Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российская академия народного хозяйства и государственной службы
при Президенте Российской Федерации» (РАНХиГС)

Воронцов С.А., Кравченко А.Г., Мамычев А.Ю., Овчинников А.И.

РАЗРАБОТКА СИСТЕМЫ МЕР И ЮРИДИЧЕСКИХ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ КОРРУПЦИИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ И ЭКОНОМИКИ

Москва 2020

Аннотация

Одной из ключевых задач государства на современном этапе является развитие цифровых технологий в сфере противодействия коррупции, в связи с возможностью средствами цифровизации существенно повысить открытость, публичность и прозрачность государственного управления, выявить коррупциогенные факторы, схемы и отношения, оптимизировать антикоррупционную деятельность правоохранительных органов и ограничить возможности коррупционеров разного уровня. Возможности цифровизации позволяют предупредить формирование новых сфер коррупции, не допустить ее финансовой теневизации.

В этой связи повышается значимость дальнейшей доктринальной разработки вопросов о содержании коррупции, теоретических, концептуально-методологических и технико-юридических основаниях оптимизации механизма правового регулирования в сфере реализации задач, сформулированных в программе «Цифровая экономика Российской Федерации» по противодействию коррупции. Необходимо определить политические, экономические, социальные и правовые условия и факторы совершенствования законодательства и провести оценку действующего нормативного правового регулирования применения цифровых технологий в противодействии коррупции с последующей разработкой предложений по системному упорядочению отдельных норм, восполнению пробелов в актах о противодействии коррупции и антикоррупционном законодательстве в целом. Выявить механизмы и инструменты противодействия коррупции, их легализации в правовых нормах, при которых законотворческая и правоприменительная антикоррупционная деятельность в сфере противодействие коррупции в условиях цифровизации государственного управления и экономики сможет обеспечить реальные результаты.

Результаты НИР могут быть использованы в интересах: подразделений Правительства Российской Федерации и органов исполнительной власти, участвующие в разработке системы мер и юридических механизмов противодействия коррупции в условиях цифровизации государственного управления и экономики. Материалы могут быть полезны широкому кругу научных и практических работников, занимающихся противодействием коррупции, использованы в системе переподготовки и повышения квалификации кадров системы государственной службы, а также при преподавании учебных дисциплин юридического цикла.

СПИСОК ИСПОЛНИТЕЛЕЙ

Руководитель НИР, доктор юрид. наук, профессор, и.о. директора Научно-учебного центра ИПНБ РАНХиГС при Президенте России	_____ подпись, дата	С.А. Воронцов (введение, подраздел 1.2, подраздел 2.1)
Исполнители: доктор юрид. наук, профессор кафедры теории и истории права и государства Южно-Российского института РАНХиГС при Президенте России	_____ подпись, дата	А. И. Овчинников (введение, подраздел 1.1, подраздел 2.1, подраздел 2.2, подраздел 2.4)
доктор юрид. наук, доцент, заведующий лабораторией политико-правовых исследований факультета политологии МГУ имени М.В. Ломоносова	_____ подпись, дата	А.Ю. Мамычев (подраздел 1.3, подраздел 2.2)
кандидат юрид. наук, доцент, заведующий кафедрой гражданского права Дальневосточного федерального университета	_____ подпись, дата	А.Г. Кравченко (подраздел 1.4, подраздел 2.3)

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования обусловлена особой значимостью получения углубленных знаний о содержании коррупции, разработка теоретических, концептуально-методологических и технико-юридических оснований оптимизации механизма правового регулирования в сфере реализации задач, сформулированных в программе «Цифровая экономика Российской Федерации» по противодействию коррупции.

К числу основных фундаментальных и прикладных задач, решаемых в рамках исследования отнесены:

- определение сущности коррупции в целях разработки моделей цифрового противодействия данному феномену;

- содействие созданию необходимых и достаточных условий институционального и инфраструктурного характера, путем выявления, предупреждения и устранения угроз коррупционного характера, возникающих в процессе создания системы цифровой экономики Российской Федерации;

- формулирование предложений по нормативному содержанию в плане противодействия коррупции в цифровой экономике и цифровом государстве;

- подготовка рекомендаций в сфере цифровой безопасности государства и предложений по оптимизации системы обеспечения информационной безопасности;

- систематизация приоритетов и принципов правовой политики РФ в сфере борьбы с коррупцией с использованием цифровых технологий.

Для решения указанных задач научно-исследовательской работы планируется:

- провести анализ понятия коррупции и теоретико-методологических аспектов противодействия данному феномену в российском законодательстве;

- изучить процесс трансформации государственного управления в условиях цифровой экономики, установить новые коррупционные риски и вызовы;

- исследовать концептуальные основания и теоретико-методологические аспекты противодействия коррупции в условиях цифровизации государства и права;

- проанализировать опыт зарубежных государств в использовании цифровых технологий в противодействии коррупции;

- оценить правовую институционализацию цифровых технологий противодействия коррупционным отношениям.

