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

Институт права
(наименование института полностью)

Кафедра «Предпринимательское и трудовое право»
(наименование)

40.04.01 Юриспруденция
(код и наименование направления подготовки)

Правовое обеспечение предпринимательской деятельности
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Правовая охрана цифровых объектов»

Обучающийся О.О. Афанасьева
(И.О. Фамилия) (личная подпись)

Научный руководитель к.п.н., доцент Е.М. Чертакова
((ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2022

Оглавление

Введение

Актуальность темы исследования обуславливается целой совокупностью факторов.

Прежде всего, сам процесс цифровизации является глобальной тенденцией развития всего мирового сообщества. Развитие цифровых технологий оказывают колоссальное влияние на нашу жизнь. Вместе с тем, происходящая в настоящее время четвертая промышленная революция характеризуется повсеместной автоматизацией и использованием искусственного интеллекта или интеллектуальных технологий. При этом общество претерпевает изменения в сторону цифровизации. В связи с этим изменяются традиционные уклады жизни общества, появляются новые институты.

Даная тема актуальна ещё и по той причине того, что в отечественное законодательство в настоящее время были внесены изменения в ГК РФ. При этом статья 128 ГК РФ напрямую называет цифровые права объектом гражданских прав, а нормы статьи 141.1 как раз и посвящены характеристике цифровых прав.

Вместе с тем есть и очевидные проблемы. В частности, существуют определенные пробелы в законодательстве. Например, недостаточно точно и чётко урегулирован вопрос структуры, существенных условий, порядка заключения смарт-контрактов. И судебная практика по таким делам минимальна.

Также, несмотря на то что проблемы охраны цифровых объектов получили достаточное изучение, но все же новых исследований пока ещё недостаточно.

Таким образом, все вышеперечисленные факторы обуславливают актуальность и значимость темы настоящей магистерской диссертации.

Степень научной разработанности темы. Проблемы, которые затронуты в настоящей работе стали предметом изучения М. М. Агаркова, С.С. Алексеева, Л.И. Бачило, С.Н. Братуся, А.Б. Венгерова, В.А. Дозорцева, О.С. Иоффе, Я.А. Канторовича, О.А. Красавчикова, Я.М. Магазинера, Н.И. Матузова, Д.И. Мейера, А.С. Муромцева, А.А. Пиленко, В.И. Серебровского, В.И. Синайского, А.И. Соловьёва, Е.А. Суханова, Ю.К. Толстого, Р.О. Халфину, Б.Б. Черепахина, Г.Ф. Шершеневича.

Вместе тем, некоторые вопросы не получили достаточного изучения, например, нет четко обоснованной типологизации цифровых объектов, большая часть исследований касается, прежде всего, охраны объектов авторского права, которые существуют в цифровой форме, не разработана должным образом теория так называемого смарт-контракта.

Цель работы системный анализ механизма правовой охраны цифровых объектов.

Задачи работы:

- охарактеризовать цифровизацию общества как глобальную тенденцию всего общественного развития;

- рассмотреть основные способы, модели правовой охраны таких объектов нормами законодательства зарубежных стран;

- определить специфику защиты прав субъектов смарт-контрактов;

- дать определение анализа охраны цифровой информации;

- определить специфику защиты авторских прав цифровых объектов;

- определить проблемы, которые возникают в названной сфере, определить направления изменений законодательства.

Объект работы система общественных отношений, которые складываются в сфере охраны цифровых объектов.

Предмет работы система правовых норм, которые регулируют названные общественные отношения.

Методологической основой работы стала совокупность многообразных методов, как общенаучных (анализ, синтез. дедукция, индукция), так и собственно частно-научных, которые используются, как правило, юриспруденцией. Такими методами стали, например, формально-юридический метод, метод сравнительного правоведения.

Нормативно-правовой основой работы стали Конституция РФ, Гражданский кодекс РФ, ФЗ «О цифровой подписи», «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», ФЗ «Об информации, информационных системах и защите информации», подзаконные акты.

Теоретической основой стали исследования таких авторов, как Акинфиева В. В., Аюшеева И.З., Бычков А.И., Дядькин, Д.С., Соловьев А. И, Иванов А.А., Камалян В.М., Морхат П.М, Новолева А.М.

Научная новизна работы заключается в том, что был осуществлен системный анализ круга цифровых объектов, выявлены основные модели правовой защиты цифровых объектов на основании законодательства зарубежных стран, выявлены проблемные вопросы и обоснованы предложения по изменению отечественного законодательства.

Положения, выносимые на защиту:

1. Выделяют типичные признаки информационного общества, такие как информационный взрыв, увеличение компетенции участников общественных отношений, максимальная быстрота во всех общественных процессах, которые протекают в рамках общества. Максимально зримое влияние процессы цифровизации оказывают на политическую и экономическую сферу, в последнем случае речь идёт о формировании такого феномена как «цифровая экономика».

2. Можно выделить две большие группы защиты прав цифровых объектов. Первая группа - это общегражданские методы и способы защиты прав, которые характерны для всего гражданского права, применимы

совершенно к любым общественным отношениям, которые регулируются нормами гражданского права. Как правило выделяют юрисдикционную и не юрисдикционную форму защиты. Если говорить про специальные формы защиты цифровых объектов, то как правило выделяют следующие виды:

- специальные формы защиты токенов;

- особые, специфические формы защиты объектов культурного наследия, которые существуют в цифровой форме;

- особые способы защиты прав субъектов смарт-контрактов.

3. Охрана государством прав человека на цифровые объекты является самым действенным механизмом стимулирования и использования интеллектуального потенциала нации. Уровень охраны прав на цифровые объекты, посредством четкой системы правовых средств, является весомым стимулом для творческой деятельности высококвалифицированных специалистов и одной из главных предпосылок социального, экономического и культурного прогресса; главным генератором развития инновационных процессов.

4. Предполагается, что совершенствование способов охраны цифровых объектов может быть достигнуто путём объединения усилий государственных и общественных структур с целью оптимизации норм Законодательства РФ об авторском праве и смежных правах, и путем развития соответствующего общественного правосознания.

5. Несмотря на особую природу программ для ЭВМ и их очевидное отличие от произведений литературы, невозможно расширять пределы охраны программы для ЭВМ нормами авторского права дальше, чем охрану исходного кода и его близкого перефразирования.

Структура работы обусловлена поставленной целью и задачами. Диссертация состоит из введения, трех разделов, объединяющих восьми параграфов, заключения, списка используемой литературы и используемых источников.

Глава 1 Теоретико-методологические подходы к охране цифровых объектов

1.1 Переход к цифровому обществу как тенденция глобального развития общественных отношений

«Несмотря на то, что в настоящее время концепция цифрового общества приобрела довольно существенный импульс развития, тем не менее каких-то единых универсальных подходов к пониманию цифрового общества в настоящее время пока ещё нет» [66]. «Теоретические основы, понятийный аппарат и методы изучения цифрового общества и цифровой социологии только формируются» [87]. «Исследования охватывают как самые общие вопросы, вроде соотношения «реального» и «виртуального» [34], сущности «цифровизации» [85], так и «конкретные ее проявления в различных сферах жизни. Разработаны теоретические концепции, объясняющие преобразования, происходящие при формировании цифрового общества» [86].

Тем не менее процессы углубления цифровизации, последовательно охватывающей все более фундаментальные социальные структуры, требуют дальнейшего осмысления. Приведем несколько концепций цифрового общества, которые обосновываются в настоящее время.

Так, например, многие исследователи «выделяют пять таких аспектов» [39].

Во-первых, это так называемый информационный аспект или «информационный взрыв». При этом, в рамках различных наук порой даются попытки дать дефинитивное определение такой категории, как «информационный взрыв».

Здесь следует обратить внимание на точку зрения Б. Б. Славина, который полагает, что информационный взрыв - это «ускоренный рост

информации, ускоренное появление новинок и изменений, быстрое обесценивание, устаревание информации и знаний, сопровождаемые интенсивным ростом индустрии информации» [64].

Таким образом, делается акцент, прежде всего, на резкости, быстроте событий, на том, что:

- происходит радикальное увеличение объема хранимой информации;

- на второй план уходит само содержание коммуницирования;

- возможно возникновение и двух, казалось бы, логически исключающих друг друга понятий, как с одной стороны информационной перегруженности, но с другой стороны информационного дефицита.

Причём, здесь даже нет неразрешимого противоречия просто человек, с одной стороны, использует только ту информацию, которая нужна ему именно сейчас, в том числе и в процессе образовательной деятельности, вся остальная информация приобретает статус «информационного шума».

Второй аспект - это так называемый информационно-коммуникативный аспект, для пользователей становится возможным взаимодействовать друг с другом и широким кругом лиц, объединяющиеся не только общим интересом, ограничений в этом смысле нет. Кроме того, сообщества в социальных сетях никак не привязаны территориально. Качество социальных сетей становятся лучше, информационно-коммуникативные системы становятся доступнее и лучше по качеству. Происходит увеличение объема общения, то есть коммуникация. «Одновременно над этим «символическим капиталом» надстраивается его модус самовозрастающая коммуникация. В итоге потребление коммуникации ради коммуницирования без границ становится массовым видом повседневных практик в информационном обществе» [27].

Третий аспект - это так называемый временной аспект, который нашёл своё объективное выражение в следующем:

- радикально увеличивается способ передачи информации, распространения информации и её обработка;

- в сфере научных исследований такой временной фактор объективно помогает исследователям более чётко излагать свои концепции, идеи, точки зрения;

- любое открытие в сфере науки, любое достижение в сфере образования распространяется максимально быстро, такие транслируемые идеи уже невозможно замолчать;

- временной фактор фактически меняет и систему, например, фондовых, аукционных торгов, а равно систему продаж и т.д.;

- естественно, временной фактор начинает проявляться и в быту, например, сервисы приносят в нашу жизнь больше комфорта и удобства в реализацию повседневных планов и дел, это касается и заказа продуктов, и вызова такси, и получение государственных сервисов и запросов.

Как подчеркнула Н.В. Кунцевич, цифровое общество, «понимаемое как концепт, требует ценностного измерения», благодаря чему «разделение оптимистического и пессимистического взглядов станет в высшей степени контрастным». [39] При этом, в рамках доктрины выделяют основные концепты, признаки закономерности развития, функционирования цифрового общества.

Так, например, А. Смирнова, выделяет «четыре концепта цифрового общества» [66].

Первый концепт - это сверхсвязанность. Сказанное означает, «что именно в условиях цифрового общества цифровые технологии максимально плотно проникают друг в друга и в жизнь человека. При этом, в настоящее время речь идёт не только про Интернет, но и вообще в жизнь человека» [57]. И в данном случае, уже можно говорить не просто о проникновении интернета во многие сферы жизни, но и влияние искусственного интеллекта.

Вторая константа - это платформизация. Данная константа означает не просто проникновение цифровой технологий и цифровых платформ в жизнь человека, а проникновение во все сферы его жизни. При этом, под цифровыми платформами понимается вся совокупность программируемой цифровой инфраструктуры. Платформы позволяют переводить в цифровую среду самые разнообразные формы, методы социального взаимодействия общение, покупки, поиск работы и т.д.

Естественно, цифровые технологии дают преимущество тем корпорациям, которые способны создавать те цифровые платформы, которые имеют трансграничный и трансконтинентальный характер.

Третий концепт - это так называемая датификация. То есть процесс монетизации человеческой жизни с помощью цифровой информации.

На основании вышесказанного можно утверждать, что возникают новые свойства информатизации, например, многообразие информации, увеличивается скорость обработки информации, увеличивается ее объем и многообразие.

Четвёртый концепт - это так называемое алгоритмическое управление. Такой концепт выдвигает на первый план идею о том, что цифровые технологии не только влияют на социальную среду, но и формирует эту среду.

Алгоритмическое управление довольно сложное и неодинаковое по своей природе начиная от простой процедуры модернизации и заканчивая формированием система социального кредита, которая, например, получила распространение в современном Китае. При этом, доктринально обосновывается точка зрения о том, что все названные 4 константы взаимно влияют друг на друга.

А. Деревянченко, «характеризуя современное цифровое общество выделяет следующие тенденции развития» [21].

Во-первых, это информационный взрыв, который выразился и конкретизировался в постоянном, неуклонном росте объёма информации. «При этом, по прогнозам исследователей только в течение 2008-2025 годов объём всей информации, которая существует в мире вырастет в 6 раз» [38].

Во-вторых, это появление новых устройств при получении информации, ее обработки. Это новые устройства и приспособления, при подключении которых к Интернету возникает дополнительная возможность обработки информации.

«В настоящее время к Интернету уже подключено всего в мире более 22 млрд. устройств» [28].

В-третьих, человек в цифровом обществе приобретает так называемый цифровой профиль, своё «цифровое «я». При этом, фактически осуществляется цифровизации не только общественной жизни человека, но и его частной жизни. При этом, как отмечается, цифровая информация о человеке фактически будет содержать больше информации, чем та информация, которую человек знает о себе.

В-четвёртых, это распространение так называемого нательного Интернета.

В рамках науки особое внимание уделяется анализу такого явления современного цифрового общества, как цифровая экономика.

В настоящее время в рамках западной науки признанным считается определение цифровой экономики, которое сформулированы и закреплены в Оксфордском словаре, а именно «цифровая экономика - это экономика, которая главным образом функционирует за счет цифровых технологий, особенно электронных транзакций, осуществляемых с использованием интернета» [28].

Такое определение касается только отечественной науки, но при это концепции могут быть разными. Так, например, В. Бондаренко полагает, что «цифровая экономика является определенной моделью отношений между

людьми, которая совместима с так называемой четвёртой промышленной революции» [12].

В свою очередь Р. Аксанов выражает мнение о том, что «цифровая экономика ничто иное, как специфический способ экономики, которая основана на производстве электронных товаров и сервисов высокотехнологичными бизнес - структурами и дистрибуции этой продукции при помощи электронной коммерции» [4].

«Одновременно, довольно распространено понимание цифровой экономики и как особого сегмента экономических отношений, где прежде всего реализуют новые технические достижения, преимущества глобальной сети, информационных систем» [23].

«Также популярным является понимание цифровой экономики, как экономики, характерной особенностью которой является максимальное удовлетворение потребностей всех ее участников за счет использования информации, в том числе персональной» [8].

«Стоит отметить, что и законодательно в России даётся определение цифровой экономики, под ней, в частности, понимают хозяйственную деятельность, в которой ключевым фактором производства являются данные в цифровом виде, обработка больших объемов и использование результатов анализа которых по сравнению с традиционными формами хозяйствования позволяют существенно повысить эффективность различных видов производства, технологий, оборудования, хранения, продажи, доставки товаров и услуг» [55].

