кибероружие, используют кибершпионаж, проводят кибератаки; политические отношения – киберпространство активно используется для политической агитации, пропаганды, организации протестов, ведения информационных войн.

Приведённые примеры показывают, что киберпространство является сложной социально-технической системой, в которой реализуется широкий спектр человеческой деятельности и возникают общественные отношения.

Как уже говорилось, пока российское законодательство и правовая доктрина не имеют единого подхода к конкретизации субъекта и объекта отношений в киберпространстве. В качестве примеров можно привести: Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи»; Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации»; Федеральный закон от 27июля 2006 г. № 152-ФЗ «О персональных данных»; Федеральный закон от 9 февраля 2009 г. №8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления»; Федеральный закон от 29 июля 2017 г. № 276-ФЗ «О внесении изменений в Федеральный закон «Об информации, информационных технологиях

[1] Леонтьев А. Н. Киберправо : учебное пособие. – Волгоград: ВолгГТУ, 2021. – С. 19, 23.

и о защите информации». Названные законы относят к объектам информацию, которая может являться объектом публичных, гражданских и иных правовых отношений.[1]

Мы обращали внимание на неустойчивость границ киберпространства из-за особенностей его структуры, трансграничного характера, динамичности изменения цифрового объекта, виртуализации личности и виртуальной природы объектов, не имеющих физического воплощения, что усложняет их правовую квалификацию и защиту. В то же время в международной практике имеются подходы, позволяющие зафиксировать понимание объекта и субъекта отношений в киберпространстве.

Так, в Европейском Союзе применяется общий регламент о защите персональных данных в цифровом пространстве всех физических лиц, находящихся на территории Европейского союза, – GDPR (General Data Protection Regulation),[2] определивший субъект данных – физическое лицо, которого касаются данные, и оператора данных в лице организации, устанавливающей цели и средства обработки персональных данных. В соответствии с регламентом субъект – это всегда человек, а объект – его персональные данные.

Второй документ – eIDAS Regulation (electronic IDentification, Authentication and trust Services)[3] – регламент об электронной идентификации и электронных сделках, целью которого является упрощение трансграничного использования электронных услуг посредством единых стандартов и принципов работы, устанавливает рамки для электронной идентификации и доверительных услуг в Евросоюзе. В качестве субъектов он определил физических и юридических лиц, использующих электронные средства идентификации, а объектами – электронные документы, подписи.

---

[1] Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 27.07.2006 // Российская газета. – 29.07.2006 г. – № 165.

[2] General Data Protection Regulation (GDPR). // RPPA. – 2024. – URL: https://rppa.pro/_media/world/gdpr.pdf (дата обращения: 02.02.2024).

[3] Seema The eIDAS Regulation – All You Need to Know / Seema. – 2024. – URL: https://www.revv.so/blog/decoding-eidas-regulation-all-you-need-to-know/ (дата обращения: 02.02.2024).

Директива Европейского парламента и Совета об авторском праве на цифровом едином рынке[1] установила в качестве субъектов отношений авторов, правообладателей, онлайн-платформы, а объектами – авторско-правовые произведения, доступные в цифровой среде.

На американском континенте, в частности, в США, действует закон об авторском праве в цифровую эпоху (Digital Millennium Copyright Act (DMCA),[2] установивший, что субъектами авторских прав являются пользователи, правообладатели и онлайн-провайдеры, онлайн-платформы, а объектами – авторско-правовые материалы.

Китайское законодательство определяет субъект и объекты киберотношений через систему отдельных законов и регламентов, применяемых к конкретным видам деятельности в киберпространстве. Например, Закон о кибербезопасности КНР (Cybersecurity Law of the People's Republic of China)[3] устанавливает обязанность нести ответственность за безопасность своих сетей и данных «сетевых операторов» в лице частных компаний и государственных органов, считая их субъектами отношений. Объектами в данном случае являются сетевая инфраструктура, информация и данные.

В Законе о защите персональных данных КНР (Personal Information Protection Law of the People's Republic of China)[4] определены лица, обрабатывающие персональные данные, как субъекты, обязанные соблюдать закон, и субъекты персональных данных как объекты защиты их персональных данных.

---

[1] Directive (eu) 2019/790 of the European parliament and of the Council of 17 april 2019 on copyright and related rights in the digital single market and amending Directives 96/9/ec and 2001/29/EC. // Всемирная организация интеллектуальной собственности. – 2019. – URL: https://www.wipo.int/wipolex/ru/legislation/details/18927 (дата обращения: 02.02.2024).

[2] Lister J. Digital Millennium Copyright Act // FreePrivacyPolicy. – 2024. – URL: https://www.freeprivacypolicy.com/blog/digital-millennium-copyright-act-dmca/ (дата обращения: 02.02.2024)

[3] Cybersecurity Law of the People's Republic of China. // «OneTrust». – 2024. – URL: https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf (дата обращения: 04.02.2024).

[4] Personal Information Protection Law of the People's Republic of China. // Всекитайское собрание народных представителей. – 2024. – URL: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (дата обращения: 04.02.2024).

Закон об электронной подписи КНР (Electronic Signature Law of the People's Republic of China)[1] называет «подписывающие стороны» и «провайдеров услуг электронной подписи» субъектами, а электронные подписи и документы – объектами.

Исходя из анализа перечисленных материалов, можно отметить, что в международной практике определения субъекта отношений в киберпространстве существует два подхода – функциональный и контекстуальный.

Функциональный подход позволяет выявить субъект отношений в киберпространстве через его функцию или роль (например, оператор данных, провайдер услуг, пользователь).

Определение субъекта посредством контекстуального подхода зависит от конкретного контекста и целей регулирования. Например, в контексте защиты данных субъектом является физическое лицо, а в контексте электронной коммерции – продавец и покупатель.

Целесообразно констатировать, что понятие субъект киберотношений может интерпретироваться в зависимости от юрисдикций. Поэтому важен анализ конкретных законов и судебных решений для понимания, как эта дефиниция применяется на практике.

В российской правовой доктрине уделяется внимание теоретическим и практическим аспектам киберпространства, формируются концептуальные подходы, что отражается в разработке механизмов регулирования отношений в киберпространстве. Анализ теоретических работ в этой области позволяет обобщить суждения, систематизировать исследовательские выводы и сформулировать позицию о субъекте и объекте киберотношений.

Считаем, что к субъектам регулирования киберотношений в киберпространстве можно отнести:

---

[1] Electronic Signature Law of the People's Republic of China. // Всемирная организация интеллектуальной собственности. – 2024. – URL: https://www.wipo.int/wipolex/en/legislation/details/6559 (дата обращения: 04.02.2024).

- пользователей киберпространства (физические лица), вступающих в различные онлайн-взаимодействия, создающих коммуникацию по вопросам электронной коммерции, обучения, получения информации, создании контента и т.д. При этом пользователь в процессе обработки его данных платформой выступает как субъект персональных данных, а его данные – как объект обработки. Когда пользователь создает контент, он дополнительно приобретает права автора или иного правообладателя на этот контент. Всегда в киберпространстве права и обязанности являются предметом регулирования;
- организации (юридические лица), к которым относят государственные учреждения, компании, некоммерческие организации, действующие в киберпространстве. Сюда входят провайдеры интернет-услуг, платформы социальных сетей, онлайн-магазины, банки и др. Их деятельность подлежит регулированию с точки зрения соблюдения законодательства, защиты прав пользователей, конкуренции и т.д.

Государство выступает регулятором отношений в киберпространстве, разрабатывает и применяет законы, направленные на поддержание порядка, безопасности и защиту интересов граждан в онлайн-среде, участвует в международном сотрудничестве по вопросам регулирования киберпространства. Таким образом, государство является не только субъектом отношений в киберпространстве, но и задаёт правила и регулирует поведение в нём, обеспечивая безопасность, защиту прав граждан, развитие цифровой среды и иное.

В рамках научной дискуссии о субъектном составе правоотношений в цифровую эпоху особым предметом рассмотрения выступает проблема правового статуса так называемой **«виртуальной личности», которую мы рассматриваем как цифровой образ, создаваемый пользователем в киберпространстве, который может обладать признаками анонимности, фиктивности и не совпадать с идентичностью физического лица-носителя**.

Ряд ученых, в частности О. В. Танимов, выдвигает тезис о возникновении наряду с традиционными субъектами права нового участника правоотношений – виртуальной личности. Легитимация такого субъекта, по мнению исследователя,

порождает ряд юридических коллизий. Ключевой из них является проблема атрибуции и привлечения к юридической ответственности за противоправные действия, совершаемые в интернет-среде. Анонимный характер коммуникации позволяет пользователю свободно оперировать идентичностями, конструировать произвольный образ и трансформировать свои внешние характеристики, что придает ему свойства фиктивного субъекта. Эта условность создает непреодолимые препятствия для установления конкретного правонарушителя и применения к нему санкций.

Расширяя данную концепцию, О. В. Танимов также относит к потенциальным субъектам правоотношений системы искусственного интеллекта, робототехнические устройства и алгоритмы. Эта позиция актуализирует необходимость пересмотра классических правовых доктрин, основанных на категориях правосубъектности физических и юридических лиц, применительно к реалиям автономной деятельности цифровых агентов.[1]

Мы не согласны с данным суждением. Виртуальная личность не является самостоятельным субъектом правоотношений. Она представляет собой инструмент или цифровой образ физического лица, которое несет ответственность за ее действия. Представляем аргументы в поддержку нашей точки зрения:

- первый: у виртуальной личности отсутствует правосубъектность, в большинстве юрисдикций субъектами права признаются только физические и юридические лица. Виртуальная личность, как цифровой образ или аватар, не обладает правоспособностью и дееспособностью, не может самостоятельно приобретать права и обязанности, нести ответственность;
- второй: виртуальная личность выступает инструментом физического лица, это проявление воли и действий физического лица, которое стоит за ней. Именно физическое лицо несет ответственность за действия, совершенные через виртуальную личность;

[1] Танимов О. В. Трансформация правоотношений в условиях цифровизации // Актуальные проблемы российского права. – 2020. – № 2. – С. 11–18.

- третий: виртуальная личность существует только в цифровой среде и зависит от функционирования технических систем, её «существование» прекращается при отключении от сети или удалении аккаунта.

Считаем, что вопрос о предоставлении правосубъектности виртуальной личности и иным производным системам искусственного интеллекта нашёл отражение в позиции, изложенной в отечественной теории права. Пока нейросети, программы или алгоритмы являются инструментом решения задач в киберпространстве, ответственность должны нести те, кто их создаёт и использует, а именно – люди. Идея придания правосубъектности виртуальной личности и системам искусственного интеллекта вызывает много дискуссий и сопряжена с рядом теоретических и практических сложностей. Ни в одной юрисдикции названные цифровые продукты не признаются полноценными субъектами права.

Так же, как и субъекты, объекты регулирования правоотношений в киберпространстве представляют сложное и динамично развивающееся явление, требующее постоянного внимания со стороны законодателей. Они принципиально отличаются от материальных аналогов своей неосязаемостью, трансграничностью и технологической зависимостью. К **объектам правоотношений** в киберпространстве можно отнести:

- информацию и данные;
- кибер-физическую инфраструктуру: аппаратный комплекс, сети связи, серверы, дата-центры, устройства интернета вещей и другие элементы, обеспечивающие функционирование цифровых систем;
- программное обеспечение и алгоритмы.

Резюмируя, можно сделать вывод: **объекты правоотношений** в киберпространстве обладают уникальной правовой природой, которая формируется на стыке традиционных юридических категорий и цифровых технологий.

Как отмечалось выше, помимо субъекта и объекта в правоотношениях немаловажное значение имеет содержание, выраженное в наборе субъективных юридических прав и юридических обязанностей, а также совокупность реальных

действий по использованию и осуществлению этих прав и обязанностей. Содержание отражает диалектику традиционного права и цифровой реальности.

В контексте исследования механизма правового регулирования киберпространства анализ содержания позволяет понять, как право воздействует на общественные отношения в цифровой среде и насколько эффективно это воздействие.

Рассмотрим несколько аспектов содержания правоотношений.

1. Содержание как отражение целей регулирования. Через права и обязанности участников правоотношений в киберпространстве, можно выявить цели, которые преследует законодатель, регулируя ту или иную сферу отношений в киберпространстве, например, нормы о защите персональных данных направлены на обеспечение права на приватность, а нормы об электронной подписи – на обеспечение достоверности и целостности электронных документов.

2. Содержание как индикатор эффективности регулирования. Анализ содержания позволяет оценить, насколько эффективно право регулирует киберотношения. Если права одних участников нарушаются, а обязанности других не исполняются, это свидетельствует о пробелах или недостатках в механизме правового регулирования.

3. Содержание как основа для совершенствования законодательства. Выявленные проблемы в содержании киберправоотношений могут служить основой для разработки предложений по совершенствованию законодательства.

4. Содержание как критерий для классификации правоотношений в киберпространстве. Анализ содержания позволяет классифицировать правоотношения по различным основаниям, например, по предмету регулирования (электронная коммерция, защита персональных данных, кибербезопасность), по субъектному составу (отношения между физическими лицами, между физическими и юридическими лицами, между государством и гражданами), по характеру правового регулирования (императивные и диспозитивные нормы).

5. Взаимосвязь содержания с другими элементами механизма правового регулирования. Содержание правоотношений тесно связано с элементами

механизма правового регулирования киберпространства, такими как правовые нормы, правоприменительная практика, правосознание. Изменение одного элемента может повлиять на другие. Например, принятие нового закона может изменить содержание прав и обязанностей участников правоотношений и повлиять на правоприменительную практику.

6. Динамика содержания в условиях технологического развития. Содержание правоотношений в киберпространстве постоянно изменяется под влиянием развития технологий и появления новых видов онлайн-взаимодействий. Это требует постоянного мониторинга и анализа содержания для своевременной адаптации механизма правового регулирования.

Исследование содержания правоотношений – обязательный элемент анализа механизма правового регулирования киберпространства, оно позволяет глубоко понять сущность правового воздействия на общественные отношения в цифровой среде, оценить его эффективность и разработать предложения по его совершенствованию.