1. Антикоррупционная правовая политика современного государства в цифровую эпоху: основные направления и приоритеты

1.1. Трансформация государственного управления в условиях цифровой экономики: новые коррупционные риски и вызовы

1.1.1. Трансформация государственного управления в условиях цифровой экономики: основные направления

В современном мире процессы цифровизации существенно влияют на государственное управление. Риски и вызовы национальной безопасности в эпоху цифрового мира становятся особенно явными в контексте цифровой глобализации, под которой следует понимать формирование нового миропорядка, конструируемого и управляемого с помощью цифровых технологий в единстве сетевой, коммуникационной и мировоззренческо-смысловой структуры. Представляется правильным говорить в таком случае о цифровой безопасности как важнейшем элементе национальной безопасности, но не в смысле технологической защиты информации. Понятие «цифровая безопасность» значительно шире, чем его часто понимают технические специалисты, например, определяя ее следующим образом: «Цифровая безопасность – это комплекс мер, направленных на защиту конфиденциальности, целостности и доступности информации от вирусных атак и несанкционированного вмешательства» [1]. Представляется, что уже в ближайшем будущем понятие «цифровая безопасность» совпадет по смысловому объему с понятием «национальная безопасность». В этом следует видеть последствия цифровой глобализации, цифровой революции, смены технологических мироукладов, которые могут уничтожить идею национального государства. Уже сейчас в международном дискурсе относительно проблем цифровой безопасности конкурируют концепции многосубъектного регулирования и управления рисками (англ. - multi-stakeholder regulation), основанные на активном участии негосударственных субъектов-регуляторов, прежде всего, граждан, активных пользователей сетей, бизнеса и институтов гражданского общества, и межгосударственного сотрудничества в данной сфере [2].

Пересмотру подвергнуты привычные для государства эпохи модерна и, даже, постмодерна понятия – национальный суверенитет, государственная валюта, механизм государства, национальная идентичность, идеология и т.п. Право и его идея также все менее связывается с государством: экстерриториальность становится базовым принципом развития права в информационном пространстве [3]. Однако самая главная трансформация ожидает идею государства.

В некоторых современных странах эта идентичность уже защищается средствами цифрового технологического характера. Примером может служить КНР, где применение искусственного интеллекта и цифровых технологий позволило создать «цифровую дискриминацию» в отношении отдельно взятого этноса в Синьцзяне [4].

В современной юридической литературе более привычным при обсуждении проблем безопасности человека, общества и государства в контексте цифровизации является термин «информационная безопасность» - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [5]. Новый технологический уклад ведет к упразднению указанных в данном определении понятий. Суверенитет, территориальная целостность, безопасность государства, само понятие «государство» – уже подвергнуто пересмотру, «цифровая безопасность» уже прокладывает себе дорогу в отечественной науке в связи с исследованием ранее неизвестных науке цифровых объектов [6].

В зарубежной научной литературе термин «цифровая безопасность» давно используется для обозначения разнообразных аспектов защищенности в цифровой среде личности и государственных институтов [7]. Рекомендации Организации экономического сотрудничества и развития по управлению рисками цифровой безопасности с целью обеспечения экономического и социального процветания 2015 года также содержат указание на данное понятие [8].

В современном мире термин «информационная безопасность» привычно ассоциируется с кибертерроризмом, вирусами, экстремизмом [9].

Еще десять лет назад цифровые потоки не оказывали существенного влияния на рост ВВП, в то время как сегодня они влияют на ВВП больше, чем многовековая торговля товарами. Об это говорится в докладе McKinsey Global Institute (MGI) «Цифровая глобализация: новая эра глобальные потоки», где авторы обращают внимание на то, что этот сдвиг позволяет компаниям выходить на международные рынки с менее капиталоемкими бизнес-моделями, однако он же создает новые риски и политические проблемы [10].

Глобализированное цифровое общество рождает инновационные стратегии управления, сферы и тенденции развития культуры, экономики, права, торговли, и даже

мышления [11]. И не всегда эти стратегии будут приводить к положительным для человека и государства итогам.

В мировоззренческом смысле цифровая глобализация несет угрозу для государства потери традиционных нравственных ценностей, так как формальный рационализм в условиях цифрового общества становится основным инструментом и критерием правильности принимаемых решений, в то время как традиционные ценности носят иррациональный характер, базируются на вере в Бога, жертвенности человека личными интересами во имя интересов общества (семьи, Отечества, Родины, блага государства, Церкви, общины, рода, племени и т.п.). По последствиям, цифровая революция и искусственный интеллект сравнимы с изобретением парового двигателя, как это верно отмечает в своей статье Стефан Холтел: вряд ли кто-то мог предполагать, что это изобретение вызовет огромные последствия: паровой двигатель увеличил промышленное производство, привел к социальным потрясениям, революциям и изменил политический ландшафт на следующие века [12].

Эксперты, исследующие данную трансформацию человечества, констатируют следующий вывод: «В настоящее время осуществляется переход от логоцентрической к цифроцентрической организации жизни с ее тотальной компьютеризацией и сетевизацией. По сути, это фундаментальный, экзистенциальный процесс в эволюции человеческой культуры» [13]. Несомненно, что цифровизация сделает мир еще более атомизированным и индивидуализированным, что явно не будет способствовать сохранению национальных суверенитетов и этнокультурных единств.