Всемирный банк выделяет следующие положительные последствия цифровизации экономики:

- расширение торговли через онлайн-магазины;

- повышение производительности труда за счёт снижение издержек во всех отраслях и сегментах экономики;

- развитие всей системы конкуренции;

- увеличение рабочих мест прежде всего за счёт так называемых маломобильных слоёв населения, таких как инвалиды, жители отдалённых и малодоступных регионов;

- повышение качества услуг, в том числе государственных услуг, когда «взаимодействие с органами публичной власти, в том числе и контролирующими и разрешительными органами сводится к минимуму» [6].

Следует отметить, что в настоящее время ведущие страны мира довольно динамично развивают цифровизацию экономики и цифровую экономику.

Так, например, в Европейском Союзе в настоящее время реализуется план «Цифровая Европа - 2020», согласно которому ожидается, что страны ЕС смогут сэкономить до пяти миллиардов долларов ежегодно.

В разных странах, цифровизация происходит по различным сценариям, законодательно закрепляются правила поведения в цифровой среде. Одним из ярких примеров, является Дания, где граждане обязаны обращаться в государственные органы посредствам Интернета. Практически каждый житель имеет выход в Интернет, где каждый субъект идентифицирован и имеет своего рода электронный паспорт.

«Бизнес, кроме коммуникации, имеет возможность осуществлять все операции через интернет, получать выписки, оплачивать налоги и отправлять отчеты (в электронном виде отправка и получение документов занимает пять минут в сравнении с пятью днями при отправке в бумажном виде») [55].

«Германия планирует к 2030 году полностью перейти к так называемому «интернетизированному производству». При этом, ежегодные инвестиции в технологии должны будут составить не менее 40 миллиардов евро» [24]. На уровне государства создаются отдельные комитеты, отслеживающие развитие и применение цифровой среды в экономике и государственного управления.

В различных отраслях жизни и инфраструктуры внедряются цифровые технологии, что влечет за собой не только удобство для граждан, но и удобство для государственного управления.

В Великобритании так же внедряется полномасштабная цифровизация во всех отраслях жизни, в том числе и в государственном управлении.

«При этом. только в 2016 году данная программа позволила сэкономить более 4,3 миллиарда долларов» [55].

Естественно, все элементы цифровой экономики развиты в США. При этом, ещё в 2009 году в США была утверждена так называемая «Облачная Стратегия».

В США, в структуру министерства торговли включен отдел цифровой экономики. Кроме того, в государственной структуре имеют место быть национальные агентства по информации и телекоммуникации, патентное ведомство и институт технологий и стандартов.

Если говорить про процессы, динамику и перспективы развития цифровой экономики в России, то следует отметить, что в настоящее время Россия не является ведущим фактором в данной сфере развития экономики и общественных отношений.

«На начало 2017 года, то есть на момент разработки основных документов в сфере развития цифровой экономики, Россия занимала 19 место в сфере рейтинга цифровой экономики. уступая даже Мексике и Аргентине» [55].

Но в настоящее время в России признана необходимость развития цифровой экономики. «В частности, в настоящее время принята национальная программа развития цифровой экономики. При этом, фактически условия, ведущих государства мира проецируются и на отечественные проекты» [49].

Так, в частности, обосновываются довольно амбициозные проекты, например:

- «достижение доли домохозяйств, имеющих широкополосный доступ к сети "Интернет» - 97 %;

- доля Российской Федерации в мировом объеме оказания услуг по хранению и обработке данных, проценты - 5 %;

- для социально значимых объектов инфраструктуры, имеющих возможность подключения к широкополосному доступу к сети «Интернет» 100 %» [49].

Вместе с тем, следует признать тот факт, что в процессе реализации принципов и основных направлений цифровой экономики возможны и определённые угрозы.

Обозначим главную угрозу - криминализацию общественных отношений. Так, например, анализируя угрозы цифровой экономики, отечественный законодатель выделяют такие угрозы, как рост киберпреступности. При этом, следует отметить, что и правоохранительные органы зарубежных стран вполне адекватно понимают и верно относятся к данной угрозе. В частности, определяется, что «потери от кибератак, реализуемых посредством компьютерных вирусов, оцениваются в десятки миллиардов долларов. В 2016 г. в мире было совершено около 600 млн. преступлений в цифровой сфере, при этом потери бизнеса составили порядка млрд. долл. США. По данным Microsoft, только в 2017 г. количество киберпреступлений в мире увеличилось в четыре раза» [67].

Мы полагаем, что в настоящее время актуальной задачей для России является как создание правовой основы развития цифровой экономики, в том числе и системы охраны цифровых объектов так и фактическая реализация тех положений, признаков, которые связаны с принципиально новым развитием экономических отношений.

Следует отметить, что «основные направления развития элементов цифрового общества закрепляются и на нормативном уровне. В частности, закрепляются следующие такие направления» [49].

Во-первых, это формирование инновационного пространства с учетом потребностей общества.

Во-вторых, это развитие всей совокупности коммуникативных структур России.

В-третьих, это создание и применение отечественных коммуникативных технологий, обеспечение их конкурентоспособности на мировой арене.

В-четвёртых, это создание новой технологической основы для развития как экономики, так и социальной сферы.

В-пятых, это обеспечение национальных интересов в области цифровой экономики.

Вместе с тем, следует отметить, что становление самого цифрового общества является весьма противоречивым процессом, для которого характерна определённа степень неравномерности, а также сочетание плюсов, достоинств и недостатков.

В частности, можно выделить следующие недостатки, минусы, издержки цифрового общества.

Автор работы уже обращал внимание на то, что сам факт, когда информация становится негативным явлением, фактически возможна угроза безопасности не только в политической, но и в повседневной жизни.

Так, например, В. Бирюков выделяет следующие угрозы, которые могут быть в повседневной жизни. Прежде всего, это утечки информации. Как отмечает автор, по всему миру обнародовано (в СМИ и иных источниках) и зарегистрировано Аналитическим центром InfoWatch 1395 случаев утечки конфиденциальной информации, что на 22% превышает число утечек, зарегистрированных в обычном порядке.

«По данным отчета, по сравнению с прошлым годом число утечек информации в мире выросло на 22%, в России - на 73%» [9].

Основные угрозы в сфере информационной безопасности обозначены и в нормативных актах. Так, например, доктрина информационной безопасности России выделяет следующие угрозы.

Во-первых, это весьма активное использование трансграничной информации для террористических, экстремистках, криминальный, иных незаконных целей.

Во-вторых, это использование глобальных информационных систем рядом стран для реализации военных целей.

В-третьих, это осуществление с помощью информационных технологий технической разведки в отношении предприятий военно-промышленного комплекса России.

В-четвертых, это расширение масштабов использования специальными службами отдельных, конкретных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

В-пятых, особенно негативное влияние такое информационное воздействие оказывает на молодёжь.

В-шестых, различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников.

В-седьмых, резко возрастает количество преступлений в компьютерной сфере, особенно в кредитной сфере, а также в сфере соблюдения тайны частной жизни человека.

В-восьмых, имеется такая тенденция как резкое и очевидное увеличение применения информационных технологий в военно-политических целях, в том числе для совершения действий, которые противоречат нормам международного права.

В-девятых, угрозу безопасности представляют собой и скоординированные компьютерные атаки на объекты информационной инфраструктуры.

В-десятых, авторы Доктрины признают недостаточной эффективным состояние информационной безопасности, как в экономической сфере, таки в сфере науки, технологий.

В-одиннадцатых, «существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети «Интернет», не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими» [72].

Мы полагаем, что и документы в сфере управления информационными технологиями в сфере обеспечения национальной безопасности недостаточное внимание уделяют информационной безопасности относительно жизни и здоровья человека.

Буквально поднимем только одну проблему - влияние Интернета на здоровье и поведение несовершеннолетних. Анализируя реальные сайты в интернете, выделим следующие виды наиболее типичных сайтов, которые представляют угрозу для несовершеннолетних. Сайты, связанные с сексом. Эти сайты, в частности пропагандируют нездоровое сексуальное поведение, то есть секс за деньги, разные извращения, гомосексуализм. Причём, некоторые эти сайты даже не содержат информацию о том, что их могут посещать лица, уже достигшие возраста 18 лет.

Не менее опасны и сайты знакомств, которые, в частности, предлагают знакомство с несовершеннолетними с целью половых отношений.

Сайты, в которых представлены информация, которая способна нанести вред несовершеннолетнему. В частности, к таким сайтам относятся сайты, которые связаны с информированием о способах причинения вреда своему здоровью, о самоубийствах, способах самоубийств.

При этом авторы большинства таких сайтов делают следующие посылки:

- смерть - это самое важное событие в жизни человека (приведена дословная цитата), у смерти есть смысл, у жизни нет;

- ты не один хочешь покончить жизнь самоубийство, давай совершим это вместе;

- лучше умереть молодым;

- решаются все проблемы;

- обосновываются наиболее безболезненные и быстрые способы самоубийства.

Сайты, которые оправдывают противоправное поведение. Такие сайты разнообразны. Есть сайты, которые вообще говорят о производстве оружия и взрывчатых веществ, есть сайты, которые напрямую призывают к преступному насилию, а равно сайты, которые пропагандируют экстремизм и терроризм.

Сайты, которые пропагандируют жестокость, терроризм, экстремизм.

«Вот таких сайтов очень много. Прежде всего, к ним относятся сайты запрещенных за терроризм и экстремизм политических организаций, тоталитарных сект, сайты, которые пропагандируют терроризм и экстремизм, жестокость.

Несколько иные проблемы, издержки выделяет А. Деревянченко, среди которых, в частности, имеют место следующие» [21].

Во-первых, современные способы поиска, восприятия и передачи информации искажают картину мира, делают её более плоской, но в тоже время емкой в информационном плане.

Как следствие, возникает ситуация, когда число людей, с которыми лицо общается дистанционно становится все большим и большим. И при этом число тактильных контактов, которые в классическом обществе являются основными уступят своё место другому виду контактов. На определённом этапе человек начинает воспринимать другого человека как аудиовизуальное животное.

Во-вторых, количество информации увеличивается радикально и перед человеком ставится цель отфильтровать, отредактировать всю эту информацию. Быстро и желательно мало затратным способом. В том случае, если человек неспособен к этому, то фактически человек становится маргиналом в современном обществе.

В-третьих, в настоящее время формируется так называемое «поколение с опущенной головой». То есть поколение, представители которого зациклены только на себе. Это происходит потому, что «цифровое зрение» даёт больше информации об окружающей среде, обществе, чем традиционное, биологическое зрение. При этом, одни мессенджеры постепенно сменяют другие, но смысл все тот же, а именно замена объективной реальности цифровой.

1.2 Понятие и классификация цифровых объектов

Сразу следует отметить, что в рамках доктрины нет единого понимания даже основных терминов, так как «употребляются такие термины, как «цифровые объекты», «цифровые активы», «цифровые права» [1].

При этом и содержание названных категорий понимается по-разному.

Так, например, в рамках первой научной парадигмы обосновывается точка зрения о том, что цифровые объекты полностью отождествляются с информационными носителями.

Под цифровыми объектами автор имеет в виду «объекты Веб, такие как ютуб видео, фейсбук профили, Flickr-картинки (типа кинокадров) и т.д., составляемые из данных и формализуемые посредством схем и онтологий, которые могут быть обобщены как метаданные» [56].

В рамках второй концепции «цифровые объекты полностью отождествляются с цифровыми активами» [42]. «В частности, соответствующий федеральный закон исходит из того, что цифровыми финансовыми активами признаются цифровые права, включающие денежные требования, возможность осуществления прав по эмиссионным ценным бумагам, права участия в капитале непубличного акционерного общества, право требовать передачи эмиссионных ценных бумаг, которые предусмотрены решением о выпуске цифровых финансовых активов в порядке, установленном настоящим Федеральным законом, выпуск, учет и обращение которых возможны только путем внесения (изменения) записей в информационную систему на основе распределенного реестра, а также в иные информационные системы» [74].

При этом, в рамках доктрины обосновываются следующие основные признаки финансовых активов.

Во-первых, это структурирование по определенным параметрам и категориям.

Во-вторых, они фиксируются на определенном цифровом носителе.

В-третьих, это возможность хранить, передавать, использовать, обменивать.

Доктринально обосновывается точка зрения о том, что к цифровым активам относят.

Во-первых, это криптовалюта.

Но здесь сразу возникают определённые проблемы, которые в известной степени возникли после некоторых судебных решений.

Так, например, при признании гражданина банкротом не была учтена информация о наличие у данного гражданина и членов его семьи криптовалюты и электронных кошельков.

«Суды трех инстанций отказали конкурсному кредитору в его требованиях, отметив, что «криптовалюта» не относится к объектам гражданских прав, находится вне правового поля на территории Российской Федерации, исполнение сделок с криптовалютой, ее транзакции не обеспечиваются принудительной силой государства, а отсутствие в системе криптовалюты контролирующего центра, анонимность пользователей криптовалют не позволяет с определенностью установить принадлежность криптовалюты в криптокошельке, находящемся в сети Интернет, конкретному лицу» [51].

В приведенном примере, суды не приняли наличие криптовалюты как доказательства, на том основании, что нет норм, регулирующих данные правоотношения. «Определением Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 28.01.2019 № 306-ЭС18-21814 конкурсному кредитору отказано в передаче кассационной жалобы для рассмотрения в судебном заседании Судебной коллегии по экономическим спорам Верховного Суда Российской Федерации» [46].

Во-вторых, это токены. Как правило, выделяют следующие основные признаки, черты токена:

- именно токены указывают на наличие гражданских прав;

- токены существуют в «блокчейне или иной распределенной системе» [11].

Третьим видом цифровых активов является любой файл, на компьютере. Но как, правило, говорят об аккаунте. И здесь следует обратить внимание на следующий факт законодательство не даётся определение аккаунта.

При этом, следует отметить, что некоторые авторы связывали ликвидацию названного пробела с принятием специального закона, которые регулируют статус цифровых активов. Но, к сожалению, пока такая надежда не оправдалась.

Ну и в рамках третьего подхода «цифровые объекты отождествляются с цифровыми правами. При этом, в известной степени правовой статус цифровых прав закрепляется легально нормами ГК РФ» [16].

Так, например, нормы статьи 128 ГК РФ напрямую закрепляет положение о том, что цифровые права являются объектами гражданских права.

Более чётко понимание цифровых прав обосновывается в статье 141.1 ГК РФ. Здесь, прежде всего, необходимо обратить внимание на следующие основные нормы и формулировки, которые закрепляются законодательно, а именно.