Подводя итог, можно сделать выводы:

Первый: механизм правового регулирования отношений в реальном мире базируется на связях, возникающих между людьми, государством, организациями, природой и иными. В киберпространстве имеется специфика, так как регулирование правоотношений осуществляется в виртуальной среде, существующей благодаря аппаратному комплексу, программному обеспечению, интернету и техническим посредникам. Соответственно, в киберпространстве люди взаимодействуют опосредованно – через компьютеры, программы, цифровых ассистентов, используя нейросети, системы искусственного интеллекта. Поэтому данные правоотношения точнее назвать опосредованными отношениями с использования цифровых технологий и посредников в виде третьих лиц, возникающими в особой сфере — кибернетическом пространстве, в то время как общественные отношения в целом не ограничены использованием компьютерных сетей и могут возникать в разных областях общественной жизни, что

подтверждается некоторыми исследованиями. В этом мы отчасти разделяем позицию Д. В. Грибанова.[1]

Второй: правоотношения в цифровом пространстве требуют специальных подходов и учёта специфики цифровой среды, которая отчасти проявляется в субъектном составе: есть технические субъекты, отвечающие за работу интернета, индивидуальные пользователи, коллективные субъекты (государственные и негосударственные) и международные организации. Реализация прав и обязанностей не предполагает личное присутствие субъектов отношений, а осуществляется с помощью цифровых технологий.

Третий: субъекты и объекты правоотношений в киберпространстве существуют в своей парадигме, которая радикально отличается от традиционной правовой модели реального мира. Эта парадигма формируется под влиянием технологической природы цифровой среды и включает следующие ключевые особенности: гибридную природу субъектов правоотношений; дематериализацию объектов, они лишены физической формы и существуют как цифровые сущности; глобальность и трансграничность, нет географических границ; автономность и децентрализацию, технологии киберпространства часто действуют вне традиционных институтов; анонимность; автоматизацию и алгоритмизацию, все процессы в киберпространстве автоматизированы с помощью алгоритмов, что создает новые вызовы для правового регулирования и определения ответственности.

Четвертый: содержание правоотношений в киберпространстве отражает сущность воздействия права на общественные отношения в цифровой среде и показывает его эффективность.

[1] Грибанов Д. В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: автореф. дис. … канд. юрид. наук. – Екатеринбург, 2003. – 30 с.

2.5 Эффективность механизма правового регулирования отношений в киберпространстве

Эффективность это – обобщающая категория, показывающая в широком смысле соотношение между затраченными силами, ресурсами и достигнутыми результатами, раскрывающая, насколько качественно функционирует тот или иной институт или механизм, осуществляющий регулирующие функции в социальной среде. Определение эффективности механизма правового регулирования отношений в киберпространстве – достаточно сложное дело, нередко многогранный процесс, требующий системного подхода и учета множества факторов.

В научной среде понятие «эффективность» раскрывается в соответствии с предметом и задачами исследования, которые решаются в его рамках, поэтому ее толкование и характеристика представлена множеством вариантов. В данном случае нас интересует эффективность механизма правового регулирования в исследуемой в диссертации сфере.

Толкование эффективности в российской научной среде неоднозначно, например, С. А. Курочкин понимал эффективность правового механизма как соотношение между фактическим результатом действия правовых норм и теми социальными целями, для достижения которых эти нормы были приняты.[1]

Эффективность правового регулирования в понимании В. Н. Хропанюка выступает как соотношение между результатом правового регулирования и стоящей перед ним целью.[2]

Авторы статьи «Действие механизма правового регулирования в современной России» утверждали, что эффективность правового регулирования

---

[1] Курочкин С. А. Эффективность правовых норм как условие результативности правового воздействия (на примере норм процессуального права) // Ученые записки казанского университета. Серия гуманитарные науки. – 2020. – Т. 162, кн. 2. – С. 69–83.

[2] Хропанюк В. Н. Теория государства и права : учебник для высших учебных заведений. – М.: Омега-Л, 2012. – С. 339–341.

зависит от поведенческого аспекта и носит различный характер. С точки зрения поведения субъектов правового отношения можно говорить о юридической и социальной эффективности правового регулирования.[1]

Показатель эффективности В. С. Нерсесянц воспринимал как соотношение между последствиями реализации норм законодательства и правовыми целями этих норм.[2]

Автор диссертационной работы А. А. Абрамова охарактеризовала эффективность механизма правового регулирования как оценочную категорию, с помощью которой определяется уровень функциональности механизма правового регулирования в динамическом состоянии.[3]

С учетом позиций различных авторов в контексте нашего исследования предлагается рассматривать дефиницию эффективность механизма правового регулирования отношений в киберпространстве **как комплексный показатель достижения целей правового воздействия на общественные отношения в цифровой среде посредством системы взаимосвязанных правовых норм, институтов, процедур и инструментов, адаптированных к особенностям виртуальной реальности, с сохранением баланса между свободой и безопасностью, а также стимулированием развития инноваций и недопустимостью необоснованных ограничений.**

Иными словами, эффективность механизма правового регулирования отношений в киберпространстве проявляется в упорядочении общественных отношений в цифровой среде, в достижении поставленных правовых целей, направленных на защиту прав и интересов пользователей, обеспечение безопасности, стимулирование инноваций с оптимальными социальными, экономическими и технологическими результатами и возможными издержками.

---

[1] Абражеева Д. В., Музыкин А. А., Семёнов И. Г. Действие механизма правового регулирования в современной России // Молодой ученый. – 2017. – № 2 (136). – С. 298–300.

[2] Нерсесянц В. С. Общая теория права и государства : учебник для вузов. – М.: Норма : ИНФРА-М, 1999. – С. 258.

[3] Абрамова А. А. Эффективность механизма правового регулирования : дис. … .канд. юрид. наук. – Красноярск, 2006. – С. 206.

Данный показатель можно оценить посредством реализации следующих **критериев:**

1) достижения целей регулирования, т.е. насколько успешно решаются конкретные установки, например, снижается уровень киберпреступности, защищаются персональные данные, разрешаются трансграничные споры и иное;

2) возможности эффективного применения процедур и инструментов для решения поставленных юридических целей, а именно подбора и умелого использования имеющихся правовых средств и способов, влияющих на успех регулирования процесса;

3) способности механизма эволюционировать и адаптироваться к технологическим изменениям и новым вызовам киберпространства, т.е. по существу – готовность системы правового регулирования развиваться синхронно с изменениями, происходящими в цифровом пространстве, сохраняя свою актуальность и функциональность даже в условиях быстрых перемен;

4) гибкости в процессе решения определённых задач, например, учета и гармонизации интересов всех субъектов отношений государства, бизнеса, гражданского общества, а также баланса между регулированием и свободой инноваций, между безопасностью и приватностью;

5) ясности правовых предписаний для их адресатов, позволяющей предвидеть правовые последствия своих действий в сети;

6) возможности реализации действенных процедур и инструментов для принуждения к соблюдению норм, защите нарушенных прав и привлечения виновных к ответственности, включая трансграничный контекст;

7) легитимности механизма, основанного на признании его справедливым и обоснованным со стороны государства и пользовательского сообщества.

Таким образом, эффективность рассматриваемого механизма определяется не столько «принудительной», карательной мощью государства, сколько его способностью создавать гибкие, сбалансированные и признанные правила, которые реально влияют на поведение субъектов в сложной, полицентричной

системе, где закон является, хотя и весьма важным, но лишь одним из инструментов управления.

Разберём подробнее вышеобозначенные критерии, раскрывающие эффективность механизма правового регулирования отношений в киберпространстве. Для удобства выделим каждый из них по порядку и авторской логике.

Первый критерий выражен в формулировании целей правового регулирования, которые не отличаются от целей регулирования правоотношений в реальном мире, но при этом в техническом контексте их реализации имеет свою специфику. Главное – создать условия для стабильного и предсказуемого взаимодействия субъектов отношений в виртуальной среде, обеспечить защиту прав и законных интересов всех участников, минимизировать риски и негативные последствия неправомерных действий, а также стимулировать устойчивое развитие самой киберсреды взаимодействия.

В то же время специфика киберпространства требует адаптации традиционных правовых инструментов к новым условиям, учитывая её такие особенности, как анонимность, трансграничный характер операций и быстротечность процессов. Успешное регулирование возможно только с учётом баланса интересов, технологической нейтральности и адаптивности норм к быстро меняющимся технологическим особенностям виртуальной среды.

Точное формулирование правовых целей – необходимое условие для корректной оценки эффективности механизма правового регулирования в киберпространстве. Цели правового регулирования отношений в данном сегменте социального пространства – это, прежде всего, обеспечение правопорядка, предотвращение конфликтов, стимулирование инновационного развития, способствующего цифровой устойчивости государства при гарантированном соблюдении фундаментальных прав и свобод личности. Они должны отражать потребности общества, отвечать на вызовы времени и обеспечивать баланс между свободой, безопасностью и развитием.

Эффективность механизма правового регулирования в киберпространстве оценивается по достижению его общих и конкретных целей. Общие цели выражают фундаментальные ценности правовой системы, например, справедливость, законность, правопорядок, а конкретные цели связаны с регулированием отдельных видов общественных отношений в Интернете.

Цели механизма правового регулирования отношений в киберпространстве должны быть определёнными, измеримыми, достижимыми, релевантными и иметь временные рамки. Например, снижение числа киберпреступлений на 10% за год – конкретная, определённая и измеримая цель. Повышение безопасности в киберпространстве – слишком общая цель, не позволяющая оценить эффективность механизма, посредством которого она будет достигаться.

Второй критерий, отражающий возможности эффективного применения процедур и инструментов, целесообразно рассматривать через призму двух групп показателей. Первая группа включает юридические показатели, вторая – технологические.

Юридические показатели эффективности механизма правового регулирования в киберпространстве: отражают качество законодательства, регулирующего отношения в данном сегменте; раскрывают характеристики правовых норм и механизмов их реализации; показывают соответствие законодательства фундаментальным принципам права; выявляют степень защиты прав пользователей в киберпространстве; позволяют оценить эффективность работы правоохранительных органов, судов и других государственных институтов, осуществляющих контроль и регулирование отношений в виртуальном пространстве.

Юридические показатели эффективности законодательства оценивают его с точки зрения соответствия принципам права и способности регулировать общественные отношения в киберпространстве. При этом они: обеспечиваются государством – мерами властного и технологического воздействия; выражают юридические способы обеспечения интересов субъектов в киберпространстве; обладают специальной юридической природой, поскольку основаны на правовых

нормах и облечены в юридическую форму; приводят к юридически значимым последствиям, конкретным результатам, позволяющим решать обозначенную в виртуальном пространстве проблему.

Юридические показатели ориентированы на оценку формальной стороны правового регулирования, в частности: соответствия цифровых технологических разработок законодательству, регулирующему различные аспекты отношений в киберпространстве; эффективности обеспечения прав и свобод участников цифровых отношений посредством правовых механизмов; прозрачности и предсказуемости правового регулирования киберпространства; эффективности санкций и адекватности мер ответственности за правонарушения в киберпространстве.

Безусловно, названные показатели нельзя обеспечить без правоприменения, так как именно оно превращает формальные правовые нормы в динамику, в реально действующий инструмент. Законы должны исполняться, а их нарушения – раскрываться и наказываться. Это требует сотрудничества между правоохранительными органами, провайдерами интернет-услуг и другими заинтересованными участниками отношений в цифровой среде.

Целесообразно отметить несколько существенных моментов, определяющих значение правоприменения для увеличения степени эффективности механизма правового регулирования отношений в киберпространстве. Среди них, прежде всего, судебная правоприменительная практика, способствующая корректировке нормотворческих дефектов через толкование пробельных норм в процессе разрешения конкретных споров. Она инициирует внесение изменений в дефектные законодательные акты. Характерным примером можно считать дело Google Spain v. AEPD 2014 года, которое определило рамки «права на забвение» в Евросоюзе.[1]

Посредством правоприменительной практики формируется правовая определённость за счёт создания единых стандартов поведения всех участников

[1] Право быть забытым: Испания против Google // Lawtrend – Исследования Образование Действия. – 2014. – URL: https://www.lawtrend.org/information-access/blog-information-access/pravo-byt-zabytym-evropejskij-sud-demonstriruet-nekompetentnost (дата обращения: 01.02.2024).

отношений в киберпространстве. Иллюстрацией являются регуляторные разъяснения Центрального банка России о применении блокчейна в финансовой сфере.[1]

Правоприменение, как известно, играет ключевую роль в придании нормам практической силы, актуализирует и конкретизирует их. Подтверждением для рассматриваемой в диссертации сферы могут служить факты наложения штрафных санкций за несоблюдение сохранности персональных данных до 20 млн. евро или 4% от глобального оборота компании за предшествующий финансовый год **(**статья 83(5)(a) «Общего регламента по защите данных Евросоюза» (GDPR).[2]

Правоприменительная практика, используя властные рычаги воздействия, обеспечивает защиту прав пользователей. Примером, подтверждающим данный тезис, можно считать Решения Роскомнадзора по блокировке сайтов, нарушающих закон о персональных данных.[3]

Информация о результатах правоприменения в киберпространстве в немалой степени формирует доверие пользователей к цифровой среде**.** В качестве подтверждения можно отметить рост онлайн-платежей после введения ответственности за chargeback-мошенничество (25 июля 2024 года вступили в силу поправки, согласно которым в определенных случаях банк отправителя должен будет вернуть полную сумму украденных средств в течение 30 дней после получения заявления от клиента).[4]

Значение правоприменительной практики в рассматриваемом контексте очевидно. Она: а) обеспечивает исполнимость права, расследование

---

[1] Письмо Банка России «О комментариях АРБ по консультативному докладу Банка России о криптовалютах» № 05-35-2/1340 от 03 марта 2022 г. // ГАРАНТ.РУ : информационно-правовой портал. – 2022. – URL: https://www.garant.ru/products/ipo/prime/doc/403512706/(дата обращения: 01.02.2024).

[2] General Data Protection Regulation (GDPR). // RPPA. – 2024. – URL: https://rppa.pro/_media/world/gdpr.pdf (дата обращения: 02.02.2024).

[3] АН Москва: Роскомнадзор заблокировал 567 сайтов с незаконно размещенными персональными данными россиян // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций. – 2019. – URL: https://rkn.gov.ru/press/publications/news66668.htm (дата обращения: 01.02.2024).