Государство все больше теряет статус монополиста в привычных сферах. Концепция «мягкого права» приходит на смену этатистскому юридическому позитивизму, банки предлагают выдавать паспорта и иные документы, образовательные организации через онлайн-обучение разрушают границы между странами и континентами, валютный рынок с помощью криптовалют пытается жить самостоятельно . Например, в связи с ростом интернет торговли уже функционируют интернет-суды: первый интернет-суд открылся в китайском городе Ханчжоу, однако сейчас создаются такие суды и в других странах, например в Канаде [14]. Президент Центра глобальных интересов (Вашингтон, США) Николай Злобин открыто заявляет: «Суверенные государства теряют свои возможности монопольно управлять главными процессами на собственных территориях. Бизнес стал по природе своей межгосударственным. Как, впрочем, и финансовая система, которая сегодня уже не может быть организована «по национальному признаку», а функционирует как единый, пусть и не очень здоровый, глобальный механизм» [15].

Среди задач государственным органам на Всемирной встрече на высшем уровне по вопросам информационного общества ключевыми определены национальные стратегии электронного государственного управления; разработка основы для безопасного хранения электронных информационных записей» [16]. При этом основными разработчиками технологий электронного правительства являются транснациональные корпорации со штаб-квартирами в США: Oracle, Microsoft, IBM, Hewlett Packard, Twitter, Mozilla, Intel, Apple, Cisco Systems [17].

Принципы глобального партнерства, а, по сути цифровой глобализации, в деле построения цифровой экономики, цифрового образования, правительства и прочего прописаны во многих международных документах [18, 19].

Между тем, стимулирование цифрового развития в сфере государственного управления должно осуществляться через научное обсуждение среди философов, культурологов, правоведов, специалистов в сфере национальной безопасности. Сегодня зарубежные корпорации занимаются в нашей стране внедрением электронного правительства и его технологических узлов [20]. Если добавить к этому создание единой базы данных со всей документацией на каждого гражданина, о которой давно говорят первые лица государства [21], то вполне очевидной станет уязвимость государства и его безопасности для внешней агрессии.

Процесс цифровизации государственного управления, таким образом, серьезно влияет на прозрачность и доступность его для внешнего контроля. Кроме того, стиль государственного управления, его методы и средства, формы и модели теряют культурные, национально-самобытные корни и особенности. Ранее не было сомнения в том, что государственное управление имеет культурное значение, является и порождением, и генератором национально-культурного творчества народа, населения. Цифровизация стандартизирует, унифицирует стили и формы государственного управления.

1.1.2. Антикоррупционный потенциал цифровизации государственного управления

Современным направлением государственно-правового развития различных стран, по общему признанию, является информатизация и цифровизация государственного управления, политической деятельности, правовой жизни, экономики, науки, образования, здравоохранения. В государственном управлении, построенном в соответствии с современными научно-техническими достижениями шестого технологического уклада

процесс цифровизации позволяет выйти на совершенно новый уровень профилактики и противодействия различным коррупционным правонарушениям, о чем неоднократно говорил и В.В. Путин: «Цифровизация всей системы государственного управления, повышение ее прозрачности – это и мощный фактор противодействия коррупции» [22].

Большая активность в пропаганде цифровизации государственного управления наблюдается со стороны бизнес-структур. Например, на одном из знаковых международных мероприятий - Гайдаровском форуме руководитель корпорации Сбер Герман Греф указал на необходимость цифровизации в качестве основного инструмента преодоления коррупции. Он подчеркнул, что избыточные правовые нормативы цифровизации могут помешать процессу развития цифровых технологий в силу большого количества различных нормативных ограничений. [23].

Коррупция, как известно, - один из самых важных и существенных вызовов системе национальной безопасности государства, и сегодня возможно указать о необходимости разработки модели антикоррупционной безопасности в совокупности с цифровой безопасностью. Государство вполне способно, внедряя современные цифровые технологии, преодолеть и противостоять данным вызовом. [24].

Популярность цифровых технологий обусловлена серьёзным увеличением гласности и открытости в деятельности органов государственной власти, возможностью ограничить и минимизировать разнообразные формы взаимоотношений между гражданами и должностными лицами, контролировать расходы и доходы представителей органов государственной власти, должностных лиц сотрудников правоохранительных органов. Большое количество государств, как подсказывает научная монография Т. Андерсена [25], стало на путь внедрения цифровых технологий и добилось совершенно иных показателей результативности борьбы с коррупцией.

Значимым механизмом противодействия коррупции в зарубежных странах следует отнести наличие такого института как антикоррупционной омбудсмен. Присутствие антикоррупционного омбудсмена в различных государствах реализуется посредством цифрового доступа. Через различные web-технологии граждане могут обращаться за решением своих проблем. Существует и парламентский орган в некоторых странах, отвечающий за рассмотрение электронных цифровых обращений граждан в наиболее коррупциогенных и важных сегментах общественно-политической жизни.

Цифровизация позволила также облегчить получение услуг гражданами со стороны органов государственного управления в сфере бытовых отношений.