- Цифровыми правами признаются обязательственные иные права, которые определяются такими в соответствии с правилами информационной системы.

- Осуществление, распоряжение, в том числе, например, передача, залог, обеспечение цифрового права возможны только в информационной системе без обращения к третьему лицу;

- В том случае, если иное не предполагается законом, обладателем цифрового права признаётся то лицо, которое имеет возможность распоряжаться названными правами;

Следует отметить, что в принципе в настоящее время разработана типологизация цифровых прав.

Автор выражает мнение о том, что утилитарными цифровыми правами в Федеральном законе от 02.08.2019 № 259-ФЗ «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в

отдельные законодательные акты Российской Федерации» [74] названы следующие:

- право требовать передачи вещей;

- право требовать передачи исключительных прав, прав использования результатов интеллектуальной деятельности;

- право требовать выполнения работ, оказания услуг, если перечисленные права изначально возникли в качестве цифровых на основании договора, заключенного с использованием инвестиционной платформы.

В связи с принятием указанного Закона высказано мнение о том, что утилитарное цифровое право фактически осуществляется в рамках обязательственного правоотношения, как имущественное право. Принятый Закон регулирует отношения коммерческого краудинвестинга.

Некоммерческий краудфандинг, являющийся одним из проявлений шеринговой платформенной экономики, остается вне сферы его правового регулирования, что ограничивает возможность формирования цифровых прав при осуществлении краудфандинговой деятельности вне созданных на основании указанного Закона инвестиционных платформ.

Перечень цифровых прав, которые можно считать цифровыми финансовыми активами, был закреплен в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» [74]. В сущности, данные права отнесены к инвестиционным цифровым правам, при этом они не признаются платежными.

В частности, нормы статьи 3 говорят о том, что в рамках таких цифровых финансовых активах в том числе фиксируется и объём прав, которые фиксируются в рамках финансовых активов.

Кроме того, нормы части 2 статьи 1 Закона определяют следующие виды цифровых прав:

- во-первых, это денежные требования;

- во-вторых, это права на эмиссию ценных бумаг;

- в-третьих, права участия в капитале не публичного акционерного общества;

- в-четвёртых, это право требовать передачи эмиссионных ценных бумаг.

Вместе с тем, следует отметить, что исследователи выявляют и некоторые проблемы, которые касаются модели закрепления цифровых прав.

Так, например, довольно дискуссионным моментом является вопрос можно ли относить информацию к цифровым правам?

Так, например, И. Ающева обосновала точку зрения о том, что «чаще всего цифровые объекты по своей сути представляют собой информацию, записанную на электронном носителе в виде файла, кода, ключа доступа и т.п. При этом указанные объекты имеют определенную стоимость, обладают признаками товарности, оборотоспособности. Сама по себе информация может являться объектом публичных, гражданских и иных правовых отношений» [5].

Таким образом, информация является цифровым правом и объектом гражданских права. И при этом обращается внимание на тот факт, что в прежней редакции ГК РФ информация рассматривалась как объект гражданских прав.

В литературе отмечается, что «информация является благом, имеющим определенный носитель, она способна участвовать в гражданском обороте и быть объектом гражданских правоотношений, иметь механизмы защиты от незаконного использования. В совокупности все эти признаки характеризуют информацию как объект гражданского права» [40].

При этом, в данном случае, исследователь ссылается на Председателя Конституционного Суда РФ В. Зорькина, который выражает мнение о том,

что «под цифровыми правами понимаются права людей на доступ, использование, создание и публикацию цифровых произведений, на доступ и использование компьютеров и иных электронных устройств, а также коммуникационных сетей, в частности к сети Интернет. А также право свободно общаться и выражать мнения в сети и право на неприкосновенность частной информационной сферы, включая право на конфиденциальность, анонимность (обезличенность) его уже оцифрованной персональной информации».

Вместе с тем, обосновывается и прямо противоположная точка зрения о том, что «информацию не следует вносить как объект гражданских прав нормы статьи 128 ГК РФ» [60].

Высказано мнение, что информация, не обладая качеством самостоятельного объекта гражданских прав, относится к результатам интеллектуальной деятельности.

Также отмечается, что информация как объект гражданско-правовых отношений обычно выступает в качестве элемента другого поименованного в ст. 128 ГК РФ объекта, например, таким объектом могут быть базы данных.

Кроме того, есть и ещё одна проблема, а именно следует ли трактовать так называемый искусственный интеллект как проявление цифровых объектов.

При этом также обращается внимание на тот факт, что «законодательно не даётся официальное легальное понимание такого определения как искусственным интеллект» [56].

«Также обратим внимание и на тот факт, что некоторые исследователи вообще ставят вопрос о целесообразности включения цифровых прав в перечень тех объектов гражданских прав, которые поименованы в статье 128 ГК РФ» [35].

«Выделяются и иные проблемы в сфере закрепления цифровых прав:

- полное отсутствие нормативно-правовой базы, определяющей основы деятельности по созданию и сохранению цифрового наследия;

- крайне слабая представленность ряда областей, в которых создание и сохранение цифровых объектов представляются необходимой мерой (охрана памятников археологии, архитектуры и градостроительства, монументального искусства, а также нематериального культурного наследия);

- не разработаны единые механизмы сохранения объектов, изначально созданных в цифровом формате и имеющих культурное значение. Частным случаем здесь является отсутствие системы сохранения культурно значимой информации, функционирующей в сети Интернет. В целом интернет-сайты отличаются нестабильным характером, и масса ныне актуальных данных спустя определенное время может быть безвозвратно потеряна;

- отсутствие принятых на федеральном уровне приемлемых стандартов для сохранения и цифрового представления каждой из разновидностей цифрового наследия.» [68]

Особым видом цифровых объектов является так называемый смарт-контракт.

Сразу следует отметить, что официального легального дефинитивного определения такой категории, как «смарт-контракт» в настоящее время нет.

Что касается определения правовой сущности смарт-контракта, то отметим, что в принципе в рамках доктрины есть точка зрения о том, что под смарт-контрактом следует признать гражданско-правовой договор.

Так, например, А. Савельев выражает точку зрения о том, что «нет никаких препятствий для признания смарт-контракта гражданско-правовым договором» [61].

Точно также, например, В. Камалян выражает мнение о том, что «анализ законодательства показывает, что в целом заключение смарт-контракта как юридически значимого соглашения не противоречит

положениям о сделках и договоре, содержащихся в ГК РФ (гл. 9, гл. 27). Следует также отметить, что смарт-контракт в целом отвечает признакам цифрового документа в его понимании нормами ФЗ «Об информации, информационных технологиях и о защите информации» и п.2 ст.434 ГК РФ [29].

Вместе с тем, конечно, следует отметить, что большинство исследователей не склонны расценивать смарт-контракты как классический пример гражданско-правового договора.

Так, например, А. Юров, координатор рабочей группы Роспатент ВЭБ ВОИР по блокчейну, выражает мнение о том, что «смарт-контракт является примером гражданско-правового договора является чисто умозрительной категорией и практической значимости не имеет, это скорее документ совершение определенных юридически значимых действий, а не классический документ» [65].

Некоторые зарубежные исследователи выражают мнение о том, что «смарт-контракт не является ни обычным контрактом, ни «интеллектуальным (умным)» контрактом, и предлагает другой термин: программные исполняемые транзакции, предполагая, что это не контракт, а программное обеспечение» [41].

Также выражается мнение о том, что смарт – контракт — это компьютерные программы, которые автоматически выполняют условия, согласованные сторонами для регулирования их отношений.

Идея заключается в том, что соглашение является самоподдерживающимся, что делает его модификацию очень сложной. «Если между сторонами возникнет конфликт, потерпевший обратится в суд после ненадлежащего соблюдения или неосновательного обогащения, поскольку смарт-контракт уже был бы выполнен или находится в процессе исполнения» [71].

При этом, следует отметить, что в настоящее время есть несколько законопроектов, которые имеют целью внести определённую ясность в процесс правового регулирования. В частности, проектом Федерального закона № 419059-7 «О цифровых финансовых активах» (ст.2) предложено понятие «смарт-контракта», под которым предлагается понимать договор в электронной форме, исполнение прав и обязательств по которому осуществляется путем совершения в автоматическом порядке цифровых транзакций в распределённом реестре цифровых транзакций в строго определенной таким договором последовательности и при наступлении определенных им обстоятельств» [71]. Но в итоге такое предложение не было принято.

Следует отметить, что исследователи выделяют и определённые особые черты, определенную «специфику смарт-контрактов».

Во-первых, таким признаком является электронный характер.

Во-вторых, обеспечение действия принципа: код — это закон, который нужно создавать по заявке сторон и уже последующих абонентов.

В-третьих, это повышенная уверенность и достоверность. То есть если обычный письменный контракт интерпретируется человеком, который в силу субъективных причин может отшибаться, то, в системе смарт-контрактов формируются электронные ключи, которые сами интерпретируют конкретный договор». [62]

При этом, очевидным преимуществом таких ключей является то, что программирование их является довольно точным, как следствие такой контракт является проверяемым, и будучи зашифрованной соответствующая информация имеет концепцию, которая подтверждает факт того, что договора есть на самом деле и что все условия названного договора согласованны.

В-четвёртых, признаком смарт-контракта кроме всего прочего является ещё и то, что он автономен и самостоятелен. То есть в том случае,

если смарт-договор с помощью соответствующих ключей запущен, то он уже не требует какого-то специального утверждения, но, с другой стороны, он уже и не может быть отменен. То есть ни стороны, ни третьи лица уже не могут влиять на само существования, названного смарт-договор.

При этом, приводится конкретный пример после того, как стороны согласовали конкретный денежный перевод и если он является не однократным, а периодическими задали конкретные параметры, то он будет автоматически осуществляться и в размерах и срок, которая изначально заложена.

В-пятых, это самодостаточность. Сказанное означает, что смарт-контракты функционируют по заданным компьютером программам.

В-шестых, это реализация принципа экономии как денежных средств, так и времени как необходимого ресурса.

Экономия достигается за счет сокращения времени, необходимого для заполнения традиционного контракта, денег, которые должны быть выплачены сотрудникам для выполнения этих задач, избегая будущих затрат за счет уменьшения ошибок и, особенно, отсутствия посредника для проверки и выполнения контракта.

В-седьмых, это безопасность. Смарт-контракты и их данные в соответствующем реестре будут гораздо более безопасными. В частности, сведения не могут быть потеряны, так как при использовании ключа их можно легко восстановить.

1.3. Модели правовой охраны цифровых объектов в законодательстве зарубежных стран

Следует отметить, что очевидной «тенденцией правового регулирования системы общественных отношений в настоящее время в глобальном смысле является тот факт, что регулирование цифровых

объектов и прежде всего, цифровых прав является предметом правового регулирования фактически всех ведущих, развитых стран» [68].

Так, например, в «Великобритании ещё в 2010 году был принят Digital Economy Act 2010» [25]. Данный закон, в частности, регулирует следующие общественные отношения:

- определяет порядок предоставления государственных услуг в цифровом виде;

- названный закон кроме того регулирует все отношения, которые связаны с защитой цифровых прав с использованием защищенных каналов для передачи данных;

- довольно значимым является и то, что в законе регулируется порядок подтверждения как электронных подписей, так и электронных платежей;

- определяется система гарантий прав пользователей Интернета от кражи их персональных данных;

- определяется применение таких мер защиты от публичной информации, такие как использование как фильтр, блокировка цифрового ресурса и т.д.;

- определяется и порядок ограничения использование цифровых ресурсов для торговли определёнными предметами.

«Аналогичный закон действует и во Франции начиная с 2016 года» [26].

При этом, следует обратить внимание на тот факт, что названный закон прежде всего направлен на правовое урегулирование защиты тех цифровых прав, которые так или иначе связаны с авторским правом, с интеллектуальной собственностью.

В рамках доктрины критикуется французская модель закрепления и защиты цифровых прав. В соответствии с законодательством Франции предусматривает обращение граждан в суд за восстановлением своих прав,

однако отсутствуют эффективные механизмы для расследования преступлений, совершенные в киберпространстве.

Практически невозможно отследить цепочку возникновения и распространение незаконного контента. И не представляется возможным выявить лицо, которое совершило противоправные действия в цифровой среде.

Подобная проблема возникает и с деятельность интернет-магазинов, расположенных за границей, которые распространяют запрещенные в гражданском обороте товары. Единственным способом остановить подобную противоправную деятельность, со стороны Франции это блокировка на своей территории подобных сайтов. При этом, государство гарантирует защиту интеллектуальную собственность, однако реализовать такую защиту не в состоянии по многим причинам.

Есть своя специфика правового регулирования названных общественных отношений правовыми актами США. Так, например, был принят такой акт, как «Digital Millennium Copyright Ac» [32]. Данный правовой акт закрепил следующие нормы, правила:

- приравнял правовой статус лиц, которые покупают товары на электронных площадках к правам потребителя;

- создал зашифрованные каналы для защиты платежей и персональных данных;

- вел норму об ответственности за хранение данных;

- отдельно есть глава о так называемом электронном правительстве;

- особое внимание уделяется установлению юридической ответственности за нарушение так называемой целостности персональных данных.

При этом, даже за неумышленную утечку данных уже накладывается штраф, за умышленную наступает уже уголовная ответственность.

В рамках доктрины обосновывается точка зрения о том, что именно США подаёт пример довольно эффективной защиты цифровых прав. При этом приводится пример президентства Д. Трампа, когда на основании указов главы государства были заблокированы китайские сайты, которые как раз допускали утечку персональных данных граждан.

Боле того, некоторые штаты в известной степени принимают революционные предписания. Так, например, в штате «Делавэр был принят закон о наследовании цифровых прав» [63].

В частности, передать по наследству можно аккаунты в социальных сетях и электронную почту. Унаследовать аккаунт в случае смерти или признания своего близкого человека недееспособными могут близкие родственники.

Вместе с тем, следует обратить внимание на тот факт, что в принципе создание организационной структуры по защите цифровых прав равно относительно редкое явления даже в зарубежных странах.

Так, например, «в Германии в 2017 году был создан фонд для защиты цифровых прав. Его основная цель - это укрепление сотрудничества между теми субъектами, кто работает в сфере защиты цифровых прав. Миссия названного фонда заключается в том, чтобы максимально эффективно использовать право на судебную защиту в ситуациях, когда речь идёт о цифровых правах граждан. В настоящее время фонд функционирует как отдельная организация» и фактически основная форма деятельности названной организации – это:

- обмен информацией по всем случаям споров в связи с нарушением цифровых прав граждан;

- поддержка судебных процессов в отношении тех кампаний и физических лиц, которые нарушают цифровые права других граждан» [63].