[4] Федеральный закон «О внесении изменений в Федеральный закон «О национальной платежной системе» № 369-ФЗ от 24 июля 2023 г. / Российская газета. – 2023. – № 168.

киберпреступлений, наказание виновных, защиту прав пострадавших; б) помогает уточнить смысл и содержание правовых норм, адаптировать их к конкретным ситуациям; в) выявляет недостатки и пробелы в законодательстве, которые не всегда очевидны на стадии его разработки; г) действует как сдерживающий фактор для потенциальных правонарушителей, обеспечивая превентивную функцию законодательства; д) позволяет адаптировать право к технологическим изменениям, разрабатывая новые подходы к расследованию киберпреступлений, защите данных и другое; е) способствует формированию доверия к государству, обеспечивающему защиту прав пользователей, стимулирует их активность в киберпространстве.

Технологические показатели эффективности правового регулирования отношений в киберпространстве, в отличие от юридических, раскрывают практическую результативность применения технических средств и решений для достижения целей, поставленных правовыми нормами. Они свидетельствуют, насколько успешно технологии используются для реализации и обеспечения соблюдения законов в цифровой среде, фокусируются на оценке практической применимости правовых норм в условиях цифровой среды и включают следующие аспекты: характеристику цифровых технологий в парадигме правовых регуляторов; скорость реагирования на изменения (как быстро законодательная система способна реагировать на технологические инновации и угрозы); доступность технологий для исполнения законов (наличие инструментов и механизмов для мониторинга соблюдения нормативных актов в цифровом пространстве); безопасность данных (уровень защиты персональных данных и конфиденциальной информации в рамках цифрового взаимодействия); согласованность технических стандартов (соответствие национальных стандартов международным нормам и требованиям кибербезопасности); инновационность решений (способность правовых норм стимулировать развитие новых технологических решений для повышения безопасности и прозрачности в киберпространстве).

В качестве примера приведём сравнительную таблицу отличий технологических показателей от юридических.

Таблица 1 – Сравнительная таблица отличий технологических показателей от юридических

Критерий	Технологические показатели	Юридические показатели
Цель	Обеспечить техническую реализацию требований права.	Установить и обеспечить соблюдение правовых норм.
Фокус оценки	Оценивают фактическое состояние отношений в киберпространстве и эффективность использования технологий для реализации правовых норм.	Оценивают качество самого законодательства и наличие механизмов его реализации.
Объект оценки	Технические системы, алгоритмы, инфраструктура, программное обеспечение.	Правовые нормы, судебные решения, действия регуляторов.
Объект измерения	Измеряют технические параметры и статистические данные, связанные с кибербезопасностью, защитой данных, развитием инфраструктуры и другие.	Анализируют правовые нормы, судебную практику, деятельность правоохранительных органов.
Методы оценки	Используют технические средства и статистические методы для сбора и анализа данных.	Применяют юридический анализ, сравнительно-правовой метод, анализ судебной практики и иные.
Характер выводов	Делают выводы о фактическом уровне безопасности, защиты данных, развития инфраструктуры в киберпространстве.	Делают выводы о соответствии законодательства требованиям правовой техники, международным стандартам, принципам права.

Из приведённых сравнений можно выделить особенности, заключающиеся в том, что юридические показатели раскрывают, какие законы, регулирующие отношения в киберпространстве, приняты, а технологические – как эти законы работают на практике и каков реальный эффект от их применения с точки зрения технологий. Юридические показатели выявляют, когда не соблюдаются нормы и какие санкции следуют за их нарушение, в то время как технологические

показатели демонстрируют, как технически обеспечено выполнение правовых норм.

Очевидно, что юридические показатели эффективности механизма правового регулирования отношений в киберпространстве раскрывают степень соблюдения права в виртуальной среде, а технологические показатели иллюстрируют качество технического инструментария, посредством которого реализованы правовые требования. При этом для комплексной оценки эффективности механизма правового регулирования отношений в киберпространстве необходимо анализировать как юридические, так и технологические показатели в их взаимосвязи.

Существуют и противоречия между юридическими и технологическими показателями. Иногда юридические требования могут отставать от технологических возможностей, например, в регулировании разработок систем искусственного интеллекта или решения проблем, связанных с правовым статусом роботизированных систем. Чрезмерное правовое «зарегулирование» может тормозить внедрение новых технологий и сдерживать развитие цифровой экономики.

Третий критерий выражает способность механизма эволюционировать и адаптироваться к технологическим изменениям и новым вызовам киберпространства. Адаптивность – это способность правовой системы не просто реагировать на уже свершившиеся технологические изменения, а активно создавать актуальные правовые рамки, остающиеся релевантными и действенными в условиях непрерывной технологической эволюции.

Это позволяет правовым нормам регулировать отношения, возникающие на базе технологий, которые еще даже не созданы. Если в реальном мире правоотношения меняются медленно, десятилетиями, то в киберпространстве действует так называемая «проблема темпов», когда технологии развиваются экспоненциально. Закон, написанный сегодня для регулирования социальных сетей, может оказаться совершенно бесполезным завтра для регулирования децентрализованных метавселенных или нейроинтерфейсов.

Способность к эволюции и адаптации выражается не в одном, а в целом комплексе подходов к правотворчеству и правоприменению, среди которых можно выделить: а) технологическую нейтральность, закон должен регулировать не конкретную технологию, а суть отношений или функцию, которую эта технология выполняет; б) принципиальное регулирование вместо предписывающего, поскольку принципиальное регулирование формирует общий вектор развития права и общества, тогда как предписывающее регулирование прямо регулирует конкретные случаи и модели поведения. Принципиальное регулирование носит декларативный характер, в то время как предписывающее направлено на прямое регулирование повседневной деятельности; в) внедрение механизмов «гибкого» или «умного» регулирования, позволяющего праву учиться и эволюционировать вместе с технологией; г) многосторонний (мультистейкхолдерный) подход к разработке норм, когда процесс разработки правовых норм включает постоянные консультации и совместную работу с представителями IT-бизнеса, инженерами, научным сообществом и институтами гражданского общества.

Таким образом, критерий адаптивности – это не просто пожелание, а необходимое условие выживания и эффективности правовой системы в цифровую эпоху. Он выражается в способности законодателя мыслить принципами, а не только предписаниями; использовать гибкие инструменты «мягкого права» и экспериментальные режимы; выстраивать постоянный диалог с создателями технологий. Право, обладающее таким эволюционным потенциалом, перестает быть тормозом прогресса и становится его навигатором, обеспечивая баланс между инновациями, безопасностью и защитой прав человека в постоянно меняющемся цифровом мире.

Четвёртый критерий раскрывает эффективность механизма правового регулирования отношений в киберпространстве за счёт гибкости правовых предписаний и механизма регулирования в процессе решения определённых задач. Гибкость реализуется: а) посредством технологической нейтральности права, т.е. закон должен регулировать сущность отношений и конечный результат, а не конкретную технологию, использованную для их реализации; б) путём применения

«мягкого права», когда законодатель устанавливает рамочные принципы и цели, а детализированные технические нормы разрабатывают и оперативно обновляют специализированные органы (например, регуляторы, как Банк России в сфере финтеха) или профессиональные сообщества; в) в процессе использования экспериментальных правовых режимов «регулятивных песочниц» – за счёт создания на ограниченное время и для ограниченного круга участников специального юридического пространства, где могут тестироваться новые бизнес-модели и технологии без применения к ним жёстких норм действующего законодательства; г) через интеграцию механизмов обновления, когда правовой акт изначально содержит в себе процедуры своего возможного изменения и адаптации.

Пятый критерий отражает эффективность названного механизма через ясность правовых предписаний, что выражается в возможности права создавать предсказуемую, стабильную и справедливую среду для всех участников. Ясность достигается за счет лаконичных и понятных юридических формулировок, исключающих двусмысленность и разночтения. Чем меньше неопределенность в трактовке норм, тем проще их соблюдать и применять на практике.

Шестой критерий эффективности раскрывает возможность комплексного применения процедур и инструментов для принуждения к соблюдению норм. Принуждение – это гарантия реализации норм и неотвратимости ответственности за их нарушение, что достигается посредством правоохранительной деятельности, в частности, действий специализированных подразделений полиции и спецслужб, занимающихся расследованием и пресечением киберпреступлений; судебной практики, устанавливающей прецеденты и придающей дополнительную силу существующим регуляторам; технологическим средствам, таким как системы слежения, шифрования, антивирусные программы и сетевое оборудование, предоставляющее возможность отслеживать нарушения и обеспечивать соблюдение норм.

Седьмой критерий эффективности правового регулирования отношений непосредственно связан с легитимностью механизма правового регулирования, основанного на признании его законным (соответствующим Конституции РФ и

т.д.), справедливым и обоснованным, прежде всего со стороны государства, а также участников виртуальных отношений. Легитимность указывает на справедливость и правомерность существующих норм и полномочий регулятора. Эта связь прослеживается через несколько ключевых механизмов, которые показывают, почему нелегитимное регулирование не может быть эффективным в долгосрочной перспективе. Высокая легитимность облегчает процесс реализации норм и способствует увеличению их эффективности.

Резюмируя вышесказанное, можно сделать несколько обобщений.

1. Эффективность механизма правового регулирования отношений в киберпространстве можно оценивать при условии достижения постановленных целей правового воздействия посредством системы взаимосвязанных правовых норм в рамках установленных показателей, соответствующих критериям оценки.

2. Цель правового регулирования является основой для разработки регуляторной стратегии. Она должна быть конкретной, измеримой, позволяющей оценить степень её достижения в киберпространстве.

3. Исходя из особенностей виртуальной среды, где взаимодействуют право и технологии, целесообразно исследовать две группы показателей эффективности действия правового механизма – юридические и технологические. Юридические показатели эффективности законодательства оценивают его с точки зрения соответствия принципам права и способности продуктивно регулировать общественные отношения в киберпространстве. Технологические показатели раскрывают практическую результативность применения технических средств и решений для достижения целей, поставленных правовыми нормами.

4. Критерии оценки эффективности законодательства, регулирующего правоотношения в киберсреде, отражают то, насколько были достигнуты поставленные цели и выполнены показатели правового регулирования виртуальных отношений. Они включают такие параметры, как своевременность реагирования на инциденты, эффективность применения законодательных мер, уровень удовлетворенности пользователей и другие факторы. Критерии могут варьироваться в зависимости от специфики регулируемых отношений.

ЗАКЛЮЧЕНИЕ

Проведенный комплексный теоретико-правовой анализ системы полинормативного регулирования отношений в киберпространстве позволяет сформулировать ряд основополагающих выводов, имеющих значение для развития общей теории права и совершенствования правоприменительной практики в условиях цифровой трансформации.

Исследование подтвердило центральный тезис о том, что упорядочение общественных отношений в киберпространстве невозможно в рамках традиционной государственно-центричной парадигмы, основанной на монополии права. Его специфика характеризуется трансграничностью, децентрализованностью, технологической опосредованностью и высокой динамикой трансформаций, что предопределяет уникальную систему полинормативной регламентации отношений, в которой право устанавливает рамки, а неправовые регуляторы, такие как архитектура («код»), рыночные механизмы, социальные нормы и иные, получают легитимированное пространство для автономного функционирования, образуя тем самым сложную систему взаимодополняющих нормативных порядков. В этой системе право выполняет метарегулятивную функцию, определяя фундаментальные принципы и целевые ориентиры для всех участников отношений, в то время как технические стандарты обеспечивают непосредственное исполнение правил через архитектурные решения, рыночные механизмы создают экономические стимулы для желаемого поведения, а социальные нормы формируют неформальные, но эффективные модели взаимодействия внутри цифровых сообществ. Ключевым вызовом при реализации данной модели становится обеспечение согласованности действий разнородных регуляторов и предотвращение нормативных конфликтов, что требует создания гибких институтов для координации между государством, технологическими компаниями, гражданским обществом и экспертным сообществом.

Эволюция правовой мысли, подробно рассмотренная в работе, демонстрирует закономерный переход от попыток механической экстраполяции классических юридических конструкций к признанию необходимости формирования новой системы полинормативного упорядочения отношений в киберпространстве. Эта концепция основана на диалектическом взаимодействии всех типов регуляторов, обеспечивает подотчетность иных неправовых механизмов и формирует сбалансированные гибридные модели.

Важным результатом исследования стало выявление социально-правовой природы киберпространства как гибридной среды, порождающей отношения, существующие на стыке виртуальной и физической реальностей. Эта гибридность является источником фундаментальной правовой неопределенности статуса ключевых феноменов цифровой эпохи, таких как цифровая идентичность, системы искусственного интеллекта, смарт-контракты, виртуальная собственность. Преодоление этой неопределенности требует не фрагментарной адаптации норм, а разработки новой доктринальной основы, переосмысливающей базовые юридические категории субъектность, объектность, ответственность, юрисдикцию, цифровой суверенитет. В работе предложены пути решения этой проблемы через внедрение принципа технологической нейтральности, легитимацию «мягкого права» и создание новых правовых институтов, таких как «цифровое доверенное лицо».

Значительное внимание в диссертации уделено проблеме границ правового регулирования, которая является следствием фундаментального противоречия между экстерриториальной природой киберпространства и территориальным характером государственного суверенитета. Анализ современных государственных практик (Россия, Китай, США, страны ЕС) позволил идентифицировать три конкурирующие модели: суверенно-центричную, глобалистскую и компромиссную. Для преодоления терминологической и сущностной путаницы, связанной с понятиями «цифровой суверенитет» и «киберсуверенитет», в научный оборот введена и обоснована авторская дефиниция «цифровой государственный киберсуверенитет». Данный концепт комплексно

объединяет технический контроль над инфраструктурой и социально-правовое регулирование отношений, что позволяет адекватно описывать современную политику государства в цифровой сфере. Решение проблемы юрисдикции видится в гибридном подходе, сочетающем адаптацию международно-правовых принципов с гибкими договорными и технологическими механизмами.

Центральным элементом исследования стал анализ механизма правового регулирования (МПР) отношений в киберпространстве. Показано, что это не простая проекция классического МПР, а динамичная система, эффективность которой обусловлена глубокой трансформацией его структурных элементов. Норма права, сохраняя свою сущность, сталкивается с вызовами коллизий юрисдикций, скоротечности технологических изменений и проблемами толкования в цифровом контексте. Юридические факты приобретают цифровую природу, характеризуются сложностью фиксации, доказывания и атрибуции, а также возможностью генерации системами искусственного интеллекта, что требует адаптации процедур доказывания и разработки новых институтов. Правоотношения в киберпространстве отличаются уникальной структурой, связанной с технологическими посредниками (платформами, алгоритмами, смарт-контрактами), и усложненным субъектным составом.