Цифровые технологии противодействия коррупции могут опираться на предоставление доступа гражданам к обмену данными относительно коррупционных действий, связей, отношений со стороны различных представителей государственной власти. Субъекты и представители современных сетевых социальных групп в интернете, различных организаций, интернет-сообществ, представителей известных блогеров, экспертов различных государств могут осуществлять влияние на противодействие коррупции. Институты гражданского общества также позволяют эффективно осуществлять противодействие коррупции с помощью цифровых технологий, что является очень важным с учётом того факта, согласно которому движущей силой коррупции порой бывают люди, на которых возложена именно борьба с ней.

Во многих государствах Европы и даже в странах Третьего мира принцип транспарентности обеспечивает максимальную прозрачность социально-экономических отношений и позволяет эффективно осуществлять меры по борьбе с коррупцией. Этот принцип закреплен и в ст. 13 «Участие общества» Конвенции Организации Объединенных Наций против коррупции [26]. В целях наличия доступа к информации необходимым представляется юридическая формализация категорий «служебная тайна» и «профессиональная тайна». Дело в том, что без юридической унификации и наличия общего подхода к служебной информации ограниченного доступа влечет за собой сокрытие важной для общественности информации [27].

1.2. Концептуальные основания и теоретико-методологические аспекты противодействия коррупции в условиях цифровизации государства и права

1.2.1. Объективные закономерности исследования сущности коррупции в философско-правовом аспекте в целях установления индикаторов коррупционной деятельности

Феномен коррупции известен человеку с древних времен. В религиозных [28] и правовых памятниках [29] древности, многочисленных литературных произведениях, научных статьях, монографиях и диссертационных исследованиях нашего времени, коррупция определяется как, безусловно, негативное явление, которое в своем развитии, как утверждал Аристотель, может привести государство к вырождению или даже к гибели [30]. Учитывая высокий уровень угроз для государства и общества, за прошедшие века человечеством разработан широкий спектр концептуальных оснований и теоретико-методологических основ противодействия коррупции, значительное число методов

выявления, предупреждения и пресечения коррупционных правонарушений, зачастую отличающихся репрессивными мерами наказания коррупционеров.

В XXI веке уровень коррупции в Российской Федерации, как, впрочем, и во многих других странах, остается неприемлемо высоким, а система мер и юридических механизмов противодействия этому явлению, по мнению значительной части населения, не соответствует уровню угрозы. Основания для подобной оценки следуют из социологического опроса, проведенного в конце 2019 года Генпрокуратурой по всей территории Российской Федерации, в ходе которого было опрошено более 38 тыс. человек, и лишь 11% респондентов увидели позитивные изменения в противодействии коррупции [31].

Возникает естественный вопрос, где «слабое звено» в системе теоретико-методологических подходов и практических мер к противодействию коррупции? [32] Чтобы ответить на данный вопрос необходимо разобраться в природе исследуемого явления. Нечеткое толкование юридически значимых терминов, регламентирующих содержание коррупции, существенно снижает эффективность противодействия этому негативному социально-правовому явлению.

Первоочередной интерес представляет дефиниция этого явления, под которой понимаем определение коррупции, отражающее ее существенные признаки и формы проявления в различных сферах жизнедеятельности государства и общества [33]. В Российской Федерации определение коррупции сформулировано в первой статье Федерального закона «О противодействии коррупции» принятого в декабре 2008 года, в соответствии с которым была организована антикоррупционная деятельность в последующие годы. Однако, в 2016 году, несмотря на определение коррупции, прописанное в законе, Президентом России была поставлена задача организовать исследование природы коррупции в современном российском обществе [34]. Основанием для постановки подобной задачи стало отсутствие в отечественном законодательстве, как, впрочем, и в правовых актах других стран, унифицированного понятия, отражающего сущность исследуемого явления [35], что затрудняет формулирование индикаторов, позволяющих своевременно выявлять, пресекать и предупреждать коррупционные проявления [36]. В контексте данной работы под индикатором коррупционной деятельности понимаем доступные наблюдению и оценке характеристики деятельности должностных и иных лиц, позволяющие судить о коррупционном характере их действий, недоступном непосредственному наблюдению [37].

Попытки сформулировать определение коррупции отмечены на ранних этапах истории античных обществ [38], в которых еще не было профессиональных чиновников, но уже возникали проблемы, связанные со справедливостью решения имущественных вопросов и властных решений.

В качестве индикатора коррупционных проявлений, первоначально рассматривались отклонения от справедливости в деятельности должностных лиц [39, 40, 41, 42, 43].

Н. Макиавелли указывал на опасность коррупции, обусловленную использованием различными служащими доверенных им публичных возможностей «в частных интересах», что также можно рассматривать в качестве индикатора коррупционных проявлений [44].

Ж.Ж. Руссо, Ш. Монтескье, Ф. Бэкон в своих научных работах характеризовали коррупцию, как значимую социально-политическую проблему, так как в условиях становления капиталистических отношений, даже власть, под влиянием коррупции, стала превращаться в товар.

М. Вебер, полагал, что у коррупции нет родины, носителем ее является чиновничество, которое может исчезнуть только при исчезновении культуры [45], поэтому коррупцию невозможно победить, но необходимо минимизировать до приемлемого уровня.