Глава 2 Основные механизмы и процедуры гражданско-правовой охраны цифровых объектов

2.1 Общая характеристик охраны цифровых прав. Защита прав субъектов смарт-контрактов

Прежде всего следует иметь в виду, что можно выделить две большие группы защиты прав цифровых объектов.

Первая группа - это общегражданские методы и способы защиты прав, которые характерны для всего гражданского права, применимы совершенно к любым общественным отношениям, которые регулируются нормами гражданского права.

Говоря о защите гражданских прав, также следует обратить внимание на доктринальные подходы, в рамках которых термин «защита гражданских прав» разграничиваются на понимание в широком и узком смысле.

По этому вопросу следует согласиться с Е. Сухановым, который, в частности, под «мерами защиты в широком смысле понимает такие меры, как компенсации убытков, взыскание неустойки, а равно компенсации морального вреда».

Все остальные меры Е. Суханов трактует как «меры защиты в узком смысле. Тесная взаимосвязь мер гражданско-правовой защиты и ответственности в действующем гражданском законодательстве позволяет указать на эту концепцию как на наиболее близкую к истине». [19]

Таким образом, в действующем ГК РФ отсутствует легальное определение защиты прав и способов их защиты, что явилось причиной длительной дискуссии ученых-цивилистов. В связи с этим, многими исследователями, обращающимся к тематике осуществления и защиты гражданских прав даны собственные определения этих категорий, которые были нами подробно рассмотрены.

Целями гражданско-правовой защиты являются: пресечение нарушения права, устранение его последствий (в том числе, путем возложения имущественных обременений на нарушителя, понуждения к совершению действия в интересах потерпевшего), предупреждение нарушений права.

Гражданское право является уникальным. Другими отраслями права предусматривается ответственность лица, совершившего правонарушение, а такая категория, как защита нарушенных либо оспоренных субъективных прав выступает в качестве исключительного признака гражданского права.

Классификация гражданско-правовых способов защиты прав имеет важное научное значение в силу того, что является кроме чисто прикладного инструмента ещё и фактором, инструментом, а равно методом научного познания.

Адекватная типологизация позволяет также в большей степени верно и полно осуществить исследование взаимосвязи между элементами все совокупности системы защиты субъективных гражданских прав, что объективно необходимо не только в рамках изучения названных проблем не только на академическом уровне, но и в рамках анализа правоприменительной практики.

Защита гражданских прав имеет две формы: юрисдикционную и не юрисдикционную.

Форма защиты прав представляет собой совокупность тех системных мероприятий, которые имеют в качестве объективных целей защиту субъективных прав и законных интересов, которые закрепляются нормами гражданского законодательства.

Юрисдикционная форма защиты представляет собой деятельность уполномоченных органов по защите нарушенных либо оспариваемых субъективных прав. Ее суть состоит в том, что субъект, чьи права и законные интересы нарушены в результате неправомерных действий, вправе

обратиться за защитой в государственные либо иные компетентные органы, имеющие полномочия по принятию необходимых мер в целях восстановления нарушенного права и пресечения правонарушения.

В соответствии с общим правилом, защита гражданских прав и охраняемых законом интересов производится в судебном порядке. Средством судебной защиты в этом случае выступает иск, представляющий собой требование к суду об отправлении правосудия, с одной стороны, и материально - правовое требование к ответчику о исполнении возложенной на него обязанности либо о признании наличия, либо отсутствия правоотношения, с другой стороны.

Кроме того, что защита гражданских прав тесно связана с иными правовыми явлениями, в частности, с охраной прав и ответственностью. На современном этапе сложились две позиции о соотношении охраны и защиты права.

Не юрисдикционной формой защиты охватываются действия физических и юридических лиц по защите гражданских прав и охраняемых законом интересов, совершаемых ими самостоятельно, без обращения к государственным и иным уполномоченным органам.

Способ защиты нарушенных и (или) оспариваемых прав-это важнейший правовой институт в науке гражданского права. Однако, на законодательном уровне до сих пор не существует единого легального определения данного понятия, что вызывает бурные дискуссии как среди ученых - цивилистов, так и среди правоприменителей.

Большинство авторов рассматривают способы защиты гражданских прав как совокупность тех средств, мер в рамках которых в конечном итоге достигается не просто восстановление прав и законных интересов, но и осуществляется ещё и компенсация тех потерь, которые вызваны нарушением этих прав.

Общий перечень мер закреплен в ст. 12 ГК РФ.

По мнению Т. Шпачевой, «способы защиты гражданских прав-это строго определенные законом меры, посредством которых происходит пресечение (предупреждение) нарушений субъективных гражданских прав». [83].

Ю. Андреев, под «способами защиты прав понимает определенную модель будущего поведения правообладателя, которую он вправе выбрать по собственному усмотрению» [2].

Резюмируя вышесказанное, можно утверждать, что под способом защиты необходимо понимать такие действия, которые способствуют восстановлению нарушенных прав, а также пресечение (предупреждение) нарушений субъективных гражданских прав.

Отечественные специалисты в сфере гражданского права в своих исследованиях определенным образом классифицируют формы и способы защиты гражданских прав.

При этом выделяют сразу несколько оснований типологизации.

Первой типологизацией является типологизация в зависимости от сферы реализации.

Данная типологизация представляется основана именно на тех нормах и правилах, которые закреплены в статье 12 ГК РФ. «Такую типологизацию следует признать наиболее популярной и распространенной в рамках отечественной цивилистики» [20].

В рамках данной типологизации признаётся деление способы защиты гражданских прав на общие, то есть универсальные, а также на специальные. При этом, как правило, те способы, которые закрепляются нормами статьи 12 ГК РФ, как правило трактуются, как универсальные, в то же самое время способы защиты гражданских прав, которые закрепляются в иных статьях ГК РФ трактуются как специальные.

Универсальные способы могут применяться к защите любых субъективных прав. В то же самое время, иные способы защиты, как правило используются для защиты только какого-то одного субъективного права.

Вместе с тем, следует отметить, что в настоящее время данная типологизация подвергается критике, по крайней мере обосновывается точка зрения о том, что такие способы, как, например, признание сделки оспоримой, взыскание неустойки возможны только для обязательственных правоотношений, но не для вещных.

Как следствие, например, С. А. Краснова делает вывод о том, что «деление способов защиты на универсальные и специальные уже не является адекватным» [37].

В связи с этим, на наш взгляд, «классификация мер защиты прав на универсальные и специальные не имеет большой практической значимости, поскольку существо защищаемого права во многом определяет способ защиты. В этом смысле универсальными являются далеко не все способы, закрепленные в ст. 12 ГК РФ (признание права, восстановление положения). В тоже время, классификация по виду защищаемых прав отличается неполнотой, поскольку указывает далеко не все защищаемые права и интересы».[70]

При этом ряд авторов склонны полагать, что «фактически в ходе реализации на практике универсальные методы начинают трансформироваться в специальные методы» [70].

Вторая типологизация способов, форм, методов предполагает зависимость от специфики процессуальных форм осуществления такой деятельности. Это, например, предъявление иска в суд, предъявление претензии, обращение в органы публичной власти, самозащита прав и т.д.

Третьим основанием типологизации можно определить целевую направленность. При этом определенным дефектом это типологизации

является тот факт, что разные авторы по-разному трактуют виды методов защиты гражданских прав в рамках этой типологизации.

Так, например, А.П. Вершинин выделяет такие «способы защиты гражданских права, как пресекательные, восстановительные и штрафные» [13].

В то же самое время, например, Б.Е. Осипов выделяет такие методы, как «регулятивные, охранительные, предупредительные» [47].

В свою очередь А.А. Павлов полагает, что «наиболее адекватным является выделение восстановительных, превентивных, пресекательных методов защиты гражданских прав» [48].

Следующим основанием типологизации может быть специфика результатов применения тех или иных методов защиты. С этой точки зрения можно выделить следующие виды методов:

- методы подтверждения права, прекращения, изменения обязанности. К таким методам, прежде всего, относят признание права; прекращение или изменение правоотношений. К таким методам, также следует отнести и присуждение к исполнению обязанности в натуре;

- методы предупреждения, пресечения правонарушения. Как правило, к таким методам относится взыскание неустойки;

- методы восстановления нарушенного права. К таким методам прежде всего, целесообразно отнести, например, возмещение убытков, а равно компенсацию морального вреда.

И наконец пятым основанием классификации является вид тех прав, которые подлежат защите в рамках гражданского права. В рамках такой типологизации следует выделить 4 типа методов защиты гражданских прав:

- методы защиты вещных прав. К методам защиты относят те, которые не предусматривают лишение собственности;

- методы защиты обязательственных прав. Истребование налогов или процентов за пользование;

- методы защиты исключительных прав. К таким методам относится, например, заключение лицензионных договоров;

- методы защиты корпоративных прав. К таким методам относят, например, признание недействительным решение собрания акционеров, совета директоров и т.д.

Мы полагаем, что признаками, свойствами защиты гражданских прав являются:

- закрепление таких способов именно нормами закона. Фактически именно так можно трактовать статью 12 ГК РФ;

- принудительный характер соответствующей процедуры [16].

Все эти методы применимы относительно защиты цифровых объектов. Но есть и определённая специфика. В частности, выделяются специфические «способы защиты таких объектов» [69].

Во-первых, это защита прав обладателей токенов, как владельцев корпоративных ценных бумаг. «Как отмечается доктринально, в этом случае применимы те способы защиты прав, которые предусмотрены для владельцев корпоративных или иных ценных бумаг» [69]. Здесь, в частности, обращается внимание на опыт США, когда Калифорнийский суд применил правила по отношению к токену Tezos аналогично тем правилам, которые применяются к способам устранения нарушений при осуществлении выпуска и размещения корпоративных ценных бумаг.

Во-вторых, это возможность признания сделки недействительной, прежде всего, касающейся первичного размещения токенов, которая совершена под влиянием заблуждения, обмана, так как в процессе ICO подлежит обязательное декларирование цель аккумулирования соответствующих средств, другого имущества, а также средства достижения названной цели.

Владельцы токенов могут требовать возмещения убытков или признать такую сделку недействительной в силу отказа в предоставлении

такой информации или её искажении в том случае, если они приобрели такие токены под влиянием заблуждения.

В этом примере ICO признается в конкретной национальной юрисдикции как совершение сделки (транзакции), для применения, например, ст. 178 Гражданского кодекса РФ (ГК РФ). Таким образом, в соответствии со статьей 128 ГК РФ, токен должен рассматриваться в качестве понятия «имущество» и соответствовать ему.

В-третьих, это защита прав, которые возникают из договорных обязательств при нарушении условий договора. Данный способ защиты возможен при передаче прав на токены, которые оформляются в виде купли-продажи или дарения.

Условия данной операции предусматриваются правами владельца токена по обязательству. Если происходит нарушение договорных условий, то на помощь приходит имущественная ответственность сторон.

В-четвёртых, это защита прав при нарушении прав потребителей или правил рекламы. Данная форма ответственности наступает только при социальной рекламе в социальных сетях.

При этом, например, нормы статей 12 и 13 Закона РФ «О рекламе» говорят о том, что «мошеннические, а равно ложные, вводящие в заблуждение сведения, нечестное поведение лица, которое осуществило выпуск токена влечет за собой ответственность в рамках гражданского законодательства» [75].

В-пятых, это ответственность фидуциарная, которая распространяется на должностных лиц или агрегаторов за злоупотребление доверием или причиняющими ущерб при размещении токенов. Сюда же автор относит халатное поведение при защите имущественных прав и законных интересов владельцев токенов.

В-шестых, это ответственность в сфере обеспечения безопасности так называемой критической информационной инфраструктуры.

Так, в статье 2 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» «безопасность критической информационной инфраструктуры определяется как состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак» [73].

При этом, к объектам критической информационной инфраструктуры относят следующие объекты:

- во-первых, это информационные системы;

- во-вторых, к таким объектам относятся также информационно-телекоммуникационные сети;

- в-третьих, это комплекс программных и программно-аппаратных средств;

- в-четвёртых, это средства для управления всем названным выше оборудованием.

Специальное внимание в рамках доктрины уделяется и вопросам «охраны, сохранения культурных цифровых ресурсов» [68].

Во-первых, это четкое применение норм гражданского законодательства, при необходимости совершенствование предписаний норм права.

Во-вторых, это создание и совершенствование системы программного обеспечения.

В-третьих, это разработка и реализации как общероссийских, так и региональных программ охраны цифровых культурных объектов.

В-четвертых, это совершенствование системы электронного архивирования.

В-пятых, это совершенствование образовательных практик, связанных с обучением и переобучением специалистов, занятых деятельностью, направленной на сохранение цифрового наследия.

В тоже самое время особое внимание уделяется и проблемам защиты субъектов смарт-контрактов. Вместе с тем, есть и специфика защиты прав субъектов данного контракта.

В частности, следует выделить следующие специфические методы такого контракта. При этом следует отметить один довольно существенный момент — это защита так называемой «слабой» стороны смарт-контракта. Такой контракт представляет дополнительные способы защиты прав потребителей.

В частности, речь идет о том, что в настоящее время смарт-контракты могут предоставить потребителю дополнительные способы защиты прав в части разрешения соответствующих конфликтов с продавцом т.д.

Как отмечается в рамках доктрины, потребители не могут повлиять на изменение договора или заключать ли такой договор вообще. Вместе с тем, определенность является важным фактом экономической деятельности и принципом действия права.

Таким образом, важнейшей гарантией прав человека в сфере смарт-контрактов становится реализация принцип добросовестности.

Также следует отметить, что такая гарантия прав человека в смарт-контрактах, как судебная защита ещё не сложилась в достаточной степени. В связи с этим предположить, как суды будут использовать (или вообще отрицать возможность их применения) принципы гражданского права в данных ситуациях, сложно. Однако проанализированные нами материалы зарубежной судебной практики позволяют говорить о том, что основополагающие начала регулирования гражданских отношений далеко не всегда противоречат правилам о смарт-контракта.

По крайне мере, суды исходят из принципа абсолютного характера в принцип защиты пора в потребителей в рамках-смарт контрактов. В частности, суды исходят из положения о том, что «использование веб-сайта для заключения договора без явного уведомления об условиях

использования, которые были просто размещены на домашней странице, также считается недостаточным принятием этих условий, особенно если стороной договора является потребитель» [71].

«Смарт-контракт в самом общем виде можно определить как запрограммированный договор, его условия прописаны в программном коде, и он автоматически исполняется с помощью блокчейна. Смарт-контракты базируются на компьютерном протоколе, который по установленным правилам посылает или получает определенную информацию или изменяет данные. Основанием является заложенный в протоколе программный код. При этом применяются простые правила «если, то»: «если» определенное условие будет исполнено, «то» будет совершено определенное действие» [87].