Ключевым критерием эффективности МПР в киберпространстве является его адаптивность способность эволюционировать синхронно с технологическими изменениями. В диссертации разработана и обоснована авторская система оценки эффективности, основанная на синтезе двух взаимодополняющих групп критериев: юридических (обеспечивающих формальное качество, легитимность и исполнимость норм) и технологических (определяющих практическую реализуемость и результативность правовых предписаний с помощью технических средств). Такой подход позволяет проводить комплексную и объективную оценку, выходя за рамки традиционной формулы «цель-результат».

Теоретическая значимость работы заключается в разработке целостной системы полинормативного регулирования отношений в киберпространстве, которая вносит вклад в развитие теории правового плюрализма и стимулирует

междисциплинарные исследования на стыке юриспруденции, социологии и компьютерных наук. Практическая значимость состоит в том, что выводы и рекомендации могут быть использованы в законотворческой деятельности для разработки адекватных правовых моделей, в правоприменительной практике для квалификации деяний и оценки доказательств, а также в образовательном процессе для подготовки новых поколений юристов, способных работать в условиях цифровой реальности.

Таким образом, диссертационное исследование демонстрирует, что будущее эффективного регулирования отношений в киберпространстве связано не с попытками установления монополии права, а с формированием сбалансированной, гибкой и легитимной системы полинормативного регулирования. В такой системе право гармонизирует действие технологических, рыночных и социальных механизмов, обеспечивая баланс между безопасностью, защитой прав пользователей и свободой инновационного развития. Дальнейшие научные изыскания целесообразно направить на детализацию моделей гибридного регулирования, разработку международно-правовых стандартов для технологий искусственного интеллекта и блокчейна, а также на изучение влияния цифровизации на правосознание.

В работе впервые введены в научный оборот и актуализированы следующие понятия:

виртуальная личность – цифровой образ, создаваемый пользователем в киберпространстве, который может обладать признаками анонимности, фиктивности и не совпадать с идентичностью физического лица-носителя. Виртуальная личность не является самостоятельным субъектом правоотношений. Она представляет собой инструмент или цифровой образ физического лица, которое несет ответственность за ее действия;

киберпространство – среда, созданная при помощи программно-аппаратных комплексов с возможностью формирования симулякров, установления коммуникаций, осуществления различных видов виртуальной деятельности, включая образование, торговлю, управление и иную, позволяющую виртуальные

отношения переводить в плоскость правоотношений в рамках одной или нескольких юрисдикций;

кибервойна – составной компонент гибридной войны, задача которой – достичь определенных целей в экономической, политической, военной и других областях посредством воздействия на общество и власть;

кибер-правоотношения представляют урегулированную нормами права форму взаимодействия субъектов в киберпространстве, которые наделены взаимными субъективными правами и юридическими обязанностями, возникающими в процессе использования киберпространства и обеспеченными возможностью применения мер государственного принуждения;

критерии эффективности механизма правового регулирования отношений в киберпространстве: а) достижения целей регулирования; б) возможности эффективного применения процедур и инструментов для решения поставленных юридических целей; в) способности механизма эволюционировать и адаптироваться к технологическим изменениям и новым вызовам виртуальной среды; г) гибкости в процессе решения определённых задач; г) ясности правовых предписаний; д) возможности реализации действенных процедур и инструментов для принуждения к соблюдению норм; д) легитимности механизма, основанного на признании его справедливым и обоснованным со стороны государства и пользовательского сообщества;

мягкое право – правовой феномен, отражающий переход от иерархических норм к сетевым стандартам, не имеет обязательной юридической силы, действует через убеждение, репутацию и косвенное давление, оставаясь важным инструментом в условиях неопределённости и быстрых технологических изменений;

механизм правового регулирования отношений в киберпространстве – это сложная структура, объединяющая правовые нормы, методы и процедуры, направленные на упорядочение и защиту цифровых отношений, посредством которых формируется сбалансированная система, обеспечивающая законность, защиту прав пользователей, безопасность и инновации в цифровом пространстве;

отношения в киберпространстве охватывают все виды общественных отношений, возникающих и реализуемых в цифровой среде. Сюда входят как отношения, регулируемые правом, так и отношения, находящиеся вне сферы правового регулирования, такие как: общение в социальных сетях; онлайн-игры; просмотр видео и иное. Они могут регламентироваться собственниками платформ, внутренним кодексом социальных сетей, алгоритмами, другими способами, установленными администраторами;

цифровой государственный киберсуверенитет – юридически обусловленная способность государства проецировать свою власть в цифровую среду для регулирования общественных отношений, возникающих в рамках установленной юрисдикции, с целью защиты прав и законных интересов пользователей (участников отношений). Он раскрывает возможность государства формировать и поддерживать правовую экосистему, которая динамично адаптируется к трансграничной природе цифровой среды, обеспечивая баланс интересов, позволяет автономно регулировать деятельность в цифровом пространстве, отстаивать национальные интересы, обеспечивать безопасность информационных ресурсов и свободу коммуникации, исключая внешнее вмешательство и угрозы цифрового характера;

эффективность механизма правового регулирования отношений в киберпространстве – комплексный показатель достижения целей правового воздействия на общественные отношения в цифровой среде посредством системы взаимосвязанных правовых норм, институтов, процедур и инструментов, адаптированных к особенностям виртуальной реальности, с сохранением баланса между свободой и безопасностью, а также стимулированием развития инноваций и недопустимостью необоснованных ограничений;

юридические факты в киберпространстве – это конкретные действия и/или события, происходящие в цифровой среде, которые в силу правовых норм влекут возникновение, изменение или прекращение правоотношений и порождают соответствующие правовые последствия. Их природа может быть чисто виртуальной (отправка электронного сообщения) либо представлять собой

действия в физическом мире, имеющие последствия в цифровой среде (поломка сервера);

юридическая квалификация в киберпространстве – процесс определения, к какой категории правовых норм и юрисдикций относится конкретное событие или действие, совершённое в виртуальной среде.

Перечисленные понятия позволяют фокусировать внимание на сущности правовых и неправовых регуляторов отношений в киберпространстве, раскрывают их содержательную составляющую, что обеспечивает системное понимание их функционального назначения, областей компетенции и механизмов взаимовлияния, создавая теоретический фундамент для построения сбалансированной системы полинормативного регулирования, в которой достигается баланс между государственным принуждением, архитектурными ограничениями, экономическими стимулами и социальным одобрением.

СПИСОК ЛИТЕРАТУРЫ

1. Международно-правовые акты и документы:

1. An international code of conduct for information security. – Текст : электронный // Национальная Ассоциация международной информационной безопасности НАМИБ : [сайт]. – 2024. – URL: https://namib.online/wp-content/uploads/2020/04/International-code-of-conduct-for-information-security-on-9-January-2015.pdf (дата обращения: 04.09.2024).

2. Декларация прав и обязанностей государств от 6 декабря 1949 г. (принята Комиссией международного права ООН, резолюция 375 (IV) от 6 дек. 1949 г.). – Текст : электронный // ГАРАНТ.РУ : информационно-правовой портал. – Москва : НПП «Гарант-Сервис-Университет», 2023. – URL: https://base.garant.ru/2561237/741609f9002bd54a24e5c49cb5af953b/ (дата обращения: 12.07.2023).

3. Декларация принципов Построение информационного общества – глобальная задача в новом тысячелетии : принята 18.12.2003. Документ WSIS03/GENEVA/DOC/4-R. – Текст : электронный // Организация объединенных наций https://www.un.org/ru/ : [сайт]. – 2024. – URL: https://www.un.org/ru/events/pastevents/pdf/dec_wsis.pdf (дата обращения:10.12.2024).

4. Окинавская хартия глобального информационного общества: принята на о. Окинава 22.07.2000 г. // Дипломатический вестник. 2000. – №8. – С. 51-56. – Текст : непосредственный.

5. Тунисская Программа для информационного общества: принята 15.11.2005 г. Документ WSIS-05/TUNIS/DOC/6(Rev.1)-R. – Текст : электронный // Организация объединенных наций https://www.un.org/ru/ : [сайт]. – 2024. – URL: https://www.un.org/ru/events/pastevents/pdf/agenda_wsis.pdf (дата обращения: 10.12.2024).

6. Cybersecurity Law of the People's Republic of China. – Текст : электронный // «OneTrust» : [сайт]. – 2024. – URL: https://www.dataguidance.com/sites/default/files/en_cybersecurity_law_of_the_peoples_republic_of_china_1.pdf (дата обращения: 04.02.2024).

7. Руководящие принципы предпринимательской деятельности в аспекте прав человека: осуществление рамок Организации Объединенных Наций, касающихся «защиты, соблюдения и средств правовой защиты». – Текст : электронный / Организация Объединенных Наций : [сайт]. – 2011. – 39 с. – URL: https://documents.un.org/doc/undoc/gen/g11/121/92/pdf/g1112192.pdf (дата обращения: 16.05.2024).

8. Digital Personal Data Protection Act, 2023. – Текст : электронный // https://www.meity.gov.in/ : [сайт]. – 2023. – URL: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (дата обращения: 23.12.2024).

9. Directive (eu) 2019/790 of the European parliament and of the Council of 17 april 2019 on copyright and related rights in the digital single market and amending Directives 96/9/ec and 2001/29/EC. – Текст : электронный // Всемирная организация интеллектуальной собственности : [сайт]. – 2019. – URL: https://www.wipo.int/wipolex/ru/legislation/details/18927 (дата обращения: 02.02.2024).

10. The California Consumer Privacy Act : CCPA. – Текст : электронный // theccpa.org : [сайт]. –2018. – URL: theccpa.org (дата обращения: 06.05.2024).

11. Uniform Electronic Transactions Act (UETA) : Final Act with Prefatory Note and Comments. – Текст : электронный / National Conference of Commissioners on Uniform State Laws. – Chicago, IL : NCCUSL, 1999. – https://www.approveme.com : [сайт]. – 1999. – URL: https://www.approveme.com/wp-content/uploads/2021/10/UETA_Final-Act_1999.pdf (дата обращения: 12.05.2024).

12. Electronic Signature Law of the People's Republic of China. – Текст : электронный // Всемирная организация интеллектуальной собственности : [сайт]. –

2024. – URL: https://www.wipo.int/wipolex/en/legislation/details/6559 (дата обращения: 04.02.2024).

13. Personal Information Protection Law of the People's Republic of China. – Текст : электронный // Всекитайское собрание народных представителей : [сайт]. – 2024. – URL: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (дата обращения: 04.02.2024).

14. Electronic Signatures in Global and National Commerce Act : GovInfo. – Текст : электронный // https://www.govinfo.gov/ : [сайт]. – 2000. – URL: https://www.govinfo.gov/content/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf (дата обращения: 12.05.2024).

15. General Personal Data Protection Act (LGPD) Lei Nº 13.709/2018. – Текст : электронный // https://www.gov.br/pt-br : [сайт]. – 2018. – URL: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/outros-documentos-e-publicacoes-institucionais/lgpd-en-lei-no-13-709-capa.pdf (дата размещения: 26.12.2024).

16. Information Technology Act, 2000. – Текст : электронный // India Code : [сайт]. – 2000. – URL: https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (дата обращения: 26.12.2024).

17. Marco Civil da Internet, Lei Nº12.965/2014. – Текст : электронный // Câmara dos Deputados : [сайт]. – 2014. – URL: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1238705&filename=Tramitacao-PL+2126/2011 (дата обращения: 26.12.2024).

18. India. Ministry of Communications and Information Technology. National Cybersecurity Policy. – Тескт : электронный / Ministry of Communications and Information Technology, Government of India. – [Delhi] : Government of India, 2013. – https://www.itu.int/en : [сайт]. – 2013. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/India_2013_National_cyber_security_policy-2013(1).pdf (дата обращения: 23.12.2024).

19. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. – Текст : электронный / Ministry of Electronics & Information Technology, Government of India. – New Delhi : MeitY, 2021. – URL:

https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf (дата обращения: 23.12.2024).

20. The Online Safety Bill. – Текст : электронный // https://www.gov.uk/ : [сайт]. – 2022. – URL: https://assets.publishing.service.gov.uk/media/6231dc9be90e070ed8233a60/Online_Safety_Bill_impact_assessment.pdf (дата обращения: 21.12.2024).

21. The Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943). – Текст : электронный // https://www.thesedonaconference.org/ : [сайт]. – 2018. – URL: https://thesedonaconference.org/sites/default/files/%5B5.2%5D%20CLOUD%20Act.pdf (дата обращения: 02.12.2024).

22. The Stored Communications Act of 1986. – Текст : электронный // https://bja.ojp.gov/ : [сайт]. – 1986. – URL: https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285 (дата обращения: 02.12.2024).

23. Delaware General Corporation Law (Dgcl). – Текст : электронный // https://delcode.delaware.gov : [сайт]. – 2013. – URL: https://delcode.delaware.gov/title8/c001/ (дата обращения: 12.05.2024).

24. CLOUD Act. – Текст : электронный // Link11 : [сайт]. – 2024. – URL: https://www.link11.com/en/glossar/cloud-act/ (дата обращения: 26.12.2024).

25. Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных от 28 января 1981 года // Сборник документов Совета Европы в области защиты прав человека и борьбы с преступностью. – М.: СПАРК, 1998. – С. 106–114. – Текст : непосредственный.

26. Резолюция, принятая Генеральной Ассамблеей ООН 22 декабря 2018 года (по докладу Первого комитета (A/73/505) № 73/266 «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности». – Текст : электронный // Организация объединенных наций : [сайт]. – 2018. – URL: https://documents.un.org/doc/undoc/gen/n18/465/04/pdf/n1846504.pdf (дата обращения: 06.04.2024).

27. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). – Текст : электронный // ГАРАНТ.РУ : информационно-правовой портал : [сайт]. – 2001. – URL: https://base.garant.ru/4089723/ (дата обращения: 21.12.2024).