С. Хантингтон допускал ограниченную возможность использования этого негативного феномена, принимая во внимание особенность коррупции создавать условия для приспособления к жесткой организации государства и общества, выступая в качестве «масла», благодаря которому экономика развивается более динамично [46]. Аналогично высказывался Крис Блаттман считавший, что коррупция, выступая в качестве смазки, уменьшает трение при контактах государственного механизма и экономики в странах с избыточным госрегулированием [47]. Однако Г.Мюрдаль, на основе анализа ситуации в ряде восточноазиатских стран утверждал, что коррупция способна принести только нищету [48].

1.2.2. Определение понятия «коррупция» в современной юридической науке

В конце XX века начинается формирование современного понимания сущности коррупции, как социально-правового явления, порождаемого многочисленными факторами6:

- содержание коррупции включает возможность подкуп служащих, что влечет за собой нарушение нормального функционирования системы государственной власти [49];

- коррупция представляет собой использование представителями власти своего служебного положения для получения имущественных и неимущественных благ вопреки действующему законодательству [50];

- коррупция выражается в моральном разложении и незаконном обогащении должностных лиц, срастании властных структур с социально-аномальной средой [51];

- коррупция выражается в использовании должностным лицом своих полномочий для получения личной выгоды, что связано с нарушением правовых норм и нравственных установок [52].

- коррупцию следует рассматривать как совокупность преступлений, совершенных, совершаемых и подготавливаемых с прямым умыслом и корыстным мотивом должностными лицами с использованием ими своего должностного положения и имеющихся полномочий, вопреки законным интересам граждан, общества, государства [53];

- коррупция представляет собой понятие, одновременно и социальное и криминологическое, следовательно, она должна оцениваться не как конкретный состав преступления, а как совокупность родственных видов деяний, направленных против интересов личности, общества и государства, в частности, таких как подкуп государственных и муниципальных служащих, корыстное использование служебных полномочий и др. [54];

- коррупция поражает не только сферу деятельности государственных и муниципальных органов, но и коммерческую сферу, превращает властные полномочия в товар, разрушая понятие социальной справедливости [55].

Анализ приведенных в историко-философских источниках определений коррупции, позволяет рассматривать в качестве ее индикаторов, необходимых при разработке мер и юридических механизмов противодействия коррупции в условиях цифровизации государственного управления и экономики, следующие элементы этого негативного феномена:

- отклонения от справедливости в деятельности должностных лиц;

- нарушение чиновниками действующих правил с целью личного обогащения;

- неосновательное обогащение должностных лиц;

- нарушение запрета одному лицу в государстве занимать ряд должностей;

- несоответствие доходов и расходов чиновников уровню их заработной платы;

- использование служащими доверенных им публичных возможностей «в частных интересах»;

- «воцарение» чиновников на своем месте, отсутствие ротации кадров;

- взяточничество чиновников;

- хищение и срастание с криминальными структурами;

- принятие подарков и подношений в связи с исполнением служебных обязанностей;

- отсутствие гласности в деятельности публичной власти.

Отсутствие систематизированных знаний о природе коррупции и универсального определения коррупции обусловлено многоаспектностью коррупционных проявлений.

С другой точки зрения, не определившись с криминологическим содержанием явления, весьма проблемно пытаться воздействовать на это явление в конструктивном направлении. Для достижения этого результата, необходимо переосмыслить подходы к исследованию природы коррупции и используемые меры противодействия этому негативному феномену, использовать современные достижения научного прогресса, в том числе разработки искусственного интеллекта.

1.2.3. Теоретико-методологические подходы к определению понятия коррупции в международном законодательстве

Изучение подходов и принципов формирования понятия коррупции в международных правовых актах позволяет лучше понять логику построения отечественных нормативно-правовых актов, регламентирующих противодействие коррупции, так как при их подготовке был учтен опыт зарубежных антикоррупционных технологий, показавших высокую эффективность в противодействии рассматриваемому феномену. Анализ международных антикоррупционных правовых актов позволяет констатировать, что они не содержат универсальной дефиниции коррупции.

Одним из наиболее значимых документов в плане установления содержания коррупции, является Конвенция по борьбе с подкупом иностранных должностных лиц [56], в которой понятие «коррупция» заменено в ней перечислением деяний, подлежащих криминализации.

Вторым по значимости международным правовым актом, определяющим сущность коррупции выступает Конвенция об уголовной ответственности за коррупцию [57] в которой качестве основного коррупционного деяния прописан подкуп должностных лиц исполнительной и законодательной власти, международных организаций; судей и

должностных лиц правоохранительных органов, представителей частного бизнеса, который различают как активный и пассивный.

Третьим по значимости документом является Конвенция против коррупции ООН [58], которая, как и вышеуказанные документы, не раскрывает термин «коррупция», но дает возможность определить его сущностное содержание путем анализа, приведенного в тексте, перечня коррупционных деяний, подлежащих криминализации.

В Модельном законе СНГ [59], также входящем в число международных правовых актов, определяющих сущность коррупции, данный феномен определяется как подкуп, либо незаконное использование должностным лицом своего статуса, в целях получения выгоды имущественного или неимущественного характера для себя, или других лиц, вопреки законным интересам общества и государства.