«Примером самого примитивного смарт-контракта может служить торговый автомат, который запрограммирован на то, что в случае, если выбран определенный товар и помещено определенное количество денежных средств, автомат в ответ выдаст сдачу и сам товар» [94].

«В смарт-контракте, основанном на технологии блокчейн, формулируются условия контракта на языке программирования, после чего смарт-контракт обычно переносится на блокчейн. Такой контракт исполняется автоматически без участия исполнителя (продавца, подрядчика, исполнителя по договору возмездного оказания услуги и т.п.) при соблюдении заранее определенных условий. Кроме того, программа такого контракта должна быть защищена от несанкционированного изменения его внутренней логики, чтобы сторона договора не могла намеренно препятствовать исполнению смарт-контракта или незаконно изменять его содержание» [17].

Сложность заключается в том, что при регулировании смарт-контрактов применяются уже существующие нормы гражданского права, в

то время как новых норм, конкретизирующие данный вид отношений в законодательстве не закреплено.

Обширной правоприменительной практики в России пока не образовалось в связи слабой распространённостью данных смарт-контрактов. За рубежом, при правоприменительной практике, выявляется минимум противоречий. «Например, сложно представить, по какой причине нормы о защите прав потребителя действительно не должны применяться в данной ситуации, если смарт-контракт соответствует критериям потребительского договора» [17].

«В частности, уже давно сложилась практика признания заключенными и действительными соглашений «click-wrap», по которым потребители на каком-либо сайте нажимают специальную кнопку «принимаю соглашение» (cM.: Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1150 (7th Cir. 1997)). При этом в некоторых ситуациях при определении того, было ли соглашение, суды внимательно изучали вопрос о том, получил ли потребитель уведомление об условиях договора, прежде чем согласиться с ним (cM.: Inc. v. Verio, Inc., 356 F.3d 393, 403 (2d Cir. 2004))» [17].

Судами устанавливается условия договора, при этом учитывается предшествующая практика в данной отрасли.

Делая промежуточный вывод, следует отметить, что защита сторон смарт-контрактов будет основываться на основополагающих принципах и принципах гражданского права, иначе, таким пробелом могут воспользоваться недобросовестные участники рынка.

2.2. Охрана права на цифровую информацию

В России правовой основой защиты такой информации являются следующие нормативно-правовые акты:

- ФЗ «Об информации, информационных технологиях и защите информации» [77];

- ФЗ «О персональных данных» [78];

- статья 152.2 ГК РФ – «Охрана частной жизни гражданина».

При этом, законы, а равно подзаконные акты выделяют 3 категории персональных данных.

Во-первых, это информация, которая относится прямо или косвенно к определенному физическому лицу, например, такая информация, как фамилия, имя, отчество, дата рождения, место рождения, адрес, семейное положение, образование, профессия, доходы и т.д.

Во-вторых, это специальная категория информации, то есть расовая, национальная принадлежность, политические, религиозные, философские взгляды, состояние здоровья, личная жизнь.

В-третьих, это биометрические персональные данные, то есть сведения, которые характеризуют физиологические и биологические особенности человека, на основе которых можно установить его личность.

Сразу отметим, что законодательно такое определение не даётся ясно ни в рамках закона, ни в рамках подзаконных актах общего действия.

Вместе с тем как отмечают исследователи, «сами отечественные суды занимают относительно консервативную позицию относительно понимания того, что именно понимать под персональными сведениями» [43].

Во-первых, это фамилия, имя, отчество лица, размер задолженности по оплате коммунальных услуг.

Во-вторых, это дата и место рождения, адрес места регистрации и фактического проживания, номера рабочего и мобильного телефонов и номер паспорта, а также дата его выдачи и наименование органа, выдавшего паспорт, сведения о работе, супруге и детях, датах их рождения, указанные в заявлении-анкете на получение потребительского кредита.

В-третьих, это копии материалов пенсионного дела.

В-четвёртых, это те данные, которые содержатся в техническом паспорте на жилое помещение.

В-пятых, это сведения о пересечении Государственной границы РФ.

В-шестых, это данные трудового договора.

Следует отметить, что отечественное законодательство меняется именно в аспекте защиты права персональных данных именно в рамках цифровых общественных отношений.

Так, в 2013 году в ФЗ «О персональных данных» были внесены определенные изменения, на основании которых, в частности, была установлена обязанность оператора локализовать базы данных, которые могут содержать персональные данные россиян.

При этом, на практике согласно данным Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций, каждая вторая проверка оператора выявляет нарушения. К примеру, «в 2019 г. по результатам проведения 195 мероприятий выявлено отсутствие в поручении лицу, которому оператором доверяется обработка персональных данных, обязанности соблюдения конфиденциальности персональных данных и обеспечения их безопасности» [84].

С развитием цифровых технологий право на защиту персональных данных порождает новые права. Поскольку Интернет существенно облегчает нарушения прав человека, законодательству необходимо адаптироваться к новым условиям. Если раньше одним из способов защиты персональных данных было опубликование опровержения информации в газетах, то теперь все чаще речь идет об удалении информации, распространенной посредством Интернета, что вряд ли достижимо с учетом молниеносного и практически бесконтрольного копирования информации в сети. Юридическим ответом на создавшуюся ситуацию стало право на забвение, которое рассматривается как право на уважение в цифровом пространстве.

При этом, возможны «следующие конфликты, которые связаны с защитой права на персональные данные» [50].

Во-первых, это защита персональных данных и публичный интерес. «Такой конфликт можно рассматривать как частный случай проявления общего конфликта публичного и частного права, поскольку публичный интерес предполагает специфическое видение проблемы глазами самого общества» [54].

Например, «согласие самого гражданина на трансграничную передачу соответствующих сведений, информации не предусмотрено, что нарушает нормы статей 23 и 29 Конституции РФ» [36].

Во-вторых, это защита персональных данных и информация ограниченного доступа. «Персональные данные и информация ограниченного доступа - это пересекающиеся понятия. При этом уже в самой постановке вопроса очевиден конфликт, который получил своё рассмотрение Конституционным Судом РФ» [44].

Конституционный Суд указал, что оспариваемое законоположение позволяет хранить информацию о состоянии здоровья граждан исключительно в целях реализации их права на охрану здоровья и медицинскую помощь, при этом конфиденциальность персональных данных обеспечивается врачебной тайной, поэтому оно не может рассматриваться как нарушающее конституционные права заявителя.

То есть высший орган конституционного контроля исходит из того, что персональные данные охватывают такое понимание как врачебная тайна и поэтому дополнительная обязанность уничтожения таких данных излишня.

Вот ещё одна позиция КС РФ, относительно данных предварительного расследования.

«В материалах уголовного дела могут содержаться сведения, прямо или косвенно относящиеся к охраняемой законом тайне (персональные

данные, налоговая, банковская, коммерческая, медицинская тайна, тайна усыновления и др.), а потому их несанкционированное распространение (разглашение) следует рассматривать как посягающее на права личности и тем самым представляющее общественную опасность» (абз. 4 п. 3.1 мотивировочной части решения) [45].

Третье противоречие - это защита персональных данных. Как правило, в литературе обосновывается мнение, что лицо должно дать информированное согласие на их обработку.

Но такое согласие предполагает принятие субъектом персональных данных принятие ряда дискретных решений на стадии сбора персональных данных. Но невозможно на этой стадии предугадать всю возможную совокупность таких сведений.

Четвёртый конфликт — это противоречие между защитой персональных данных и нейтральностью Интернета.

Нейтральность Интернета (сетевой нейтралитет) один из базовых принципов данной технологии, означающий обеспечение равной скорости доступа к любым веб-сайтам независимо от их контента, без каких-либо приоритетов и привилегий. Наиболее очевидно этот конфликт проявляется в связи с распространением так называемых фейковых новостей, а также устаревшей информации, что, конечно же, не может не затрагивать персональные данные.

И последнее противоречие — это противоречие между защитой персональных данных и другими правами человека.

При этом, ВС РФ, руководствуясь в том числе и нормами международного права определил следующие факторы, которые подлежат учету:

- представляет ли дискуссия общественный интерес;
- идет ли речь о публичной фигуре и на сколько она известна;
- была ли информация достоверной;

- каковы были форма, последствия публикации;

- были ли серьезные наказания.

Выработанные судебной практикой позиции в отношении защиты частной жизни, как правило, применимы и к защите персональных данных. При этом многое зависит от того, идет ли речь о публичном лице (пристальное внимание к поведению которого является необходимым атрибутом демократического общества), либо о сугубо частном лице, к защите персональных данных последнего государство должно подходить с особой тщательностью.

2.3. Охрана объектов авторского права, выраженных в цифровой форме

Прежде всего, следует отметить, что «в сфере охраны авторских прав» действует норма статьи 2 Бернской конвенции «Об охране литературных и художественных произведений» [7]. При этом, названное определение охватывает все произведения в области литературы, науки, искусства, в какой бы именно форме они не выражались.

Одновременно, нормы пункта 3 статьи 1259 ГК РФ закрепляют положение о том, что названные «произведения могут быть выражены в любой форме и при этом приводятся примерные формы» [17]:

- письменная форма;

- устная форма;

- форма изображения;

- форма звука или видео записи;

- объёмно-пространственная форма.

Таким образом, в названном перечне отсутствует такая форма, как форма цифрового объекта. Но, конечно, возникает вопрос перевода

произведений в цифровые формы. И при этом, обосновываются определенные подходы к пониманию произведений в цифровых формах.

Так, например, Я.А. Карев обосновал точку зрения о том, что «отличие электронного документа от документа, составляемого на бумажном носителе (далее - бумажный документ), заключается в особенностях его формы» [31]. При этом, обосновывается мнение о том, что эта разница является весьма существенной.

Вместе с тем, некоторые исследователи напротив «обосновывают мнение о том, что такая разница в формах не является существенной» [10]. Но, естественно, фактически такие различия, конечно, есть. «При этом, выделяют следующие такие различия» [56].

Во-первых, если цифровой объект помещён в Интернет, он становится открытой информацией и доступ к такой информации получает неограниченный круг лиц.

Во-вторых, произведение, которое выражено в цифровой форме оторвано от материального носителя.

В-третьих, существенным отличием является и отличие по таким показателям, как тиражи и количество изданных экземпляров.

В-четвёртых, в отличии от других произведений в том случае, если произведение выражено в цифровой форме, то не всегда возможно разграничить оригинал и копию.

В-пятых, это максимально высокая скорость распространения соответствующих материалов в Интернете.

При этом, следует отметить, что в России сферу защиты авторских прав в сфере цифровых объектов регулируют нормы ГК РФ, ГПК РФ, КОАП РФ.

Также, многие исследователи обращают внимание также и на тот факт, что в 2013 г. был принят ФЗ от 2 июля 2013 г. № 187-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации по

вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях», именуемый в СМИ как «Антипиратский» закон» [73].

Изначально, объектом правовой защиты названного закона были видеофильмы, телефильмы, кинофильмы. Но уже с 2015 года список объектов, которым была предоставлена защита, расширился фактически и стал распространяется на такие объекты, как компьютерные программы, музыкальные произведения, литературные произведения и т.д.

Действие антипиратского закона применимо в случае незаконного размещения на сайтах в сети Интернет без согласия автора тех объектов, которые охраняются авторским правом. При этом, в данном случае имеет место так называемый запрещенный или нелегальный контент.

При этом, некоторые исследователи относят к особой группе объекты авторских прав «гиперссылки на ресурсы» [56], но большинство авторов все же воздерживаются от такой трактовки.

Нормы статьи 15.7 ФЗ «Об информации, информационных технологиях и защите информации» предусматривают досудебную процедуру взаимодействия в случае выявления правообладателя названного произведения, размешенного без согласия такого правообладателя.

Инициатором проведения такой процедуры может быть сам правообладатель, или уполномоченное им лицо, а также лицензиат по договору о предоставлении исключительной лицензии. Именно они в случае нарушения авторских прав правообладателя вправе направить в адрес владельца сайта, на котором размещено соответствующее авторское произведение, заявление о нарушении своих прав. Адресатом заявления должен быть только владелец сайта, на котором расположен нелегальный контент. Заявление может быть подано как в письменной, так и в электронной форме. При этом, как правило, в заявлении указывается просьба удалить соответствующий контент.

Вместе с тем, как отмечается, доктринально в досудебном порядке, такая процедура осуществляется крайне редко, что переводит отношения сторон в сферу судебного разбирательства.

При этом, возникает вопрос в какой именно суд следует обратиться для разрешения названных споров.

По смыслу статей 22 и 26 ГПК РФ [18] и ст. 27 и 28 АПК РФ [3] споры, связанные с защитой авторских прав, с участием авторов при нарушении личных неимущественных прав подлежат рассмотрению в судах общей юрисдикции.

Так, нормы части 3 статьи 26 ГПК РФ закрепляют положение о том, что именно Московскому городскому суду подсудны «в качестве суда первой инстанции гражданские дела, связанные с защитой авторских и (или) смежных прав, кроме прав на фотографические произведения и произведения, полученные способами, аналогичными фотографии, в информационно-телекоммуникационных сетях, в том числе в сети Интернет, и по которым им приняты предварительные обеспечительные меры в соответствии со ст. 144.1 Кодекса» [18].

То есть, казалось бы, все споры по нелегальному контенту решает именно Московский городской суд. Но если только заявлено о применении обеспечительных мер. Если нет таких требований, то действует общие правила подсудности гражданских споров [59].

Кроме того, следует иметь в виду, что на основании «статьи 33 АПК дела по спорам о защите прав интеллектуальной собственности рассматриваются именно арбитражными судами. При этом, Пленум ВАС РФ в своё время принял разъяснения, согласно которой не имеет значения, выступает ли такая организация от имени правообладателя или от своего имени; является ли правообладатель юридическим лицом, гражданином, зарегистрированным в качестве предпринимателя или незарегистрированным [52].

Глава 3. Проблемы в сфере охраны цифровых объектов

3.1. Проблемы законодательства и правоприменительной деятельности в сфере охраны цифровых объектов

Информационные ресурсы, имеющие нелегальный контент подлежат блокировке, данный механизм является защитой авторских прав цифровых объектов, закрепленный на законодательном уровне.