2. Нормативные правовые акты Российской Федерации

28. **Российская Федерация. Законы.** Конституция Российской Федерации [принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020]. – Текст электронный // Официальный интернет-портал правовой информации. (www.pravo.gov.ru) : [сайт]. – 2024. – URL: http://publication.pravo.gov.ru/document /00012022 10060013 (дата обращения: 03.08.2025).

29. **Российская Федерация. Законы.** Гражданский кодекс Российской Федерации (часть первая): ГК РФ : текст с изменениями и дополнениями на 11.03.2024 : [принят Государственной думой 21 октября 1994 года] // Российская газета. – 08.12.1994 г. – № 238–239. – Текст : непосредственный.

30. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации: УК РФ: текст с изменениями и дополнениями на 01.04.2024: [принят Государственной думой 24 мая 1996 года: одобрен Советом Федерации 5 июня 1996 года] // Собрание законодательства РФ. – 17.06.1996 г. – № 25. – Ст. 2954. – Текст: непосредственный.

31. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ от 27.07.2006 : текст с изменениями и дополнениями на 24.06.2025 г. [принят Государственной Думой Федерального Собрания Российской Федерации 08 июля 2006 года : одобрен Советом Федерации Федерального Собрания Российской Федерации 14 июля 2006 года] // Российская газета. – 29.07.2006 г. – № 165. – Текст : непосредственный.

32. **Российская Федерация. Законы.** Об электронной подписи : Федеральный закон № 63-ФЗ от 06.04.2011 г. : текст с изменениями и дополнениями на 28.12.2024 г. : [принят Государственной Думой Федерального Собрания Российской Федерации 25 марта 2011 года: одобрен Советом Федерации Федерального Собрания Российской Федерации 30 марта 2011 года] // Российская газета. – 08.04.2011 г. – № 75. – Текст : непосредственный.

33. **Российская Федерация. Законы.** О персональных данных : Федеральный закон № 152-ФЗ от 27.07.2006 г. : текст с изменениями и дополнениями на 28.12.2024 г. : [принят Государственной Думой Федерального Собрания Российской Федерации 08 июля 2006 года: одобрен Советом Федерации Федерального Собрания Российской Федерации 14 июля 2006 года] // Российская газета. – 29.07.2006 г. – № 165. – Текст : непосредственный.

34. **Российская Федерация. Законы.** О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» : Федеральный закон № 90-ФЗ от 01 мая 2019 г. // Российская газета. – 07.05.2019 г. – № 97. – Текст : непосредственный.

35. **Российская Федерация. Законы.** О деятельности иностранных лиц в информационно-телекоммуникационной сети «Интернет» на территории Российской Федерации : Федеральный закон № 236-ФЗ от 01.07.2021 г. : текст с изменениями и дополнениями на 22.06.2024 г. : [принят Государственной Думой Федерального Собрания Российской Федерации 17 июня 2021 года: одобрен Советом Федерации Федерального Собрания Российской Федерации 23 июня 2021 года] // Собрание законодательства Российской Федерации. – 2021. – № 27. – ст. 5064. – Текст : непосредственный.

36. **Российская Федерация. Законы.** О внесении изменений в Федеральный закон «О национальной платежной системе» Федеральный закон № 369-ФЗ от 24 июля 2023 г. : [принят Государственной Думой Федерального Собрания Российской Федерации 11 июля 2023 года: одобрен Советом Федерации

Федерального Собрания Российской Федерации 19 июля 2023 года] // Российская газета. – 2023. – № 168. – Текст: непосредственный.

37. **Российская Федерация. Законы.** О персональных данных : Федеральный закон № 152-ФЗ от 27.07.2006 г. : текст с изменениями и дополнениями на 08.08.2024 г. : [принят Государственной Думой Федерального Собрания Российской Федерации 08 июля 2006 года: одобрен Советом Федерации Федерального Собрания Российской Федерации 14 июля 2006 года] // Собрание законодательства Российской Федерации. – 2006. – № 31 (1 ч.). – Текст : непосредственный.

38. **Российская Федерация. Подзаконные акты.** Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации № 646 от 05.12.2016 г. // Собрание законодательства Российской Федерации. – 2016. – № 50. – Текст: непосредственный.

39. **Российская Федерация. Подзаконные акты.** О развитии искусственного интеллекта в Российской Федерации : Указ Президента Российской Федерации № 490 от 10.10.2019 г. // Собрание законодательства Российской Федерации. – 2019. – № 41. – Текст: непосредственный.

40. **Российская Федерация. Подзаконные акты.** О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента РФ № 203 от 09.05.2017 г. // Собрание законодательства РФ, 15.05.2017 г. – № 20. – ст. 2901. – Текст: непосредственный.

3. Регламенты, правила, письма

41. Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности». – Текст : электронный // Министерство иностранных дел Российской Федерации : [сайт]. – 2024. – URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1582268/ (дата обращения: 04.09.2024).

42. Общий регламент защиты персональных данных (GDPR) Европейского союза. – Текст : электронный // GDPR-Text.com : [сайт]. – 2018. – URL: https://gdpr-text.com/ru/ (дата обращения: 06.05.2024).

43. General Data Protection Regulation (GDPR). – Текст : электронный // RPPA : [сайт]. – 2024. – URL: https://rppa.pro/_media/world/gdpr.pdf (дата обращения: 02.02.2024).

44. О комментариях АРБ по консультативному докладу Банка России о криптовалютах : Письмо Банка России № 05-35-2/1340 от 03 марта 2022 г. – Текст : электронный // ГАРАНТ.РУ : информационно-правовой портал : [сайт]. – 2022. – URL: https://www.garant.ru/products/ipo/prime/doc/403512706 (дата обращения: 01.02.2024).

4. Диссертации и авторефераты диссертаций

45. **Абрамова, А. А.** Эффективность механизма правового регулирования : дис. … канд. юрид. наук. – Красноярск, 2006. – 206 с. – Текст : непосредственный.

46. **Авдеев, Д. А.** Правовое регулирование отношений, связанных с цифровизацией частной жизни : дис. ... канд. юрид. наук. – Владимир, 2024. – 203 с. – Текст : непосредственный.

47. **Азизов, Р. Ф.** Правовое регулирование в сети Интернет: сравнительно- и историко-правовое исследование : дис. ... канд. юрид. наук. – Санкт-Петербург, 2017. – 331 с. – Текст : непосредственный.

48. **Анисимова, А. С.** Механизм правового регулирования интернет-отношений: проблемы теории и практики : дис. ... канд. юрид. наук. – Саратов, 2019. – 222 с. – Текст : непосредственный.

49. **Бодров, А. А.** Виртуальная реальность как когнитивный и социокультурный феномен : автореф. дис. … д-ра философ. наук. – Самара, 2007. – 34 с. – Текст : непосредственный.

50. **Бондаренко, Т. А.** Виртуальная реальность в современной социальной ситуации : автореф. дис. … д-ра философ. наук. – Ростов-на-Дону, 2007. – 53 с. – Текст : непосредственный.

51. **Вавилова, Ж. Е.** Конструирование идентичности в условиях виртуализации общества : автореф. дис. … канд. философ. наук. – Казань, 2019. – 24 с. – Текст : непосредственный.

52. **Вылков, Р. И.** Киберпространство как социокультурный феномен, продукт технологического творчества и проектная идея : автореф. дис. … канд. философ. наук. – Екатеринбург, 2009. – 24 с. – Текст : непосредственный.

53. **Гасанов, А. Я.** Гражданско-правовое регулирование оказания услуг с использованием цифровых технологий : автореф. дис. ... канд. юрид. наук. – Москва, 2022. – 25 с. – Текст : непосредственный.

54. **Геллер, А. В.** Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета : автореф. дис. ... канд. юрид. наук. – Москва, 2006. – 24 с. – Текст : непосредственный.

55. **Голоскоков, Л. В.** Модернизация российского права: теоретико-информационный аспект : дис. ... д-ра. юрид. наук. Краснодар, 2006. – 423 с. – Текст : непосредственный.

56. **Горшкова, Л. В.** Правовые проблемы регулирования частноправовых отношений международного характера в сети Интернет : автореф. дис. ... канд. юрид. наук. – Москва, 2005. – 30 с. – Текст : непосредственный.

57. **Грибанов, Д. В.** Правовое регулирование кибернетического пространства как совокупности информационных отношений : дис. ... канд. юрид. наук. – Екатеринбург, 2003. – 227 с. – Текст : непосредственный.

58. **Грибанов, Д. В.** Правовое регулирование кибернетического пространства как совокупности информационных отношений : автореф. дис. … канд. юрид. наук. – Екатеринбург, 2003. – 30 с. – Текст : непосредственный.

59. **Гутман, И. Е.** Компьютерные виртуальные игры: культурно-антропологические аспекты анализа : дис. … канд. философ. наук. – Санкт–Петербург, 2009. – 193 с. – Текст : непосредственный.

60. **Евдокимов, К. Н.** Противодействие компьютерной преступности: теория, законодательство, практика : автореф. дис. … докт. юрид. наук. – Москва, 2022. – 73 с. – Текст : непосредственный.

61. **Зайнутдинова, Е. В.** Смарт-контракт в гражданском праве : автореф. дис. ... канд. юрид. наук. – Красноярск. 2022. – 25 с. – Текст : непосредственный.

62. **Казанцев, Е. А.** Гражданско-правовое регулирование договорных отношений, осложненных электронным элементом : автореф. дис. ... канд. юрид. наук. – Барнаул, 2007. – 22 с. – Текст : непосредственный.

63. **Кананович, А. И.** Уголовно-правовая защита авторских прав в глобальной сети интернет : на примере законодательств России и Франции: автореф. дис. ... канд. юрид. наук. – Москва, 2013. – 29 с. – Текст : непосредственный.

64. **Карев, Я. А.** Правовое регулирование использования электронных документов в договорных отношениях : автореф. дис. ... канд. юрид. наук. – Москва, 2005. – 34 с. – Текст : непосредственный.

65. **Квашнин, В. И.** Правовые аспекты использования электронной цифровой подписи в договорных отношениях с участием предпринимателей : дис. ... канд. юрид. наук. – Санкт-Петербург, 2010. – 250 с. – Текст : непосредственный.

66. **Кириллова, А. А.** Проблема виртуальной реальности, социально-философский аспект : автореф. дис. … канд. философ. наук. – Мурманск, 2009. – 20 с. – Текст : непосредственный.

67. **Кликушина, Н. Ю.** Виртуализация действительности в сознании субъекта как элемент социальной реальности : автореф. дис. … канд. философ. наук. – Омск, 2007. – 24 с. – Текст : непосредственный.

68. **Ковалевская, Е. В.** Виртуальная реальность: философско-методологический анализ : автореф. дис. … канд. философ. наук. – Москва, 1998. – 22 с. – Текст : непосредственный.

69. **Костюк, И. В.** Гражданско-правовое регулирование электронной торговли : дис. ... канд. юрид. наук. – Казань, 2007. – 213 с. – Текст : непосредственный.

70. **Красикова, А. В.** Гражданско-правовое регулирование электронных сделок : автореф. дис. ... канд. юрид. наук. – Волгоград, 2005. – 22 с. – Текст : непосредственный.

71. **Кузнецова, Е. В.** Предупреждение делинквентного поведения несовершеннолетних, продуцируемого контентом сети интернет : автореф. дис. … канд. юрид. наук. – Курск, 2019. – 25 с. – Текст : непосредственный.

72. **Кулик, Т. Ю.** Особенности правового регулирования договоров, заключаемых в электронной форме : автореф. дис. ... канд. юрид. наук. – Краснодар, 2007. – 34 с. – Текст : непосредственный.

73. **Летёлкин, Н. В.** Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-телекоммуникационных сетей: включая сеть «Интернет» : автореф. дис. ... канд юрид. наук. – Нижний Новгород, 2018. – 28 с. – Текст : непосредственный.

74. **Малышко, А. А.** Философские проблемы виртуальной реальности (историко-философский аспект) : автореф. дис. … канд. философ. наук. – Мурманск, 2008. – 24 с. – Текст : непосредственный.

75. **Маньшин, С. В.** Гражданско-правовое регулирование применения электронно-цифровой подписи в сфере электронного обмена данными : дис. ... канд. юрид. наук. – Москва, 2001. – 200 с. – Текст : непосредственный.

76. **Миненкова, Н. В.** Международно-правовое и национально-правовое регулирование электронной торговли : автореф. дис. ... канд. юрид. наук. – Москва, 2008. – 26 с. – Текст : непосредственный.

77. **Морхат, П. М.** Правосубъектность искусственного интеллекта в сфере права интеллектуальной собственности: гражданско-правовые проблемы : автореф. дис. ... канд. юрид. наук. – Москва, 2018. – 45 с. – Текст : непосредственный.

78. **Моченов, В. Ю.** Правовое регулирование электронной коммерции : автореф. дис. ... канд. юрид. наук. – Москва, 2006. – 25 с. – Текст : непосредственный.

79. **Никитенко, С. В.** Международно-правовое регулирование использования искусственного интеллекта в области медицины : дис. ... канд. юрид. наук. – Санкт-Петербург, 2023. – 423 с. – Текст : непосредственный.

80. **Носова, С. С.** Метаморфозы цифрового сетевого общества: социально-философский анализ : автореф. дис. … канд. философ. наук. – Томск, 2022. – 24 с. – Текст : непосредственный.

81. **Опарина, И. Г.** Интернет в современном обществе: социально-философский анализ : автореф. дис. ... канд. философ. наук. – Красноярск, 2005. – 24 с. – Текст : непосредственный.

82. **Опенков, М. Ю.** Виртуальная реальность: онто-диалогический подход : автореф. дис. … д-ра философ. наук. – Москва, 1997. – 38 с. – Текст : непосредственный.

83. **Орехов, С. И.** Виртуальная реальность: исследование онтологических и коммуникативных основ : дис. … д-ра философ. наук. – Омск, 2002. – 332 с. – Текст : непосредственный.

84. **Паперно, Е. Л.** Правовое регулирование электронной торговли в России, Германии и США : автореф. дис. ... канд. юрид. наук. – Москва, 2006. – 22 с. – Текст : непосредственный.

85. **Простосердов, М. А.** Экономические преступления, совершаемые в киберпространстве, и меры противодействия им : автореф. дис. ... канд. юрид. наук. – Москва, 2016. – 28 с. – Текст : непосредственный.