Таким образом, опираясь на международные правовые акты, устанавливающие содержание понятия «коррупция», можно отнести к числу признаков данного явления противоправное использование должностным лицом, руководствующимся корыстной целью и прямым умыслом, своего публичного статуса, регламентирующего постоянное, временное либо по специальному полномочию выполнение должностных или служебных обязанностей, а также управленческих функций.

Системный анализ положений международных антикоррупционных документов позволяет вывести понятие коррупции через интеграцию указанных в правовых актах наиболее существенных признаков этого явления, в качестве которых следует выделить различные формы подкупа в государственном и частном секторе, вымогательство, хищения, торговлю влиянием, легализацию финансовых средств, полученных преступным путем. Наряду с имущественными выгодами, предметом коррупции могут выступать выгоды неимущественного характера.

1.2.4. Теоретико-методологические аспекты противодействия коррупции в российском законодательстве

В Российской Федерации за последние десятилетия создана современная правовая основа антикоррупционной деятельности, разработаны антикоррупционные стандарты, сформирована система государственных органов и общественных комиссий, реализующих антикоррупционные технологии, внедрены технологии антикоррупционного просвещения и дополнительного образования государственных и муниципальных служащих, существенно возросла гласность принимаемых мер вне зависимости от служебного положения лиц, арестованных за совершение преступлений

коррупционной направленности. Отмечено, что противодействие коррупции оказывает не только благотворное влияние на развитие государства, но и одновременно способствует совершенствованию природы людей, формированию условий для перехода индивидов на новые уровни сознания. Поэтому научное сообщество стремится к более глубокому познанию сущности коррупции, установлению признаков этого социально-правового явления, выступающих в качестве индикаторов, демаскирующих коррупционные проявления, исследованию детерминант и перспектив развития коррупции, происходящего параллельно с развитием общества.

Эффективность правовых норм, регламентирующих противодействие коррупции, во многом зависит от точности определения природы коррупции в современной России [60].

В настоящее время в отечественной научной литературе сложились две основные точки зрения по данному вопросу:

- понимание сущности коррупции как взяточничества, подкупа;

- определение коррупции как разложения механизма государственного управления [61].

Для углубленного изучения причин и факторов, способствующих сохранению коррупционных отношений в Российской Федерации, особенностей восприятия населением коррупции в современный период, установления концептуальных оснований и теоретико-методологических аспектов противодействия коррупции в условиях цифровизации государства и права, в рамках настоящей НИР, Южно-Российским институтом управления РАНХиГС при поддержке Института права и национальной безопасности РАНХиГС при Президенте России 17 апреля 2020 года проведена Всероссийская научно-практическая конференция с международным участием «Противодействие коррупции на государственном и муниципальном уровне в современной России» [62]. При подготовке конференции в марте-апреле 2020 года осуществлен социологический опрос методом анкетирования в 13 субъектах РФ, в котором приняло участие 1080 экспертов. Результаты опроса приведены в сборнике информационно-аналитических материалов [63].

Согласно материалам экспертного опроса 42,2% экспертов традиционно для нашей страны воспринимают коррупцию как получение или дачу взятки. На вторую ранговую позицию эксперты поставили использование должностного положения в личных корыстных целях. Подарки должностным лицам, которые еще несколько лет назад многие граждане не считали проявлением коррупции, поставлены на третью ранговую позицию. Основную опасность коррупции для личности, общества, государства эксперты видят в

том, что коррупция сводит на нет уровень политической лояльности граждан к государству и его политическим лидерам, поскольку последние не соблюдают закон, и их действия противоречат принципам справедливости, на что много веков назад указывали Гесиод, Гераклит, Платон и Аристотель.

Нормативно-правовое определение коррупции в современном российском законодательстве прописано в статье 1 ФЗ «О противодействии коррупции» [64].

Анализ данного определения, сформулированного в форме перечня конкретных правонарушений, гносеологически означает отсутствие перехода в познании рассматриваемого феномена от непосредственного знания о нем к опосредованному. Таким образом, если сущность коррупции не определена, то противодействие данному феномену сводится к борьбе с явлением, сущность которого неизвестна [65].

Стремление законодателя раскрыть понятие коррупции путем перечисления конкретных преступлений, представляется некорректным, так как это, с одной стороны, упрощает понимание этого сложного социально-правового явления, с другой - низводит его содержание до борьбы исключительно с вредными последствиями рассматриваемого явления. Можно согласиться с мнением экспертов о необходимости уточнения дефиниции коррупции [66], раскрывающей сущность этого сложного социально-правового явления, ибо, чем выше точность предписаний нормативных правовых актов, тем выше вероятность их правомерного исполнения субъектами права.

В то же время, несмотря на отмеченные недоработки терминологического характера, Федеральный Закон «О противодействии коррупции» является основным нормативным правовым актом, регламентирующим противодействие коррупции и устанавливающим основные понятия в данной сфере. Опираясь на действующее законодательство, актуализируется задача разработки соответствующих современному развитию научного прогресса алгоритмов противодействия коррупции, связанных с внедрением устройств искусственного интеллекта на рутинных процессах противодействия этому феномену, где труд роботов будет более эффективным, чем труд человека.