Такая процедура довольно подробно регламентируется «приказом Роскомнадзора от 12.08.2013», и данная процедура включает следующие этапы:

- инициирует процесс блокировки правообладатель. При этом, уже отмечалось, что возможна как письменная, так и электронная форма такого обращения;

- при этом, нормы статьи 144.1 ГПК РФ закрепляют нормы об обеспечительных мерах, которые в данном случае могут быть реализованы, а именно:

а) после рассмотрения фактических материалов дела может быть вынесено решение о блокировке сайта;

б) в случае, когда нелегальный контент все же остается на сайте, то Роскомнадзор может потребовать от оператора ограничение доступа и изменения в доменном имени.

При этом с 2015 года действует положение, которое создает дополнительные гарантии авторских прав, а именно если был обнаружен факт систематического нарушения авторских прав на платформе интернет, то блокировка возможна без инициативы соответствующего управомоченного лица [58]. Кроме того, создается ещё и такая гарантия, как «вечная» блокировка [56].

Многие авторы обозначают проблему относительно ответственности информационного посредника за нарушения авторских прав и применения пункта 1 статьи 1253.1 ГКРФ, в соответствии с которой информационный посредник несет ответственность

В пункте 3 ст. 1253.1 ГК РФ предусмотрено, что одним из условий освобождения информационного посредника от ответственности является принятие им необходимых и достаточных мер для прекращения нарушения. Возникает вопрос, какие меры считать таковыми?

Правоприменительная практика и выявляет некоторые условия, при которых возникает возможность незаконного размещения объектов авторского права:

- для аудиодорожки, принадлежащая правообладателю, возможно отключение звука;

- блокировка воспроизведения видео;

- добавление рекламы в ролик, при этом доход о рекламы делится между правообладателем и тем лицом, которое загрузило ролик.

«Ещё одним из довольно интересных способов является и так называемый «цифровой отпечаток». Его использование приводит к тому, что при загрузке на сайт файлов произведений, в отношении которых уже поступали жалобы правообладателей, их скачивание будет невозможно: при попытке скачать такой файл появляется сообщение о том, что он удалён по требованию правообладателя» [14].

Одновременно, есть смысл установить, как гражданскую, так и административную ответственность за попытку обойти блокировку нелегального контента.

Самым распространенным режимом охраны цифровых объектов является охрана нормами авторского права. Так, рассмотрим проблемы сфере охраны цифровых объектов на примере ЭВМ. В соответствии с нормами Гражданского кодекса РФ, так и Бернской Конвенции по охране

литературных и художественных произведений (ст. 2) на программы для ЭВМ распространяется режим авторского права. В частности, в соответствии с ГК РФ на программы для ЭВМ распространяется режим охраны литературных произведений. Такое приравнивание программ для ЭВМ к произведениям литературы, как представляется, все же не вполне учитывает особую технологическую и функциональную природу программ для ЭВМ.

«Учитывая, что процессы цифровизации проникают абсолютно во все сферы социальных отношений, в современной литературе в качестве относительно обособленной группы прав человека все чаще выделяют «цифровые» права, под которыми понимают права человека, связанные с использованием современных цифровых технологий и функционированием в цифровой среде» [13].

Одним из часто используемых «цифровым» правом является доступ в интернет. Данный способ может осуществляться свободно, может сопровождаться некоторыми ограничениями, выражающиеся в отношении определенной инфраструктуры, где необходимо предоставить согласие на обработку персональных данных. В последнем случае, только индивид решает, воспользоваться ему сервисом или нет. Так как предоставленные данные могут быть использованы в результате кибератаки на сервер организации. Главной проблемой не только личностного характера, но и на мировом, межгосударственной, является сбор и хранение информации, а при цифровизации мы все становимся, помимо воли, участниками информационного обмена. Современные технологии позволяют весьма быстро обрабатывать колоссальные объёмы информации. Не исключено и недобросовестное использование предоставляемых данных в сети Интернет. Это может выражаться в навязывании рекламы, путем отслеженных предпочтений конкретного человека. При этом, происходящее имеет своей целью лишь получение прибыли.

«В то же время все чаще имеют место факты использования таких данных в криминальных целях, при совершении, прежде всего, корыстных преступлений, связанных с хищением денежных средств, находящихся на банковских счетах граждан, обслуживаемых электронным способом. Так, согласно экспертным данным, только за 2021 г. ущерб от так называемых «киберпреступлений» составил 90 млрд рублей» [88].

Кроме того, выявляются нарушения не только имущественных прав человека, но и для иных правонарушений, таких как неприкосновенность частной жизни, посягательства на половую неприкосновенность в отношении несовершеннолетних и деятельность преступных сообществ.

Регулятивная функция государства не может остановить цифровизацию и обмен информации, равно как и моментально пресекать незаконную деятельность в цифровом поле. В связи с этим, необходимо на государственном уровне вырабатывать направление правовых и политических мер по противодействию цифровой дискриминации.

«Обоснованные опасения вызывают и процессы так называемой «уберизации» (от наименования фирмы “Uber”) экономики, которые состоят в том, что работник, который с точки зрения трудового законодательства выступает в роли свободного агента, самозанятого, вступает в фактические трудовые отношения не с конкретным работодателем, а с определенной цифровой платформой, которая, по существу, выступает лишь информационным посредником между заказчиками и поставщиками услуг. Подобная система создает колоссальные риски нарушения трудовых прав граждан, по сути, полностью лишая работников, вовлеченных в подобные экономические отношения, социальных гарантий, предусмотренных трудовым законодательством» [40].

Резюмируя вышеизложенное, следует подчеркнуть, что необходимое вмешательство государства в регулятивную функцию цифровой среды, и как следствие внесение новых норм в гражданское законодательство, влечет за

собой и изменения в трудовое законодательство. Поскольку работники также являются участниками цифровой среды и их трудовые функции связаны с обработкой данных.

Кроме того, следует упомянуть о цифровом документообороте, занявший практически весь спектр в данной сфере. В обозримом будущем возможен полный отказ от документов в бумажном носителе. Однако для такого развития событий необходима безопасная цифровая среда, в рамках которой должна быть установлена такая высоко технологичная защита, гарантирующая полную безопасность. Создание такой безопасной цифровой среды продиктовано необходимостью защитить все растущие объемы информации. Используемое программное обеспечение не обеспечивает защиту и сохранность информации. Так как, на сегодняшний день, такая информация подвергается легкому тиражированию и системы не приспособлены для длительного хранения информации.

«Существующие физические носители цифровой информации крайне недолговечны и редко служат дольше 10-15 лет, в то время как программы обработки и хранения информации обновляются еще быстрее. Что же касается «облачных» технологий, за которыми, безусловно, будущее, то и они в настоящее время далеко несовершенны. При этом, с учетом складывающейся в последнее время геополитической обстановкой следует учитывать, что подавляющее большинство датацентров, обеспечивающих хранение таких данных, расположены за пределами нашей страны, что, в случае неблагоприятного развития международной обстановки, может привести к полной утрате доступа к ним российских обладателей и пользователей хранящейся в них информации» [40].

На основании этого, учеными и общественностью предлагается сохранить гибридный способ сохранения информации и сегодня сложно отказать полностью от бумажных носителей в документообороте.

Кроме того, в современных острых внешнеполитических условиях и внешнего воздействия на нашу страну посредствам санкций поднимается проблема цифрового суверенитета. Который должен обеспечить не только цифровую независимость государства, выражающаяся в приоритете интересов государства и граждан. Созрела необходимость создавать собственную цифровую инфраструктуру, безопасность.

«В качестве необходимых средств достижения такого рода суверенитета может быть рекомендовано создание соответствующих регулятивных механизмов, прежде всего, национальных технических стандартов и специального правового режима, создание и использование защищенных от внешнего воздействия аппаратных и программных средств связи отечественного производства, в том числе создание отечественной системы дата-центров, а также способов доведения информации до конечного потребителя, государственно-частное партнерство, которое особенно важно для контроля над сбором, обработкой, хранением и использованием больших массивов данных отечественных пользователей. Кроме того, важнейшей составляющей цифрового суверенитета государства, который бы обеспечивал соблюдение соответствующих прав российских граждан, должно стать создание эффективного механизма «очистки» внутренней виртуальной среды от нежелательной или вредоносной информации, а также инструментов противодействия интегрированным в импортируемый информационный продукт враждебным социально-политическим, историческим, религиозным, нравственно-культурным и другим идеологическим установкам» [77].

Следует так же отметить, что влияние, оказываемое транснациональными компаниями весьма внушительно и это может выражаться не только влиянием на экономику, но и на идеологию целых государств.

«Так, крупнейшие зарубежные глобальные цифровые платформы и социальные сети, оперирующие в нашей стране, – Google, Meta** (признана в России экстремистской организацией и запрещена) (Facebook* (социальная сеть, признанная экстремистской и запрещенная на территории Российской Федерации)), Twitter, Instagram* (социальная сеть, признанная экстремистской и запрещенная на территории Российской Федерации), TikTok, YouTube все чаще становятся инструментом деструктивного идеологического воздействия на российских граждан, доведения до них недостоверной информации, а также дискредитации нашей страны и ее граждан в глазах мирового сообщества» [40].

Рассматриваемый случай и является прямым посягательством на цифровой суверенитет. Ответ должен быть быстрым и адекватным, реализуемый на законодательном уровне.

«Так, в ответ на беспрецедентные действия компания Meta** (признана в России экстремистской организацией и запрещена), которая в свете проводимой Российской Федерацией специальной военной операции в связи с ситуацией в Луганской Народной Республике и Донецкой Народной Республике разрешила призывы к насилию в социальных сетях Facebook* и Instagram* (социальные сети, признанные экстремистскими и запрещенные на территории Российской Федерации) в отношении российских граждан, Роскомнадзор принял решение об ограничении доступа к социальной сети Instagram* (социальная сеть, признанная экстремистской и запрещенная на территории Российской Федерации)» [48].

Такие меры, несомненно, ограничили цифровые права граждан, но являются необходимыми, для обеспечения безопасности, а в современных условиях такие меры будут системными. В соответствии с данными условиями, законодательство, в свою очередь, должно своевременно реагировать на новые меры охраны цифровой среды государства.

Необходимо установить исчерпывающий перечень мер, направленных на безопасность гражданина и государства.

3.2. Основные направления совершенствования законодательства в сфере охраны цифровых объектов

Субъект, обладающий интеллектуальным потенциалом и способный его реализовать, положительно влияет на благосостояние государства. В свою очередь государство должно обеспечить защиту результатов интеллектуальной деятельности субъекта, сохранив за ним исключительное право на интеллектуальную собственность.

Развитие человечества невозможно без прогресса, обеспечивающегося результатами интеллектуальной деятельности граждан. Созданные инновации непременно воздействуют на науку, культуру, технологии и технику.

Результаты интеллектуальной деятельности сопровождаются умственным трудом различных специалистов. Поскольку специалисты - это кадры высокой квалификации, то необходимы финансовые ресурсы. Отсюда возникает необходимость регулирования имущественных и неимущественных прав и обязанностей на законодательном уровне. Кроме национального законодательства, данный вид отношений регулируется международными соглашениями и актами. Имущественные права включают в себя право на вознаграждение, право на монопольную коммерческую реализацию результатов интеллектуальной деятельности. Рассматривая отдельно неимущественные права следует выделять авторское право, право на защиту результатов интеллектуальной деятельности и право на название. Однако следует учесть то правило, что неимущественные права действуют по умолчанию с момента оформления авторства. Имущественные права,

напротив, требуют официального оформления авторства или исключительных прав.

На современном этапе развития экономики и социальной составляющей требует от субъектов определенного оформления результатов интеллектуальной деятельности в вид интеллектуальной собственности.

В Конституции Российской Федерации закреплена норма об охране интеллектуальной собственности, но не раскрывается само понятие и не дано четкое определение, равно, как и в большинстве других западных странах. Но в Гражданском Кодексе Российской Федерации определена юридическая природа термина «интеллектуальная собственность» и представлена, как список результат интеллектуальной деятельности и приравненных к ним средств индивидуализации. На основании ст. 1225 части четвертой Гражданского Кодекса Российской Федерации гарантируется правовая защита.

«По определению Всемирной организации Интеллектуальной Собственности «в самом широком смысле интеллектуальная собственность означает закрепленные законом права, которые являются результатом интеллектуальной деятельности в промышленной, научной, литературной и художественной областях». В широком понимании термин ИС означает закрепленные законом временные исключительные права на результат интеллектуальной деятельности или средства индивидуализации» [7].

«Под объектами ИС специалисты обычно понимают:

- права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий;
- патентное право;
- авторское право и права, смежные с ним;
- право на ноу-хау (секреты производства);
- право на топологии интегральных схем;
- право на селекционные достижения.

Самыми распространенными являются первые три разновидности (патентное, авторское право и смежные с ним, права на средства индивидуализации юридических лиц, товаров, работ, услуг и предприятий).

В современной экономике объекты ИС становятся главным фактором конкурентоспособности, экономического роста и формирования благосостояния, важнейшим стратегическим ресурсом повышения эффективности промышленности и конкурентоспособности продукции и услуг на мировом рынке. Помимо экономического значения, объекты ИС имеют важное социальное значение. Большой удельный вес в валовом внутреннем продукте высокоразвитых государств занимает индустрия ИС, которая охраняется авторским правом и смежными правами. Научные произведения, произведения литературы и искусства являются важнейшими элементами культурного развития общества, обеспечивающими удовлетворение потребностей и желаний людей» [7].

Использование результатов интеллектуальной деятельности в рамках закона, создают благоприятные условия для самих носителей интеллектуальной собственности, и для всего общества в целом. В идеальном варианте развития событий в выгодном свете предстают и общество, и государство, и компании. Для государства, использование интеллектуальной собственности, играет одну из главных ролей, такое использование способствует развитию экономики, внедрений новейших технологий в производство, привлечение инвестиций и как следствие увеличение казны государства за счет налоговых отчислений, таможенных пошлин, лицензионных платежей.

Кроме того, на рынке возникает здоровая конкуренция среди компаний, использующие передовые технологии и использующие новейшее программное обеспечение, что позволяет расширять свои возможности и рынки. Фирмы так же вправе продавать объекты интеллектуальной деятельности, что неминуемо ведет к увеличению финансового оборота.

Вышеперечисленные условия весьма значительны и для государства, как международного субъекта, который имеет преимущества более глобального характера, как сильного игрока на международной арене.

На основании вышеизложенного, следует подчеркнуть, что охрана государством объектов интеллектуальной собственности одна из приоритетных стратегий, гарантирующая не только экономическую стабильность, но и национальную безопасность в современном, крайне нестабильном мире.

Национальное законодательство предусматривает не только регулятивную функцию субъектов интеллектуальной собственности, но и механизм защиты, путем определенных методов и средств, социальных, экономических, правовых.

К сожалению, Россия не является локомотивом в области интеллектуального регулирования. Рынок интеллектуальной собственности недостаточно развит и защищен.