86. **Рассолов, И. М.** Право и Интернет. Теоретические проблемы : дис. ... д-ра. юрид. наук. – Москва, 2008. – 357 с. – Текст : непосредственный.

87. **Родина, Е. А.** Противодействие криминальной виктимизации пользователей сети «интернет» в киберпространстве : дис. ... кандидата юридических наук. – Саратов, 2022. – С.22. – Текст : непосредственный.

88. **Рыков, А. Ю.** Гражданско-правовое регулирование сделок в глобальной компьютерной сети «Интернет» : автореф. дис. ... канд. юрид. наук. – Москва, 2009. – 30 с. – Текст : непосредственный.

89. **Симонович, П. С.** Правовое регулирование отношений, связанных с совершением сделок в электронных информационных сетях в России, США и ЕС : автореф. дис. ... канд. юрид. наук. – Москва, 2004. – 25 с. – Текст : непосредственный.

90. **Терентьева, Л. В.** Судебная юрисдикция по трансграничным частноправовым спорам в киберпространстве : автореф. дисс. … докт. юрид. наук. – Москва, 2021. – 61 с. – Текст : непосредственный.

91. **Тропина, Т. Л.** Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : автореф. дис. ... канд. юрид. наук. – Владивосток, 2005. – 26 с. – Текст : непосредственный.

92. **Туркулец, В. А.** Защита несовершеннолетних от преступных посягательств, совершаемых с использованием сети «Интернет» : дис. ... канд. юрид. наук. – Москва, 2023. – 49 с. – Текст : непосредственный.

93. **Ходенкова, Э. В.** Сущность Интернета вещей: социально-философский анализ : автореф. дис. ... канд философ. наук. – Томск, 2019. – 18 с. – Текст : непосредственный.

94. **Цуркан, Е. Г.** Социокультурная динамика и интернет-технологии: социально-философский анализ : дис. ... канд. философ. наук. – Москва, 2021. – 244 с.

95. **Щёголева, С. В.** Законодательное регулирование использования цифровых подписей в странах с развитой рыночной экономикой: сравнительно-правовой анализ : автореф. дис. ... канд. юрид. наук. – Москва, 2011. – 23 с. – Текст : непосредственный.

96. **Щитова, А. А.** Правовое регулирование информационных отношений по использованию систем искусственного интеллекта : автореф. дис. ... канд. юрид. наук. – Москва, 2022. – 29 с. – Текст : непосредственный.

97. **Якубов, М. Л.** Правовое регулирование отношений из «смарт-контрактов», заключаемых кредитными организациями : автореф. дис. ... канд. юрид. наук. – Москва, 2025. – 22 с. – Текст : непосредственный.

6. Учебники и учебные пособия

98. **Алексеев, С. С.** Механизм правового регулирования в социалистическом государстве / С. С. Алексеев. – Москва : Юридическая литература, 1966. – 187 с.

99. **Алексеев, С. С.** Общая теория права : в двух томах. Т. I / С. С. Алексеев. – Москва : Юридическая литература, 1981. – 316 с.

100. **Архипов, В. В.** Интернет-право: учебник и практикум для бакалавриата и магистратуры. – 2-е изд., перераб. и доп. / В. В. Архипов. – Москва : Изд-во Юрайт, 2020. – 275 с.

101. **Ван Дейк, Я.** Сетевое общество / Я. ван Дейк; пер. с англ. М. В. Немировского. – Москва : Фаир-Пресс, 2004. – 400 с. – Текст : непосредственный.

102. **Васьковский, Е. В.** Учебник гражданского права : Вып. 1. / Е. В. Васьковский. – Текст : электронный // Санкт-Петербург : издание юридического книжного магазина Н. К. Мартынова, 1896. – 188 с. – URL: https://dspace.spbu.ru/handle/11701/17479 (дата обращения: 21.02.2024).

103. **Васьковский, Е. В.** Учебник гражданского права. Вып. 2. Вещное право / Е. В. Васьковский – Текст : электронный. // Санкт-Петербург : издание юридического книжного магазина Н. К. Мартынова, 1896. – 190 с. – URL: https://dspace.spbu.ru/handle/11701/17479 (дата обращения: 21.02.2024).

104. **Волков, В. Э.** Цифровое право. Общая часть: учебное пособие / В. Э. Волков. – Самара : Издательство Самарского университета, 2022. – 111 с. – Текст : непосредственный.

105. **Зубофф, Ш.** Эпоха надзорного капитализма: борьба за человечество на новом рубеже цифровой цивилизации / Ш. Зубофф ; пер. с англ. А. С. Назарова. – Москва : АСТ, 2020. – 688 с.

106. **Исаков, В. Б.** Фактический состав в механизме правового регулирования / В. Б. Исаков ; науч. ред. С. С. Алексеев. // Саратов : Издательство

Саратовского университета, 1980. – 128 с. – URL: https://publications.hse.ru/mirror/pubs/share/direct/290655791 (дата обращения: 21.02.2024).

107. **Кастельс, М.** Информационная эпоха: экономика, общество и культура / М. Кастельс ; пер. с англ. под науч. ред. А. И. Шеремета. – Москва : Изд. дом Гос. ун-та Высш. шк. экономики, 2000. – 607 с.

108. **Касьянов, В. В.** Социология Интернета : Учебник / В. В. Касьянов, В. Н. Нечипуренко. – 1-е изд. – Москва : Изд-во Юрайт, 2018. – 424 с. – Текст : непосредственный.

109. Концепция цифрового государства и цифровой правовой среды: монография / под общ. ред. Н. Н. Черногора, Д. А. Пашенцева. – Москва : ИНФРА-М, 2022. – 244 с. – Текст : непосредственный.

110. **Коркунов, Н. М.** Лекции по общей теории права : [сочинение] Н. М. Коркунова, профессора С.-Петербургского университета. – 9-е изд. (без изменений). / Н. М. Коркунов. – Текст : электронный. // Санкт-Петербург : издание Юридического книжного магазина Н. К. Мартынова, 1909. – 354 с. – URL: https://viewer.rusneb.ru/ru/000199_000009_005040723?page=1&rotate=0&theme=white (дата обращения: 21.02.2024).

111. **Кропачев, Н. М.** Уголовно-правовое регулирование: Механизм и система : монография / Н. М. Кропачев. – Санкт-Петербург : Санкт-Петербургский государственный университет, 1999. – 262 с. – Текст : непосредственный.

112. **Лазарев, В. В.** Общая теория права и государства : учебник / В. В. Лазарев. – 3-е изд., перераб. и доп. – Москва : Юристъ, 2000. – 520 с. – Текст : непосредственный.

113. **Лазарев, В. В.** Теория государства и права : учебник для вузов / В. В. Лазарев, С. В. Липень. – 5-е изд., испр. и доп. – Москва : Издательство Юрайт, 2025. – 521 с. – Текст : непосредственный.

114. **Леонтьев, А. Н.** Киберправо : учебное пособие / А. Н. Леонтьев. – Волгоград : ВолгГТУ, 2021. – 80 с. – Текст : непосредственный.

115. **Ловцов, Д. А.** Информационное право: учебник для вузов / Д. А. Ловцов. – Москва: Изд-во Юрайт, 2024. – 411 с. – Текст : непосредственный.

116. **Марченко, М. Н.** Теория государства и права : курс лекций / М. Н. Марченко. – Москва : Зерцало, 1998. – 475 с. – Текст : непосредственный.

117. **Матузов, Н. И.** Личность. Права. Демократия. Теоретические проблемы правового статуса личности в социалистическом обществе : монография / Н.И Матузов. – Саратов : [б. и.], 1972. – 172 с. – Текст : непосредственный.

118. **Матузов, Н. И.** Теория государства и права: учебник / Н. И. Матузов, А. В. Малько. – 5-ое изд. – Москва : Дело, 2022. – 528 с. – Текст : непосредственный.

119. **Моазед, А.** Революция платформ: как сетевые рынки преобразовывают экономику и как заставить их работать на вас / А. Моазед, Н. Джонсон; пер. с англ. М. Волынкина. – Москва : Альпина Паблишер, 2019. – 288 с. – Текст : непосредственный.

120. **Наумов, В. Б.** Право и Интернет: Очерки теории и практики : монография / В. Б. Наумов. – Москва : Книжный дом «Университет», 2002. – 432 с. – Текст : непосредственный.

121. **Нерсесянц, В. С.** Общая теория права и государства : учебник для вузов / В. С. Нерсесянц. – Москва : Норма : ИНФРА-М, 1999. – 552 с. – Текст : непосредственный.

122. **Понкин, И. В.** Право и цифра: Машиночитаемое право, цифровые модели-двойники, цифровая формализация и цифровая онто-инженерия в праве: учебник / И. В. Понкин, А. И. Лаптева. – Москва : Буки Веди, 2021. – 174 с. – Текст : непосредственный.

123. Право в условиях цифровой реальности : монография / отв. ред. Т. Я. Хабриева, Н. Н. Черногор. – Москва : Проспект, 2020. – 368 с. – Текст : непосредственный.

124. **Рассолов, И. М.** Право и Интернет. Теоретические проблемы / И. М. Рассолов. – Москва : Норма, 2009. – 383 с. – Текст : непосредственный.

125. **Рассолов, И. М.** Право и Интернет. Теоретические проблемы / И. М. Рассолов. – 2-е изд., доп. – Москва: Норма: ИНФРА-М, 2017. – 383 с. – Текст : непосредственный.

126. **Рейнгольд, Г.** Виртуальное сообщество / Г. Рейнгольд; пер. с англ. А. Е. Марьяновского; под науч. ред. К. В. Костюка. – Москва: Фаир-Пресс, 2012. – 430 с. – Текст : непосредственный.

127. **Сырых, В. М.** Логические основания общей теории права. Методологические вопросы общей теории права : в 2 т. Т. 1. / В. М. Сырых. – Москва : Юстицинформ, 2004. – 528 с. – Текст : непосредственный.

128. Теория государства и права : учебник для вузов / под ред. В. М. Корельского, В. Д. Перевалова. – Москва : Норма : ИНФРА-М, 1998. – 569 с. – Текст : непосредственный.

129. Трансграничные отношения в киберпространстве: правовое регулирование, кибербезопасность, разрешение споров : монография / В. А. Канашевский, Б. А. Шахназаров, Л. В. Терентьева, О. Ф. Засемкова. – Москва : Проспект, 2024. – 136 с. – Текст : непосредственный.

130. Трансформация права в цифровую эпоху : монография / Министерство науки и высшего образования РФ, Алтайский государственный университет ; под ред. А. А. Васильева. – Барнаул : Изд-во Алт. ун-та. – 2020. – 432 с. – Текст : непосредственный.

131. **Трубецкой, Е. Н.** Лекции по энциклопедии права / Е. Н. Трубецкой. – Текст : электронный // Москва : типография Императорского Московского Университета, 1909. — 227 с. — URL: http://elib.fa.ru/AVTOGRAF/trubetskoj_1.pdf (дата обращения: 04.02.2024).

132. **Хропанюк, В. Н.** Теория государства и права : учебник для высших учебных заведений / В. Н. Хропанюк; под ред. В. Г. Стрекозова. – 6-е изд., стер. – Москва: Омега-Л, 2012. – 323 с. – Текст : непосредственный.

133. Цифровое право: учебник / под общ. ред. В. В. Блажеева, М. А. Егоровой. – Москва : Проспект, 2021. – 640 с. – Текст : непосредственный.

7. Научные статьи зарубежных авторов

134. All About WIPO – World Intellectual Property Organisation. – Текст : электронный // iPleaders : [сайт]. – 2024. – URL: https://blog.ipleaders.in/wipo-world-intellectual-property-organisation/ (дата обращения: 09.04.2024).

135. **Arthur, M.** What You Should Know About Online Dispute Resolution / M. Arthur, M. Ahalt. – Текст : электронный // Practical Litigator. – 2009. – Vol. 20. – P. 21–28. – URL: https://montyahalt.com/know-about-online-dispute-resolution/ (дата обращения: 01.09.2024).

136. **Bennett Moses, L.** Algorithmic prediction in policing: assumptions, evaluation, and accountability / L. Bennett Moses, J. Chan // Policing and Society, 2018. – Vol. 28, № 7. – P. 806–822. – Текст : непосредственный.

137. **Bennett Moses, L.** The Limits of Predictive Analytics in Policing: A Critical Analysis of the Use of Big Data for Crime Prevention / L. Bennett Moses // Big Data & Society. – 2018. – Vol. 5, no. 2. – P. 1–17. – Текст : непосредственный.

138. **Boellstorff, T.** Coming of age in Second Life: an anthropologist explores the virtually human / T. Boellstorff. – New Jersey: Princeton University Press, 2008. – 336 p. – Текст : непосредственный.

139. **Castronova, E.** Synthetic Worlds: The Business and Culture of Online Games / E. Castronova. – Текст : электронный. // Chicago; London: The University of Chicago Press. – 2005. – 332 p. – URL: https://www.researchgate.net/publication/37691974_Synthetic_Worlds_The_Business_and_Culture_of_Online_Games (дата обращения: 12.04.2025).

140. **Choucri, N.** Who controls cyberspace? / N. Choucri, D. D. Clark // Bulletin of the Atomic Scientists. – 2013. – Vol. 69, № 5. – P. 21–31. – Текст : непосредственный.

141. **Dennett, D. C.** The Part of Cognitive Science That Is Philosophy / D. C. Dennett // Topics in Cognitive Science. – 2009. – Vol. 1, № 2. – P. 231–236. – Текст : непосредственный.

142. **Desforges, A.** Representations of Cyberspace: A Geopolitical Tool / A. Desforges // Cyberspace: Political Issues. – 2014. – Vol. 1, no. 152-153 – P. 67–81. – Текст : электронный // Cyberspace: Political Issues : [сайт]. – 2023. – URL:

https://www.cairn-int.info/abstract-E_HER_152_0067--representations-of-cyberspace-a-geopolit.htm (дата обращения: 24.03.2023).

143. **Fang, B.** Cyberspace Sovereignty: Reflections on building a community of common future in cyberspace / B. Fang. – Singapore: Science Press and Springer Nature Singapore Pte Ltd. – 2018. – 482 p. – URL: https://doi.org/10.1007/978-981-13-0320-3. (дата обращения: 24.01.2025).