1.3. Опыт современных государств в использовании цифровых технологий в противодействии коррупции

1.3.1 Коррупция и «цифра»: постановка проблемы

Ключевым драйвером трансформации современных общественных систем в настоящее время становятся сквозные цифровые технологии. Здесь следует отметить, что под сквозными (или еще их обозначают в качестве дизуруптивных технологий понимают

широкий круг современных инновационных форм, технологий и практик, которые связаны с цифровыми алгоритмическими системами. В этом плане когда используется понятие цифровые технологии следует иметь ввиду, что это по большому счету научная метафора или собирательная категория, отражающая весь спектр цифровых новаций, внедряемых в общества (системы слабого и сильного искусственного интеллекта, технологии блокчейна, автономные роботизированные алгоритмы, формы дополненной и виртуальной реальности и многое другое. Это понятие собирательное, отражающее целый спектр инновационных цифровых технологий – систем искусственного интеллекта, автономных цифровых алгоритмов, роботизированных технологий, цифровых форм виртуальной дополненной реальности.

Все эти цифровые новации и алгоритмические решения, внедряемые в общественное взаимодействие, кардинально меняют социальную организацию общества, и существенно трансформируют формы и практики социальной коммуникации и обмена. Очевидно, что последнее напрямую влияет и на развитие самой коррупции как социального феномена. Очевидно, что с момента возникновения и эволюции государственно-правовых форм организации общества видоизменялась и сама коррупция, а коррупционное взаимодействие трансформировалось с инструментов коммуникации, технологий обмена и проч.

Одно из ключевых направлений научных и экспертных разработок в этой сфере, ориентировано на анализ форм и механизмов использование интернета и виртуальной среды в противоправных целях. Например, для противодействия коррупционным и другим противоправным взаимодействиям исследуется алгоритм причинно-следственных связей деструктивного использования информационно-коммуникационных технологий в интернет-пространстве [67].

Кроме того, отмечается, что современные цифровые инструменты используются для развития такого феномена как «киберкоррупция», которая распространяется на всех уровнях государственного управления, на международном уровне и противодействие ей только национальными юридико-политическими способами сегодня невозможно [68].

Коррупция наряду с другими преступлениями анализируется и в юридико-криминологическом аспекте, как исторически эволюционирующее явление, которое существенно трансформируется и приобретает новые черты, качественные характеристики и траектории развития под воздействием внедрения информационных технологий в противоправных целях [69]. Отмечается, что благодаря бесчисленным

способам злоупотребления информационными технологиями, сегодня наблюдается технологический сдвиг в характере преступлений.

1.3.2. Противодействие коррупции в цифровом мире: обзор зарубежных исследований

Целая плеяда зарубежных научно-исследовательских работ посвящена комплексному междисциплинарному исследованию теоретических, практических и правовых аспектов противодействия современным угрозам, возникающим в киберпространстве, в виртуальном взаимодействии граждан и государства, а также оценки коррупционных рисков и угроз, с которыми люди, предприятия и правительства сталкиваются каждый день в цифровой среде [70]. Это позволяет прогнозировать и моделировать возможные сценарии эволюции коррупционных сетей взаимодействия в современном мире. Здесь можно выделить серию публикаций, которые представляют аналитический, экспертный, эмпирический и другой материал, отражающих развитие цифровых технологий, потенциальных рисков и угроз для общества, национальной и международной безопасности [71].

В основном проявление коррупции и иных киберпреступлений анализируются в настоящее время по четырём взаимосвязанным направлениям:

1) противоправные деяния с использованием современных ИТК (информационно-коммуникативных технологий), направленные против конфиденциальности, целостности, доступности, бесперебойном функционировании и т.п. компьютерных данных и систем;

2) преступления, направленные на различные формы мошенничества с использованием компьютерных систем и получения незаконных финансовых выгод;

3) преступления, связанные с нарушением авторских прав и смежных прав;

4) преступления, связанные с содержанием того или иного контента в цифровой среде, т.е. в содержание противоправной деятельности входит производство, распространение или представление доступа, передача, приобретение, использование, владение запрещенной информации, образов, действий и проч.

В условиях нарождающихся угроз в киберпространстве актуализируется насущная потребность в адекватном объяснении влияния коррупции на развитие киберпреступной деятельности, кибертерроризма и других явлений современной социальной действительности с последующим определением их юридических контуров [72].

На доктринальном уровне остается также открытым вопрос о правоприменительной эффективности юридических мер в отношении актуальных и

нарождающихся угроз цифровой коррупции. В настоящее время имеется достаточно широкий круг научных статей, аналитических материалов, данных о реализации определенных стратегий развития нормативного регулирования отношений в данной сфере. В этом аспекте противодействие киберкоррупции целесообразно рассматривать в контексте развития международного конвенционного механизма борьбы с этим явлением в современных условиях [73], а также в национальном законодательстве сообразно уровню развития правосознания, правовой культуры, юридической техники и организационно-технического потенциала отдельной страны [74].