«Важным обстоятельством является то, что большинство современных российских организаций не оформляют должным образом права на созданные результаты интеллектуальной деятельности, вследствие чего основная масса имеющихся РИД существует в неохраняемом виде. К основным причинам этого можно отнести: крайне низкий уровень общественного правосознания, когда авторы результатов интеллектуальной деятельности не знают способов их охраны; низкую квалификацию работников, занимающихся вопросами охраны РИД, которые плохо знают соответствующие юридические нормы и слабо представляют возможности их реализации. В свою очередь, это может быть следствием того, что в целом ряде отечественных юридических вузов и факультетов вопросы авторского и патентного права освещаются в учебном курсе гражданского права в объеме, как правило, не более 10 часов. В результате авторы, изобретатели и иные творческие работники зачастую не могут получить квалифицированную

юридическую помощь по интересующим их вопросам, а судьи и работники правоохранительных органов также слабо разбираются в вопросах ИС. При этом нарушители авторских и иных прав на ИС нередко сами не знают элементарных положений действующего законодательства об интеллектуальной собственности» [7].

Государство, не умеющее защитить интеллектуальную собственность обречено нести убытки и терять квалифицированные кадры. Поэтому Правительство Российской Федерации разрабатывает социальные программы для разработчиков искусственного интеллекта, разработчиков интеллектуальной собственности и программного обеспечения с тем, чтобы результаты их деятельности оставались внутри государства и действовали на благо государства. Так как современные вызовы характеризуются жесткостью по отношению к России. Это касается и экономического сектора, и политического, и социального.

«Кроме того, отсутствие возможностей для охраны некоторых РИД нередко обусловлено отсутствием самого соответствующего объекта права. Например, в настоящее время вне сферы правовой защиты остаются такие важные объекты возможной правовой охраны, как названия средств массовой информации, названия лекарственных средств и кулинарных блюд, названия морских и речных судов, и т.д.» [8].

Кроме того, существующие пробелы в законодательстве, приводят к определенным решениям, будь то предприниматель, специалист, разработчик, инвестор, в отношении результатов интеллектуальной деятельности. Что является неуверенностью отношений в бизнесе, нестабильной материальной составляющей и многими другими проблемами.

Огромное количество нарушений можно наблюдать в наукоемких отраслях, которые требую крупных инвестиций со стороны государства. И как следствие, поддельная продукция вытесняет более качественный отечественный продукт. А это может привести к ослаблению не только

экономической сферы, но и к уничтожению моральных стимулов разработчиков и высококвалифицированных кадров.

Например, «владелец бизнеса, не имеющий возможность должным образом обеспечивать охрану своих интеллектуальных прав, может столкнуться с серьёзными проблемами в виде: потери деловой репутации и оттока клиентов в случае использования товарного знака конкурентами; снижения конкурентоспособности и сокращения занимаемой доли рынка; нежелания инвесторов сотрудничать с предпринимателем, не способным защитить собственные активы. А в масштабе страны это приводит к возникновению и увеличению размеров технологической зависимости страны от западных технологий в основных гражданских областях экономики» [7].

В настоящее время, действующие санкции со стороны западных и европейских стран дают нашему государству шанс, возобновить собственные производства, отойти от зависимости импорта.

Помимо экономического аспекта, важную роль играет и социальная составляющая. Квалифицированная и достойная охрана таких объектов, как художественного или технического творчества не только выступает стимулом для дальнейшей деятельности, но служит примером для других авторов. Что в свою очередь еще больше обогащает культурный уровень общества.

«С целью сохранения в России научно-технического потенциала и защиты национальных интересов в сфере экономики и технологической безопасности необходимо усиление государственного контроля и регулирования экспорта российских технологий гражданского назначения, созданных на средства федерального бюджета. Для этого должен быть установлен порядок обязательной регистрации бизнес-сделок и получения разрешений на экспорт технологий, созданных на средства федерального бюджета. При этом, особого внимания заслуживают вопросы передачи за

рубеж технологий, относящихся к здравоохранению и безопасности, а также и к другим важным для удовлетворения жизненных потребностей страны отраслям науки и техники. При этом необходимы оценки затрат на организацию использования этих технологий в отечественном производстве, с целью обеспечения внутреннего рынка продукцией, произведенной на их основе. Эти затраты должны сопоставляться со стоимостью готовой продукции, которую государство, возможно, вынуждено будет экспортировать. Необходимо предусмотреть систему государственной регистрации лицензионных договоров (контрактов, соглашений) на передачу технологий общегражданского назначения, вне зависимости от наличия правовой охраны объекта экспорта, с выдачей удостоверения о его регистрации» [7].

Приобретая опыт в области защиты прав на результаты интеллектуальной деятельности необходимо совершенствовать законодательство в данной области. Наличие в Гражданском Кодексе Российской Федерации четкого понятийного аппарата и механизма защиты результатов интеллектуальной деятельности и его объектов приведет не только к экономическому благополучию, но и развитию во многих областях науки и техники, в том числе и IT-технологиях. Уже сегодня возникает необходимость выявления и развития изобретательского потенциала, творческих талантов во многих отраслях. Со временем, и технологические достижения превратятся в прибыльный бизнес не только на внутреннем рынке, но и на мировом уровне.

Заключение

Цифровизация во всех отраслях нашей жизни стала реальностью и как следствие необходимо правовое регулирование цифровых объектов. Подходы к решению данной проблематики достаточно обширны и многочислены. Научному сообществу небезразличен спектр общественных отношений, подвергшийся цифровизации. На сегодняшний день, не существует единого подхода к решению вопроса о сущности цифровых объектов. Некоторые научные школы склонны отожествлять цифровые объекты и цифровые права, другие, напротив разделяют данные понятия. Связано это прежде всего с тем, что отсутствует правовой базис регулирования, нет многих определений существующих программных продуктов и цифровых объектов. Становление данной отрасли только зарождается, поэтому не определены четкие критерии и понятия.

Следует отметить, что очевидной тенденцией правового регулирования системы общественных отношений в настоящее время в глобальном смысле является тот факт, что регулирование цифровых объектов и прежде всего, цифровых прав является предметом правового регулирования фактически всех ведущих, развитых стран. Можно обратить внимание на тот факт, что правовой опыт отдельных стран заслуживает внимания, например, правовые положения некоторых штатов США по вопросам наследования цифровых активов. В ряде стран создаётся и специальная организационная структура в сфере защиты цифровых объектов, такая структура создана, например, в Германии.

Важным является защита права на цифровую информацию. Прежде всего охрана такого права конкретизируется в защите персональных данных. Законы, а равно подзаконные акты выделяют три категории персональных данных:

- информация, кающаяся непосредственно конкретного физического лица, фамилия, имя, отчество, дата рождения, прописки;

- специальная информация, о принадлежности к расе человека, национальности, религия, состояние здоровья;

- биометрические данные, фото сетчатки глаза, запись голоса человека.

Защита персональных данных приобретает новые смыслы и новое правовое регулирование, поскольку информационно-коммуникативные системы раз за разом подвергаются их бесконечному копированию. Если раньше информация отражалась на бумажных носителях и достаточно было печатного опровержения, то на сегодняшний день, Интернет не является гарантом защиты данных. И даже полное удаление информации из информационно-коммуникативных систем оставляет след или хранится на серверах.

Есть определённая специфика объектов авторского права, которые выражены в цифровой форме. Во-первых, если цифровой объект помещён в Интернет, он становится открытой информацией и доступ к такой информации получает неограниченный круг лиц. Во-вторых, произведение, которое выражено в цифровой форме оторвано от материального носителя. В-третьих, существенным отличием является и отличие по таким показателям, как тиражи и количество изданных экземпляров. В-четвёртых, в отличии от других произведений в том случае, если произведение выражено в цифровой форме, то не всегда возможно разграничить оригинал и копию. В-пятых, это максимально высокая скорость распространения соответствующих материалов в Интернете.

Основным способом защиты цифровых объектов в цифровой форме является блокировка нелегального контента. Инициирует процесс блокировки правообладатель. При этом, уже отмечалось, что возможна как письменная, так и электронная форма такого обращения. При этом, статья

144.1 ГПК РФ закрепляет нормы об обеспечительных мерах, которые в данном случае и могут быть реализованы. После рассмотрения фактических материалов дела может быть вынесено решение о блокировке сайта. Если же и по истечении трех рабочих дней нелегальный контент все еще будет присутствовать на сайте, то Роскомнадзор принимает меры по блокировке сайта на уровне операторов связи посредством внесения информации о сетевом адресе, доменном имени и URL'е сайта в специальную информационную систему, на основании которой оператор связи обязан ограничить доступ к нелегальному контенту (а при невозможности – ко всему сайту в целом) в течение суток.

На сегодняшний день, разработка и реализация механизмов защиты прав на цифровые объекты, является одной из приоретеных задач государства, от этого зависит будущее развитие страны и реализация интеллектуального потенциала. Кроме того, является определенным стимулом для творческой и научной деятельности гражданина и как следствие дальнейшее благополучное развитие экономики, культуры и общества в целом.

Предполагается, что совершенствование способов охраны цифровых объектов может быть достигнуто путём объединения усилий государственных и общественных структур с целью оптимизации норм Законодательства РФ об авторском праве и смежных правах, и путем развития соответствующего общественного правосознания.

«Согласно Люциусу Мэйдеру, экспериментальное законодательство- это «закон, принятый на ограниченный период времени для проверки того, сможет ли конкретная законодательная мера эффективно достичь определенных целей»; это «форма законодательства, обладающая определенными характеристиками: оно должно быть ограничено во времени; в нем следует четко указать свою цель; в нем следует указать цели планируемых законодательных действий и указать критерии, используемые

для оценки соответствия положений, принятых на временной основе; в нем следует указать данные, которые необходимо собрать, и определить обязанности по сбору данных и оценке результатов и так далее» [99].

Необходимо отслеживать и принимать опыт зарубежных стран, на примере Китайской Народной Республики можно видеть обширный спектр применяемого экспериментального законодательства.

Для активизации работы в области охраны прав на цифровые объекты представляется целесообразным ввести в учебную программу высших учебных заведений специальную дисциплину «Правовая охрана интеллектуальной собственности». Это позволило бы подготовить высококвалифицированных специалистов (инженеров, юристов, таможенников, врачей и др.), владеющих основами патентного права, авторских и смежных прав, а также основами правовой защиты других цифровых объектов.

Список используемой литературы и используемых источников

1. Акинфиева В. В. Утилитарные цифровые права в современных условиях трансформации экономики // Пермский юридический альманах. – 2020. – № 3. – С. 397.
2. Андреев Ю.Н. Механизм гражданско-правовой защиты. – М.: Норма, 2019.
3. Арбитражный процессуальный кодекс Российской Федерации от 24.07.2002 № 95-ФЗ (ред. от 31.07.2021) // Российская газета. – 2002. – № 137.
4. Асанов Р.К. Формирование концепции «цифровой экономики» в современной науке // Социально-экономические науки и гуманитарные исследования. – 2016. – № 15. – С. 143–148.
5. Аюшеева И.З. Цифровые объекты гражданских прав // Lex russica. – 2021. – Т. 74. – № 7. – С. 32
6. Банке Б. Россия онлайн? / Б. Банке, В. Бутенко. – [Электронный ресурс]. – URL: http://russiaonline.info/story/short-summary (дата обращения 14.11.2022)
7. Бернская конвенция по охране литературных и художественных произведений от 9 сентября 1886 года. – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)
8. Бийчук А.Н. Цифровая трансформация бизнеса в современной экономике // Экономическая среда. – 2017. – № 2 (20). – С. 14-16.
9. Бирюков В.А. Стратегия информационной безопасности медиаорганизации // Вестник Владимирского государственного университета. – 2017. – № 1. – С. 81.
10. Богомолов Е. А., Воронин М.В., Российский экономический университет им. Г.В. Плеханова// Совершенствование правовой охраны интеллектуальной собственности как фактор развития современного общества

11. Богомолов Е. А., Воронин М.В., Современное состояние рынка общественного питания Ивановской области и обоснование ожидаемых результатов его развития. В сборнике: Региональная экономика и потребительский рынок: современное состояние и тенденции развития. Сборник материалов научно-практической конференции преподавателей, аспирантов, магистрантов Ивановского филиала Российского экономического университета имени Г. В. Плеханова, в рамках Межрегионального форума "Перспективы развития регионального потребительского рынка". 2016. С. 237- 243.

12. Болдырев С.И. Авторские права в современном информационном телекоммуникационном пространстве Российской Федерации: Гражданско-правовое регулирование и защита: Дис. ... канд. юрид. наук. – Курск, 2017.

13. Варламова Н.В. Цифровые – новое поколение прав человека? // Труды Института государства и права РАН. 2019. Т. 14. № 4. С. 9-46.

14. Василевская Л.Ю. Токен как новый объект гражданских прав: проблемы юридической квалификации цифрового права // Актуальные проблемы российского права. – 2019. – № 5. – С.113.

15. Введение в «Цифровую» экономику / А.В. Кешелава, В.Г. Буданов, В. Ю. Румянцев и др.; под общ. ред. А. В. Кешелава; гл. «цифр.» конс. И. А. Зимненко. – М.: ВНИИ Геосистем, 2017.

16. Вершинин А.П. Способы защиты гражданских прав в суде. – СПб: Изд-во Санкт – Петербургского государственного университета, 1997. – С. 29-38.

17. ВКонтакте ввела цифровые отпечатки для книг перед судом с правообладателями: [сайт]. – [Электронный ресурс]. – URL: https://vc.ru/n/vk-books-check (дата обращения 14.11.2022)

18. Волос Ф.Ф. Некоторые проблемы защиты прав и законных интересов сторон смарт-контракта

19. Воронин М.В., Богомолов Е.А. Современное состояние рынка

общественного питания Ивановской области и обоснование ожидаемых результатов его развития // В сборнике: Региональная экономика и потребительский рынок: современное состояние и тенденции развития. Сборник материалов научно-практической конференции преподавателей, аспирантов, магистрантов Ивановского филиала Российского экономического университета имени Г.В. Плеханова, в рамках Межрегионального форума «Перспективы развития регионального потребительского рынка». – 2016. – С. 237-243.

20. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 02.07.2022) // Собрание законодательства РФ. – 1994. – № 32. – Ст. 3301.

21. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 29.12.2021) // Российская газета. – 2006. № 289.

22. Гражданский процессуальный кодекс Российской Федерации от 14.11.2002 № 138-ФЗ (по состоянию на 31.07.2021) // Собрание законодательства РФ. – 2002. – № 46. – Ст. 4532.