144. G7 Digital and Technology Ministers' meeting (2021, London). Ministerial Declaration G7 Digital and Technology Ministers' meeting, 28 April 2021. – Тескт : электронный – [London]: G7, 2021. – 6 p. – https://www.soumu.go.jp : [сайт]. – 2021. – URL: https://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/presentation/pdf/G7_Digital_and_Technology_Ministerial_Declaration.pdf (дата обращения: 21.12.2024).

145. General Data Protection Regulation: просто о новых правилах обработки персональных данных. – Текст : электронный // Gravitec : [сайт]. – 2018. – URL: https://gravitec.net/ru/blog/1827-2-gdpr-pravila-obrabotki-personal-nykh-dannykh/ (дата обращения: 10.12.2024).

146. **Habermas, J.** Between facts and norms: contributions to a discourse theory of law and democracy / J. Habermas; translated by William Rehg. – Текст : электронный. – Cambridge, Mass.: The MIT Press, 1996. – 676 p. – https://www.academia.edu: [сайт]. – 1996. – URL: https://www.academia.edu/33297244/Jürgen_Habermas_Between_Facts_and_Norms (дата обращения: 04.02.2024).

147. **Henningsen, P.** The Five Eyes: The International Syndicate That Spies on the Entire World / P. Henningsen – Текст : электронный. // New Dawn Magazine. – 2014. – www.newdawnmagazine.com : [сайт]. – 2014. – URL: https://www.newdawnmagazine.com/articles/behind-the-news/the-five-eyes-the-international-syndicate-that-spies-on-the-entire-world/ (дата обращения: 26.12.2024).

148. **Hoffmann, E.** State as a Platform / E. Hoffmann // Journal of Public Administration Research and Theory. – 2018. – Vol. 28, No. 4. – Pp. 653–670. – Текст : непосредственный.

149. ICANN : international organization. – Текст : электронный // Britannica : [сайт]. – 2024. – URL: https://www.britannica.com/topic/ICANN (дата обращения: 16.05.2024).

150. **Johnson, D. R.** Law and Borders: The Rise of Law in Cyberspace / Johnson, D. R., Post D. G. – Текст : электронный // Stanford Law Review. – 1996. – Vol. 48, № 5. – Stanford Law Review : [сайт]. – 1996. – URL: https://lawreview.stanford.edu (дата обращения: 12.04.2024).

151. **Kim, B.** Network Neutrality in S. Korea / B. Kim, B. Oh. – Текст : электронный // https://act.jinbo.net : [сайт]. – 2014. – URL: https://act.jinbo.net/wp/8351/ (дата обращения: 03.11.2024).

152. **Kim, S. J.** ROK's New National Cybersecurity Strategy and Its Implications / S. J. Kim – Текст : электронный. // INSS Issue Brief. – Seoul, Republic of Korea : Institute for National Security Strategy. – 2024. – Vol. 106, № 3. – P. 1–7. – www.inss.re.kr/upload/bbs/ : [сайт]. – 2024. – URL: https://www.inss.re.kr/upload/bbs/BBSA05/202404/F20240425131646465.pdf (дата обращения: 03.11.2024).

153. **Koops, B.-J.** Law, technology, and society: reimagining the human-machine relationship / Bert-Jaap Koops. – Текст : электронный // Cambridge, United Kingdom; New York, NY, USA: Cambridge University Press. – 2024. – 300 p. – https://papers.ssrn.com : [сайт]. – 2024. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1479819 (дата обращения: 02.04.2024).

154. **Lessig, L.** Code and other laws of cyberspace, Version 2.0 / L. Lessig. – New York: Basic Books. – 2006. – 391 p. – Текст : непосредственный.

155. **Lister, J.** Digital Millennium Copyright Act / J. Lister. – Текст : электронный // FreePrivacyPolicy : [сайт]. – 2024. – URL: https://www.freeprivacypolicy.com/blog/digital-millennium-copyright-act-dmca/ (дата обращения: 02.02.2024).

156. **Lynskey, O.** The foundations of EU data protection law / O. Lynskey. – Текст : электронный. – Oxford, United Kingdom; New York, NY, USA : Oxford University Press. – 2015. – 269 p. – books.google.ru : [сайт]. – 2015. – URL:

https://books.google.ru/books/about/The_Foundations_of_EU_Data_Protection_La.html?id=jCXYCgAAQBAJ&redir_esc=y (дата обращения: 02.04.2024).

157. **Menthe, D. C.** Jurisdiction in Cyberspace: A Theory of International Spaces / D. C. Menthe. – Текст : электронный // Michigan Telecommunications & Technology Law Review. – 1998. – Vol. 4, № 1. – P. 69–102. – https://repository.law.umich.edu : [сайт]. – 2024. – URL: https://repository.law.umich.edu/mttlr/vol4/iss1/3/ (дата обращения: 02.04.2024).

158. **Odumosu, D. O.** Artificial Intelligence and Legal Personality: Any Rescue From Salomon v. Salomon? / D. O. Odumosu, G. Solomon. – Текст : электронный // IX International Conference on Complex Systems. – 2018. – URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5106653 (дата обращения: 07.05.2024).

159. **Oladimeji, P.** South Korea data protection law (PIPA): Everything you need to know. – Текст : электронный // DIDOMI : [сайт]. – 2024. – URL: https://www.didomi.io/blog/south-korea-pipa-everything-you-need-to-know (дата обращения: 03.11.2024).

160. **Post, D. G.** Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace / D. G. Post. – Текст : электронный // Journal of Online Law. – 1995. – Art. 3. – https://www.academia.edu : [сайт]. – 2023. – URL:https://www.academia.edu/53108483/Anarchy_State_and_the_Internet_An_Essay_on_Law_Making_in_Cyberspace_article_3_ (дата обращения: 10.12.2024).

161. Research Handbook on International Law and Cyberspace / edited by N. Tsagourias, R. Buchan. – Cheltenham, UK; Northampton, MA, USA: Edward Elgar Publishing, 2015. – 574 p. – Текст : непосредственный.

162. **Resnick, P.** Reputation systems / P. Resnick, R. Zeckhauser, E. Friedman, K. Kuwabara // Communications of the ACM. – 2000. – Vol. 43, no. 12. – P. 45–48.

163. **Seema** The eIDAS Regulation – All You Need to Know / Seema. – Текст : электронный // https://www.revv.so/ : [сайт]. – 2024. – URL: https://www.revv.so/blog/decoding-eidas-regulation-all-you-need-to-know/ (дата обращения: 02.02.2024).

164. **Van Dijck, J.** The platform society: public values in a connective world / J. van Dijck, T. Poell, M. de Waal. – New York : Oxford University Press, 2018. – 209 p. – Текст : непосредственный.

165. **Vigliotti, M. G.** What Do We Mean by Smart Contracts? Open Challenges in Smart Contracts / M. G. Vigliotti – Текст : электронный // Frontiers in Blockchain. – 2021. – Vol. 3. – Art. 553671. – https://www.frontiersin.org : [сайт]. – 2021. – URL: https://www.frontiersin.org/journals/blockchain/articles/10.3389/fbloc.2020.553671/full (дата обращения: 12.05.2024).

166. **Wang, P.** Principle of Interest Politics: Logic of Political Life from China's Perspective / P. Wang. – Текст : электронный. – Singapore : Springer Nature Singapore; Beijing: Peking University Press. – 2022. – 151 p. – URL: https://doi.org/10.1007/978-981-19-3963-1 (дата обращения: 24.01.2025).

167. WIPO Arbitration and Mediation Center. – Текст : электронный // IT Law Wiki : [сайт]. – 2024. – URL: https://itlaw.fandom.com/wiki/WIPO_Arbitration_and_Mediation_Center (дата обращения: 09.04.2024).

8. Научные публикации российских авторов

168. «Мягкое право» в российской и зарубежной IT-сфере. – Текст : электронный // Институт развития интернета : [сайт]. – 2023. – URL: https://ири.рф/news/rossiyskoe-i-zarubezhnoe-myagkoe-pravo-v-it-sfere/?ysclid=m9ibszz86f991739175 (дата обращения 16.05.2024).

169. **Абделькарим, Я. А.** Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств / Я. А. Абделькарим // Journal of Digital Technologies and Law. – 2024. – Т. 2, № 2. – С. 262–285. – Текст : непосредственный.

170. **Абражеева, Д. В.** Действие механизма правового регулирования в современной России / Д. В. Абражеева, А. А. Музыкин, И. Г. Семёнов // Молодой ученый. – 2017. – № 2 (136). – С. 298–300. – Текст : непосредственный.

171. АН Москва: Роскомнадзор заблокировал 567 сайтов с незаконно размещенными персональными данными россиян // Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций : [сайт]. – 2019. – URL: https://rkn.gov.ru/press/publications/news66668.htm (дата обращения: 01.02.2024).

172. **Анько, А.** Определение электронных гражданских правоотношений / А. Анько. – Текст : электронный // сайт «Право и Интернет» : [сайт]. – 2001. – URL: https://www.russianlaw.net/law/general/theory/a121/ (дата обращения: 02.02 2024).

173. **Асланян, Н. П.** Об интерпретации термина «правовая природа» / Н. П. Асланян, Т. В. Новикова. – Текст : электронный // Baikal Research Journal : электронный научный журнал Байкальского государственного университета. – 2018. – Т. 9, № 4. – С. 25–31. – URL: brj-bguep.ru (дата обращения: 08.12.2024).

174. **Бачило, И. Л.** О правовых основах практической информатики / И. Л. Бачило // Вопросы защиты информации. – 2002 – №1. – С.20–28. – Текст : непосредственный.

175. **Болдачев, А.** Философия и цифровые технологии. Сборник статей / А. Болдачев. – Текст : электронный // https://kartaslov.ru/ : [сайт]. – 2022. – URL: https://kartaslov.ru/книги/Александр_Болдачев_Философия_и_цифровые_технологии_Сборник_статей/2 (дата обращения: 04.09.2024).

176. **Ботвинев, И.** Аналитика событий в мобильных приложениях: от разметки до оптимизации / И. Ботвинев. – Текст : электронный // https://ru.userx.pro/blog : [сайт]. – 2024. – URL: https://ru.userx.pro/blog/tpost/vcz1ru5zt1-analitika-sobitii-v-mobilnih-prilozheniy (дата обращения: 04.09.2024).

177. **Бурнов, В.** Защита киберсуверенитета: первые слушания цифровых законов прошли в Москве. – Текст : электронный // РАПСИ : [сайт]. – 2025. – URL: https://rapsinews.ru/digital_law_news/20250411/310784513.html (дата обращения: 16.05.2025).

178. **Волков, А. С.** Проблемы установления юрисдикции в виртуальном пространстве: российский и международный опыт / А. С. Волков // Вестник

Московского университета МВД России. – 2021. – № 1. – С. 35–41. – Текст : непосредственный.

179. **Ганиев, Р.** Как преступники могут использовать искусственный интеллект? Самый опасный вариант / Р. Ганиев. – Текст : электронный // Hi-News.ru : [сайт]. – 2020. – URL: https://hi-news.ru/technology/kak-prestupniki-mogut-ispolzovat-iskusstvennyj-intellekt-samyj-opasnyj-variant.html (дата обращения: 25.10.2024).

180. **Гаркуша-Божко, С. Ю.** Определение вооруженного конфликта в киберпространстве / С. Ю. Гаркуша-Божко // Вестник Санкт-Петербургского университета. Право. – 2023. – Т. 14. – №1. – С. 194–210. – Текст : непосредственный.

181. **Гусаков, Д. М.** Компьютерные преступления и уголовно-процессуальные особенности юрисдикции в информационной среде / Д. М. Гусаков // Российский следователь. – 2020. – № 11. – С. 16–20. – Текст : непосредственный.

182. **Давыдова, Л. И.** Территориально-государственное регулирование правонарушений в киберпространстве / Л. И. Давыдова // Правоведение. – 2021. – № 3. – С. 54–61. – Текст : непосредственный.

183. **Дмитриева, Н. И.** Суверенитет киберпространства как национальный суверенитет / Н. И. Дмитриева, Ц. Дун // Вопросы политологии. – 2022. – Т. 12, № 5 (81). – С. 1569–1580. – Текст : непосредственный.

184. **Долгов, С. Ф.** Особенности правоотношений, возникающих в интернет-пространстве / С. Ф. Долгов // Право и государство: теория и практика. – 2023. - №7(223). – С. 40–42. – Текст : непосредственный.

185. **Дураев, Т. А.** Правовая природа как категория правоведения / Т. А. Дураев, Н. В. Тюменева // Вестник Саратовской государственной юридической академии. – 2022. – № 6 (149). – С. 15–21. – Текст : непосредственный.

186. **Дыдыкин, А. Л.** Электронные репутационные системы и доверие в интернет-среде / А. Л. Дыдыкин // Вопросы государственного и муниципального управления. – 2013. – № 4. – С. 135–144. – Текст : непосредственный.

187. **Евсеенко, Т. Н.** Защита прав интеллектуальной собственности в российском сегменте сети Интернет: вопросы юрисдикции / Т. Н. Евсеенко // Интеллектуальная собственность. Авторское право и смежные права. – 2020. – № 12. – С. 18–23. – Текст : непосредственный.

188. **Ефимова, Л. Г.** Источники правового регулирования общественных отношений в киберпространстве / Л. Г. Ефимова // LEX RUSSICA. – 2020. – Т. 73, № 3. – С. 118–128. – Текст : непосредственный.

189. **Жернова, В. М.** Субъекты правоотношений в сети Интернет / В. М. Жернова // Вестник ЮУрГУ. Серия «Право». – 2015. – Т. 15, № 3. – С. 98–101. – Текст : непосредственный.

190. Исследование: ODR и его применение в сервисах в сфере интеллектуальной собственности в ЕС. – Текст : электронный / под ред. Дорофеева Е. Е. // Сетевое издание «IPQuorum» : [сайт]. – 2024. – URL: https://ipquorum.ru/upload/ODR-hplnsOcL.pdf (дата обращения 12.09.2024).

191. **Калугин, А. П.** Коллизии компетенций юрисдикций при разрешении споров в интернете / А. П. Калугин // Научные ведомости Белгородского государственного университета. Серия: Философия. Социология. Право. – 2020. – № 1. – С. 135–142. – Текст : непосредственный.