23. Гражданское право. Общая часть: Учебник: в 4 т. / В.С. Ем, Н.В. Козлова, С.М. Корнеев и др.; под ред. Е.А. Суханова. – 3-е изд., перераб. и доп. – М.: Волтерс Клувер, 2014. Т. 1.

24. Гражданское право: учебник в 4 т. / Отв. ред. Е.А. Суханов. – М.: Волтерс Клувер, 2014. – Том I.

25. Деревянченко А.А. О влиянии социальных сетей на социализацию современных детей // Актуальные проблемы гуманитарных и социально-экономических наук. – М.: Изд-во «Спутник». 2019. – С. 308-312.

26. Европейская патентная конвенция (подписана в Мюнхене в 1973 году, вступила в силу 1 октября 1977 года). – [Электронный ресурс]. – Режим доступа: https://online.consultant.ru (дата обращения 14.11.2022)

27. Евтянова Д.В. Критерии создания цифровых платформ управления экономикой // Экономические системы. – 2017. – Т. 10, № 3 (38).

– С. 54–57.

28. Еримушкин В.А. Инфокоммуникационное технологическое пространство цифровой экономики // Круглый стол «Цифровая трансформация бизнеса на основе технологий связи следующего поколения», 28 марта 2017 г. / Центральный научно-исследовательский институт связи. – [Электронный ресурс]. – URL: https://bi.hse.ru (дата обращения 14.11.2022)

29. Закон Великобритании «О цифровой экономике» (Digital Economy Act 2010). – [Электронный ресурс]. – URL: https://www.legislation.gov. uk/ukpga/2010/24/contents (дата обращения 14.11.2022)

30. Закон от 7 октября 2016 г. «О цифровой республике». – [Электронный ресурс]. – URL: https://www.legifrance.gouv.fr (дата обращения 14.11.2022)

31. Игнатьев В. И. Информационная перегрузка социальной системы и её социальные последствия // Социологические исследования. – 2017. – № 7. – С. 3-11.

32. Интернет вещей, IoT, M2M мировой рынок (2019). – [Электронный ресурс]. – URL: http:// www.tadviser.ru/index.php/Статья:Интернет_вещей,_IoT,_M2M_(мировой_рынок) (дата обращения 14.11.2022)

33. Камалян В.М. Понятие и правовые особенности смарт-контрактов // Юрист. – 2019. – № 4. – С. 20.

34. Каминская Е.И. Вопросы охраноспособности и ответственности за нарушение авторских прав в отношении шрифтов, карт, фотографий как объектов авторского права // Комментарий судебной практики / отв. ред. К.Б. Ярошенко. – М.: Институт законодательства и сравнительного правоведения при Правительстве РФ, КОНТРАКТ. – 2018. – Вып. 23. – С. 73-95.

35. Карев Я.А. Электронные документы и сообщения в коммерческом обороте: Правовое регулирование. – М., 2006.

36. Касаткина В. В. Токен и криптовалюта: их понятие и взаимосвязь в цифровой экономике // Цифровые технологии в экономической сфере: возможности и перспективы: сборник научных статей. – Тамбов, 2017. – С. 22–25.

37. Кобыляцкий Д.А. Правовая охрана произведений в сети Интернет: Дис. ... канд. юрид. наук. – Саратов, 2015.

38. Колозариди П.В., Макушева М.О. Интернет как проблемное поле социальных наук // Мониторинг общественного мнения: экономические и социальные перемены. – 2018. – № 1. – С. 1-11.

39. Колосова Т.Е. Проблемы реализации охранительной функции государства в сфере защиты прав человека в цифровом пространстве // Актуальные проблемы государства и права. 2022. Т. 6. № 2. С. 151- 157. DOI 10.20310/2587-9340-2022-6-2-151-157

40. Конобеевская И.М. Цифровые права как новый объект гражданских прав // Изв. Сарат. ун-та. Нов. сер. Сер. Экономика. Управление. Право. – 2019. – Т. 19. – Вып. 3.

41. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных от 01.07.2020) // Собрание законодательства РФ. – 2009. – № 4. – Ст. 445.

42. Краснова, С.А. Теоретические основы классификации гражданско-правовых способов защиты // Российский юридический журнал. – 2015. – № 2. – С. 43.

43. Кривошапко, Ю. Большие данные станут еще больше. – [Электронный ресурс]. – URL: https:// rg.ru/2019/03/17/globalnaia-sfera-dannyh-vyrastet-bolee-chem-v-piat-raz-v-blizhajshie-gody.html. (дата обращения 14.11.2022)

44. Кунцевич Н.В. Вызовы цифрового общества // Молодой ученый. – 2021. – № 30 (372). – С. 59-63.

45. Лебедева Д.С., Яценко А.О. Информация как объект

гражданского права // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. – 2017. – Т. 3 (69). – № 4.

46. Макарчук Н.В. Публично-правовые ограничения использования цифровых активов и технологий // Предпринимательское право. – 2019. – № 1. – С. 40.

47. Навальный А.А., Алексеева Е.В. Понятие и виды цифровых активов // Новый юридический вестник. – 2021. – № 4. – С. 34.

48. Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. – 2016. – № 2. – С. 186-196.

49. Об ограничении доступа к социальной сети Instagram*. URL: https://rkn.gov.ru/news/rsoc/news741 80.htm (дата обращения: 18.10.2022).

50. Определение Конституционного Суда РФ от 06.10.2015 № 2443-О по жалобе граждан Динзе Дмитрия Владимировича и Сенцова Олега Геннадьевича на нарушение их конституционных прав положениями пункта 3 части второй статьи 38, части третьей статьи 53 и статьи 161 Уголовно-процессуального кодекса Российской Федерации // Вестник Конституционного Суда РФ. – 2016. – № 1.

51. Определение Конституционного Суда РФ от 16.07.2013 № 1176-О об отказе в принятии к рассмотрению жалобы гражданина Круглова Александра Геннадьевича. – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

52. Определение Судебной коллегии по гражданским делам Верховного Суда Российской Федерации от 28.01.2019 № 306-ЭС18-21814. – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

53. Осипов Б.Е. Защита гражданских прав: учеб. и практич. пособие. – Алматы, 2015.

54. Павлов А.А. Присуждение к исполнению обязанности как способ защиты гражданских прав в обязательственных правоотношениях: теория и практика гражданского права и гражданского процесса. – СПб.: Юридический центр Пресс, 2001.

55. Паспорт национального проекта «Национальная программа «Цифровая экономика Российской Федерации»» (утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7). – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

56. Петрыкина Н.И. Правовое регулирование оборота персональных данных. Теория и практика. – М., 2021.

57. Постановление Девятого арбитражного апелляционного суда от 15.05.2018 № 09АП16416/2018 по делу № А40-124668/2017. – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

58. Постановление Пленума ВАС РФ от 08.10.2012 № 60 «О некоторых вопросах, возникших в связи с созданием в системе арбитражных судов Суда по интеллектуальным правам». – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

59. Постановление Пленума Верховного Суда РФ от 23 апреля 2019 г. № 10 «О применении части четвертой Гражданского кодекса Российской Федерации» // Российская газета. – 2019. – № 96.

60. Проскурякова М.И. Персональные данные: российская и германская национальные модели конституционно-правовой защиты в сравнительной перспективе // Сравнительное конституционное обозрение. – 2016. – № 6. – С. 84-98.

61. Пьянкова С.Г., Митрофанова И.А. Цифровизация экономики: российский и зарубежный опыт // Региональная экономика. Юг России. – 2018. – № 3 (21) – С 22.

62. Рахматулина Р.Ш. Цифровая форма объектов авторского права. //

Право и цифровая экономика. – 2019. – № 1.

63. Резаев А.В., Трегубова Н.Д. «Искусственный интеллект», «онлайн-культура», «искусственная социальность»: определение понятий // Мониторинг общественного мнения: экономические и социальные перемены. – 2019. – № 6. – С. 35-47.

64. Решение Ленинского районного суда Твери от 28.12.2015 по гражданскому делу № 3-846/2015. – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

65. Решение Хорошевского районного суда г. Москвы по делу № 2-167/14 по иску ООО «Лига-ТВ» к Никитину Павлу Олеговичу о возмещении убытков, защите интеллектуальных прав. – [Электронный ресурс]. – URL: https://rospravosudie.com/court-xoroshevskij-rajonnyj-sud-gorod-moskva-s/act-471857460/ (дата обращения 14.11.2022)

66. Рожкова М.А. Цифровые активы и виртуальное имущество: как соотносится виртуальное с цифровым // Закон. ру. – [Электронный ресурс]. – URL:https://zakon.ru/blog/2018/06/13/cifrovye_aktivy_i_virtualnoe_imuschestvo_kak_sootnositsya_virtualnoe_s_cifrovym (дата обращения 14.11.2022)

67. Савельев А.И. Договорное право 2.0: «умные» контракты как начало конца классического договорного права // Вестник гражданского права. – 2016. – № 3. – С. 3

68. Савельев А.И. Некоторые правовые аспекты использования смарт-контрактов и блокчейн-технологий по российскому праву // Закон. – 2017. – № 5. – С. 94

69. Санникова Л. В., Харитонова Ю. С. Правовая сущность новых цифровых активов // Закон. – 2018. – № 9. – С. 86–89.

70. Славин Б. Б. Эпоха коллективного разума: О роли информации в обществе и о коммуникационной природе человека. – М., 2014.

71. Смарт-контракты: взгляд юриста на жизнеспособность – [Электронный ресурс]. – URL: https://bitnewstoday.ru/market/blockchain/smart-

kontrakty-vzglyad-yurista-nazhiznesposobnost (дата обращения 14.11.2022)

72. Смирнов А.В. Цифровое общество: теоретическая модель и российская действительность // Мониторинг общественного мнения: экономические и социальные перемены. – 2021. – № 1. – С. 129-153.

73. Соловьева О. РФ обещает прыгнуть в цифровой мир // Независимая газета. – 2017. – С. 2-4.

74. Сохранение цифрового наследия в России: методология, опыт, правовые проблемы и перспективы: монография / И. И. Горлова, А. Л. Зорин, А. А. Гуцалов; отв. ред. А. В. Крюков; Юж. ф-л Рос. науч.- иссл. ин-та культурного и природ. наследия им. Д. С. Лихачёва. – М.: Институт Наследия, 2021.

75. Старосельцева М.М., Брусова П.И. К вопросу о защите цифровых прав сквозь призму гражданского права // Ученые записки Казанского юридического института МВД России. – 2020. – Т. 5. – № 2(10). – С. 227 - 230.

76. Сулейменов М.К. Понятие и способы защиты гражданских прав. – Алматы: НИИ частного права КазГЮУ, 2016.

77. Тапалина Э.В. Защита персональных данных в цифровую эпоху: российское право в европейском контексте - [Электронный ресурс]. – URL: https://www.it-world.ru/cionews/manage_secure/135966.html (дата обращения 14.11.2022)

78. Трунцевский Ю.В., Севальнев В.В. Смарт-контракт: от определения к определенности // Право. Журнал Высшей школы экономики. – 2020. – № 1. – С. 118.

79. Указ Президента РФ от 05.12.2016 № 646 №Об утверждении Доктрины информационной безопасности Российской Федерации». – [Электронный ресурс]. – URL: https://online.consultant.ru (дата обращения 14.11.2022)

80. Федеральный закон от 02.07.2013 № 187-ФЗ «О внесении

изменений в отдельные законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях» // Собрание законодательства РФ. – 2013. – № 27. – Ст. 3479.

81. Федеральный закон от 02.08.2019 № 259-ФЗ (ред. от 14.07.2022) «О привлечении инвестиций с использованием инвестиционных платформ и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. – 2019. – № 31. Ст. 441.

82. Федеральный закон от 13.03.2006 № 38-ФЗ (ред. от 14.07.2022) «О рекламе» // Собрании законодательства РФ. – 2006. – № 12. – Ст. 1232.

83. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (ред. от 02.07.2021) // Собрание законодательства Российской Федерации от 31 июля 2017. – № 31 (часть I). – Ст. 4736.

84. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 18.03.2021) Об информации, информационных технологиях и защите информации: // Собрание законодательства РФ. – 2006. – № 31 (ч. 1). – Ст. 3448.

85. Федеральный закон от 27.07.2006 № 152-ФЗ (ред. от 02.07.2021) О персональных данных. // Собрание законодательства РФ. – 2006. – № 31 (часть I). – Ст. 3451.

86. Федеральный закон от 31.07.2020 № 259-ФЗ (ред. от 02.07.2021) «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» // Собрание законодательства РФ. – 2020. – № 31 (часть I). – Ст. 5018.

87. Федоров Д.В. Токены, криптовалюта и смарт-контракты в отечественных законопроектах с позиции иностранного опыта // Вестник гражданского права. 2018. № 2. С. 33.

88. Цифровая трансформация и защита прав граждан в цифровом пространстве: доклад Совета при Президенте Российской Федерации по

развитию гражданского общества и правам человека. М., 2021. С. 49-50.

89. Чурилов А. Режимы охраны программ для ЭВМ: изобретение, коммерческая тайна или литературное произведение? // ИС. Авторское право и смежные права. – 2017. – № 7. – С. 35-44.

90. Чурилов А.Ю. Особенности правовых режимов охраны программного обеспечения // Хозяйство и право. – 2017. – № 8. – С. 35-44.

91. Чурилов А.Ю. Правовое регулирование интеллектуальной собственности в игровой индустрии // ИС. Авторское право и смежные права. – 2017. – № 10. – С. 59-68.

92. Шпачева Т.В., Шпачев Е.В. О способах защиты права (законного интереса) в арбитражном суде // Арбитражные споры. – 2016. – № 4. – С. 45.

93. Шудрова К. Проверка Роскомнадзора по персональным данным.

94. Эксперт оценил ущерб от киберпреступлений в России в 2021 году. URL: https://ria.ru/20211222/kiberprestupleniya-1764832102.html (дата обращения: 18.10.2022)

95. Dufva T., Dufva M. Grasping the Future of the Digital Society. Futures. Vol. – 2019. – P. 17-28.

96. Katzenbach C., Ulbricht L. Algorithmic Governance. Internet Policy Review. – 2019. – Vol. 8. – No. 4.

97. Selwyn N. (2019) What is Digital Sociology? Cambridge,2019 UK: PolityPres

98. Lauslahti K., Mattila J. Seppälä T. Smart Contracts – How will Blockchain Technology Affect Contractual Practices? // ETLA Raportit – ETLA Reports. № 68. P. 14

99. Mader L. Evaluating the Effects: A Contribution to the Quality of Legislation // Statute Law Review. 2001. Vol. 22. № 2. P. 119—131.