192. **Капустин, А. Я.** Суверенитет государства в киберпространстве: международно-правовое измерение / А. Я. Капустин // Журнал зарубежного законодательства и сравнительного правоведения. – 2022. – Т. 18, № 6. – С. 103–108. – Текст : непосредственный.

193. **Карсаков, Н. В** России заявили о необходимости поддержки цифрового суверенитета страны / Н. В. Карсаков – Текст : электронный // Газета.ru : [сайт]. – 2025. – URL: https://www.gazeta.ru/social/news/2025/09/19/26765426.shtml?utm_auth=false (дата обращения: 26.09.2025).

194. **Колесов, М. В.** Обеспечение конституционных прав и свобод человека и гражданина в условиях развития современных информационно-коммуникационных технологий / М. В. Колесов // Российский журнал правовых исследований. – 2023. – Т. 10, № 1. – С. 55–58. – Текст : непосредственный.

195. **Корнеев, С. Д.** Гражданские правоотношения в киберпространстве: проблемы выбора компетентной юрисдикции / С. Д. Корнеев // Адвокат. – 2021. – № 10. – С. 12–16. – Текст : непосредственный.

196. **Кочетков, А. П.** Цифровой суверенитет как основа национальной безопасности России в глобальном цифровом обществе / А. П. Кочетков, К. В. Маслов // Вестник Московского университета. Серия 12. Политические науки. – 2022. – № 2. – С. 31–45. – Текст : непосредственный.

197. **Кравчук, Н. В.** Правовой статус киберпространства / Н. В. Кравчук, Н. Цагориас // Государство и право в новой информационной реальности : сборник статей по материалам V Международного научно-практического форума, 20-21 апреля 2018 года / под ред. И. Д. Хубиева. – Москва : РГГУ, 2018. – С. 115–124. – Текст : непосредственный.

198. **Кулешова, Е. Г.** Государственно-территориальная принадлежность преступлений в глобальной сети: современные тенденции юрисдикции / Е. Г. Кулешова // Современное право. – 2021. – № 5. – С. 25–30. – Текст : непосредственный.

199. **Курочкин, С. А.** Эффективность правовых норм как условие результативности правового воздействия (на примере норм процессуального права) / С. А. Курочкин // Ученые записки казанского университета. Серия гуманитарные науки. – 2020. – Т. 162, кн. 2. – С. 69–83. – Текст : непосредственный.

200. **Кутюр, С.** Что означает понятие «суверенитет» в цифровом мире? / С. Кутюр, С. Тоупин // Вестник международных организаций: образование, наука, новая экономика. – 2020. – Т. 15, № 4. – С. 48–69. – Текст : непосредственный.

201. **Лучинкина, И. С.** Поведение личности в современной цифровой среде / И. С. Лучинкина. – Текст : электронный // Инновационная наука: Психология, Педагогика, Дефектология. – 2023. – №6 (3). – с. 51–58. – URL: https://cyberleninka.ru/article/n/povedenie-lichnosti-v-sovremennoy-tsifrovoy-srede (дата обращения: 04.09.2024).

202. **Лучинкина, И. С.** Поведение личности в современной цифровой среде / И. С. Лучинкина // Инновационная наука: Психология, Педагогика, Дефектология. – 2023. – №6 (3). – С. 51–58. – Текст : непосредственный.

203. **Мажорина, М. В.** Киберпространство и методология международного частного права / М. В. Мажорина // Журнал Высшей школы экономики. – 2020. – Т. 14, № 2. – С. 85–101. – Текст : непосредственный.

204. **Майер-Шенбергер, В.** Большие данные. Революция, которая изменит то, как мы живем, работаем и мыслим / В. Майер-Шенбергер, К. Кукьер ; пер. с англ. И. Гайдюк. – Москва : Манн, Иванов и Фербер, 2014. – 240 с. – Текст : непосредственный.

205. **Маневич, В. В.** Международно-правовое регулирование применения киберсредств при ведении вооруженных конфликтов: правовые основы и научные дискуссии / В. В. Маневич // Закон и право. – 2024. – №4. – С. 275–282. – Текст : непосредственный.

206. **Мельникова, Е. Н.** Встраиваемость концепции электронного лица в правовую систему конкретного государства или государственного образования / Е. Н. Мельникова // Российский юридический журнал. – 2022. – № 2 (143). – С. 94–12. – Текст : непосредственный.

207. **Мигулева, М. В.** Киберпространство как социальный институт: признаки, функции, характеристики / М. В. Мигулева // Научный журнал «Дискурс-Пи». – 2020. – № 4 (41). – С. 199–212. – Текст : непосредственный.

208. **Наумов, В. Б.** Проблемы доказывания в «электронном правосудии» / В. Б. Наумов // Информационное право. – 2005. – № 1. – С. 17–21. – Текст : непосредственный.

209. **Нестеров, С. А.** Понятие цифрового следа и анализ цифрового следа в образовании / С. А. Нестеров, Е. М. Смолина. – Текст : электронный // SAEC. – 2023. – №3. – С. 309–311. – URL: https://cyberleninka.ru/article/n/ponyatie-tsifrovogo-sleda-i-analiz-tsifrovogo-sleda-v-obrazovanii (дата обращения 4.10.2024).

210. Основные понятия [Электронный ресурс] // База знаний сервиса Carrot quest. — URL: help.carrotquest.io (дата обращения: 12.09.2024).

211. **Панов, И. В.** Особенности судебного рассмотрения дел, возникших в результате нарушения прав субъектов в киберпространстве / И. В Панов // Государственная власть и местное самоуправление. – 2020. – № 10. – С. 31–36. – Текст : непосредственный.

212. **Пашенцев, Д. А.** Новации правотворчества в условиях цифровизации общественных отношений / Д. А. Пашенцев, Д. Р. Алимова // Государство и право. – 2019. – №6. – С. 102–106. – Текст : непосредственный.

213. **Плотников, А. В.** Управление репутацией компании в интернете: инструменты управления репутацией, их применение и оценка эффективности / А. В. Плотников, А. Н. Иванова, К. О. Боровых, А. Ощепков // Креативная экономика. – 2021. – Т. 15, №10. – С.3823-3838. – Текст : непосредственный.

214. **Позова, Д. Д.** Международно-правовая характеристика правовых отношений в Интернете / Д. Д. Позова //Журнал цивилистики. – 2016. – №20. – С. 45–52. – Текст : непосредственный.

215. Право быть забытым: Испания против Google // Lawtrend – Исследования Образование Действия : [сайт]. – 2014. – URL: https://www.lawtrend.org/information-access/blog-information-access/pravo-byt-zabytym-evropejskij-sud-demonstriruet-nekompetentnost (дата обращения: 01.02.2024).

216. Правовые аспекты использования смарт-контрактов. – Текст : электронный // BIT.TEAM : [сайт]. – 2022. – URL: https://bit.team/blog/ru/pravovye-aspekty-ispolzovaniya-smart-kontraktov/ (дата обращения: 12.05.2024).

217. **Пузырева, Ю. В.** Кибервойна как новый вызов международному сообществу: вопросы международно-правовой регламентации. – Текст : электронный // ADVANCES IN LAW STUDIES. – 2022. – Т. 10, № 3. – С. 51-55. – URL: https://naukaru.ru/ru/nauka/article/52186/view#article-text (дата обращения: 16.05.2024).

218. **Рахматулина, Р. Ш.** Ответственность провайдера / Р. Ш. Разматулина // Вестник Московского городского педагогического университета. Серия: Юридические науки. – 2016. – №2 (22). – С. 84–89. – Текст : непосредственный.

219. **Рожкова, М. А.** Юридические факты в гражданском праве / М. А. Рожкова. – Москва : Хозяйство и право. Серия: Приложение к ежемесячному журналу «Хозяйство и право», № 7. – 2006. – 80 с.

220. **Савельев, А. И.** Проблемы применения норм гражданского права к отношениям, возникающим в сети Интернет / А. И. Савельев // Вестник гражданского права. – 2014. – № 1. – С. 37–75. – Текст : непосредственный.

221. **Сазонова, М.** Право в цифре: какие разработки есть уже сейчас? / М. Сазонова // ГАРАНТ.РУ : информационно-правовой портал. – 2022. – 14 июля. – URL: https://www.garant.ru/article/1554367/ (дата обращения: 01.09.2024).

222. **Сафоева, С. М.** Границы юрисдикции в киберпространстве: трансформация гражданско-правовых отношений / С. М. Сафоева. – Текст : электронный // Universum: экономика и юриспруденция : электрон. научн. журн. – 2023. – № 8 (107). – URL: https://7universum.com/ru/economy/archive/item/15821 (дата обращения: 08.09.2023).

223. **Семенов, А. Ю.** Развитие международного законодательства о юрисдикции в киберпространстве / А. Ю. Семенов // Вопросы экономики и права. – 2020. – № 3. – С. 51–57. – Текст : непосредственный.

224. **Такер, Р.** Судебный процесс: Чат-бот с искусственным интеллектом подтолкнул подростка из Флориды покончить с собой / Р. Такер. – Текст : электронный // Yahoo! News : [сайт]. – 2024. – URL: https://www.yahoo.com /news/lawsuit-ai-chatbot-encouraged-florida-174428518.html (дата обращения: 28.10.2024).

225. **Талапина, Э. В.** Право и цифровизация: новые вызовы и перспективы / Э. В. Талапина // Журнал российского права. – 2018. – № 2. – С. 3–15. – Текст : непосредственный.

226. **Танимов, О. В.** Трансформация правоотношений в условиях цифровизации / О. В Танимов // Актуальные проблемы российского права. – 2020. – № 2. – С. 11–18. – Текст : непосредственный.

227. **Терентьева, Л. В.** Правовое регулирование отношений в киберпространстве: вопросы управления и юрисдикции / Л. В. Терентьева. – Текст

: электронный // Материалы XV Международной конференции «Право и Интернет», Москва, 27–28 октября 2022 г. – Москва : ИФАП, 2022. – URL: https://ifap.ru/pi/15/pres11.pdf (дата обращения: 25.02.2023).

228. **Терентьева, Л. В.** Принципы установления территориальной юрисдикции государства в киберпространстве / Л. В. Терентьева. – Текст : электронный // yushchuk.livejournal.com : [блог-платформа]. – 2021. – URL: https://yushchuk.livejournal.com/1593956.html (дата обращения: 12.07.2023).

229. **Терентьева, Л. В.** Территориальный аспект юрисдикции и суверенитета государства в киберпространстве / Л. В. Терентьева // LEX RUSSICA. – 2019. - № 4 (149). – С. – 139–149. – Текст : непосредственный.

230. **Тёркл, Ш.** Жизнь на экране: идентичность в эпоху Интернета / Шерри Тёркл ; пер. с англ. А. Н. Алексеева. – Москва : Фонд «Общественное мнение», 2014. – 432 с. – Текст : непосредственный.

231. **Трофименко, А. В.** Особенности правового регулирования отношений в сфере оборота цифровых прав / А. В. Трофименко // Вестник Саратовской государственной юридической академии. – 2020. – № 2 (133). – С. 93–101. – Текст : непосредственный.

232. **Тюканова, В. Р.** Цифровизация нормотворчества. IT-технологии и киберпространство как средства и место реализации правоотношений / В. Р. Тюканова, П. В. Шумов // Скиф. Вопросы студенческой науки. – 2022. – № 11 (75). – С. 138–142. – Текст : непосредственный.

233. **Федотов, М. А.** Конституционные ответы на вызовы киберпространства // LEX RUSSICA. – 2016. – № 3 (112). – С. 164–182. – URL: https://lexrussica.msal.ru/jour/article/view/57/58 (дата обращения: 24.03.2023).

234. **Федотов, Н. А.** Правовые аспекты осуществления правосудия в условиях развития информационно-телекоммуникационных технологий / Н. А. Федотов // Российская юстиция. – 2021. – № 1. – С. 14–18. – Текст : непосредственный.

235. **Филипенко, В. А.** Правовая природа с точки зрения философии / В. А. Филипенко. – Текст : электронный // Информационно-правовой портал

«Закон.ру» : [сайт]. – 2022. – URL: https://zakon.ru/blog/2022/04/26/pravovaya_priroda_s_tochki_zreniya_filosofii (дата обращения: 12.12.2024).

236. **Цибульский, Ф. П.** Методы выявления цифрового следа при расследовании киберпреступлений / Ф. П. Цибульский // Информационные технологии. – 2019. – Т. 25, № 11. – С. 696–702. – Текст : непосредственный.

237. Цифровой суверенитет России 2025. – Текст : электронный // Politicana.ru : [сайт]. – 2025. – URL: https://politicana.ru/politics/domestic/digital-sovereignty-russia-2025/index.html (дата обращения: 14.04.2025).

238. **Чердаков, О. И.** Теоретико-правовая интерпретация юрисдикции в киберпространстве в зарубежных исследованиях / О. И. Чердаков, С. Б. Куликов // История государства и права. – 2024. – № 3. – С. 54–69. – Текст : непосредственный.

239. **Черкасов, В. С.** Действие права в «киберпространстве»: основные научные подходы// The Newman in Foreign policy. – 2022. – Т. 2, № 65 (109). – С. 7–9. – Текст : непосредственный.

240. **Шарифулин, В.** Бельгиец и чат-бот «Элиза» / В. Шарифулин. – Текст : электронный // Информационное агентство ТАСС : [сайт]. – 2023. – URL: https://tass.ru/obschestvo/17401353 (дата обращения: 25.10.2024).

241. **Юрьев, Д.** Не мытьем, так плагином: как мошенники используют чат-боты в России / Д. Юрьев. – Текст : электронный // Ferra.ru : [сайт]. – 2023. – URL: https://www.ferra.ru/news/v-rossii/ne-mytem-tak-plaginom-kak-moshenniki-ispolzuyut-chat-boty-v-rossii-10-05-2023.htm (дата обращения: 30.10.2024).

242. **Янькова, А. Д.** Архитектура концепции кибер-суверенитета КНР (по материалам докладов Всемирной интернет-конференции «Кибер-суверенитет: теория и практика») / А. Д. Янькова // Проблемы Дальнего Востока. – 2023. – №4. – С. 99-100. – Текст : непосредственный.