В целом и общем анализ отечественной и зарубежной специальной литературы, посвященной изучению сквозных технологий и цифровизации социальных отношений в контексте актуальных и нарождающихся киберугроз, позволяет констатировать освещение следующих проблемных аспектов:

1) отсутствие четкого теоретико-методологического и юридического определения «киберкоррупции» и цифровых форм коррупционного взаимодействия;

2) отсутствие адекватных критериев, позволяющих провести отграничение киберкоррупции от смежных с ним киберугроз;

3) наличие нерешенных проблем, связанных с разработкой адекватной системы юридических форм и мер противодействия актуальным и нарождающимся угрозам развития киберкоррупции (различных цифровых форм коррупции);

4) гипотетическое и дескриптивное освещение рисков возникновения деструктивных эффектов, проецируемых в цифровом пространстве в результате широкого распространения и интенсивного применения сквозных технологий в современных условиях научно-технического прогресса;

5) слабое изучение криминологических характеристик цифровых форм коррупционного взаимодействия (состояние, динамика, детерминистский комплекс, тенденции развития, характер общественной опасности и связь с другими формами и видами преступности, социальные и экономические последствия преступности, обусловленные информационными технологиями);

6) регулятивное запаздывание в развитии нормативной правовой базы в контексте предупреждения актуальных и нарождающихся угроз от развития коррупционных цифровых форм.

1.3.3. Основные интерпретации коррупционных фактов

Обобщая современные исследования и юридическую практику в сфере противодействия коррупции в цифровой век трансформации общественных отношений, следует отметить, что в трактовке данного противоправного феномена сохраняются как устойчивые традиционные характеристики, так и привносятся новые элементы в интерпретации последней. Последнее связано с рядом объективных и субъективных характеристик.

Во-первых, уже устоявшимся фактом государственно-правовой жизни общества является то, что коррупция представляет собой устойчивое и неискоренимое (речь может идти лишь об уровни и масштабах этой антиобщественной и противоправной формы взаимодействия) социальное явление. В соответствие с этим, очевидным является и тот факт, что трансформация общественной жизни, форм коммуникации и социального обмена, ведёт и к качественному изменению коррупции, ее сущностных характеристик, форм и направлений проявления и т.д.

Во-вторых, социально-правовое прогнозирование (например, в рамках правовой политики государства) и моделирование (например, в рамках правотворческой и законотворческой деятельности публично-властных органов власти) направлений трансформации коррупционного взаимодействия, появление и развитие новых коррупциогенных факторов, условий, причин должно учитывать ключевые траектории развития общественных отношений и векторы их трансформации. Иными словами, система социально-правовой превенции и юридического противодействия коррупции должно быть адекватно факторам и условиям социальной динамики.

Учитывая данные два фактора, нужно сделать важное замечание, что антикоррупционная правовая политика не должна быть простым отражением новых факторов, условий, причин или прямого копирования инновационных технологий и форм общественной коммуникации. Напротив, последняя должна базировать на формах опережающего правотворчества и социально-правового прогнозирования ключевых трендов трансформации общественных отношений, моделирования возможных форм и условий социального обмена.

В специализированной литературе и на практике последнее получило название «устойчивый эффект предубеждения систем». Самый яркий пример – это разработанная американская автономная технология на основе системы искусственного интеллекта, которая в режиме реального времени работает с большим массивом данных, мониторит целый спектр показателей и высчитывает индекс криминогенности социальных субъектов. Эффект предубеждения данной системы проявился в том, что более высокий уровень

криминогенности система автоматически выставляла чернокожим мужчинам, а также представителям латиноамериканской социальной группы, считая их более агрессивными и склонными к преступности.

Обращаясь к формам противодействия коррупции в современном цифровом мире, здесь следует выделить два аспекта.

Во-первых, это использование цифровых технологий для обеспечения, выработанной на международной арене «единой стратегии» в формах и методах борьбы с коррупцией, сформированной на основе успешного государственного опыта различных стран, являющихся лидерами рейтинга Transparency International.

Во-вторых, это формы противодействия, которые ориентированы на принципиально новые виды коррупционного взаимодействия.

1.3.4 Инновационные формы публично-властной организации общества и коррупция

Цифровые технологии и внедрение интерактивных технологий интенсифицировали развитие четырех инновационных форм публично-властной организации, которые были определены в качестве приоритетных в развитии государств XXI века. Внедрение последних в публичную организацию и процесс управления должны качественно изменить не только систему организации функционирования публичной власти, внутриорганизационных систем управления, формы и методы управленческого воздействия, но и принципы, и систему отношений между государством и гражданским обществом, снизив возможности для бюрократического произвола и коррупционного взаимодействия.

В государственном управлении эти четыре инновационные формы взаимосвязаны и взаимообусловливают друг друга [75].

Во-первых, это e-public network, представляющие собой электронные публичные сети, обеспечивающие мобильное, а главное, постоянно контролируемое цифровыми алгоритмами, взаимодействие различных субъектов публично-властного взаимодействия. Здесь цифровые технологии обеспечивают режим полной открытости и контролируемости любого публично-властного взаимодействия, снижая возможности любого коррупционного взаимодействия (как низового, так и в верхних эшелонах власти). Развитие этой идеи началось достаточно давно, в XX веке

Во-вторых, это перевод в цифровой формат административного публично-властного управления (e-public administration), а также реализацию ключевых, прежде

всего, социальных функций государства с дальнейшим переводом всей государственной деятельности в цифровой формат (или по крайне мере дублирование реальных и виртуальных форматов властно-управленческой деятельности, властной коммуникации между государством и обществом и т.д.) – *virtual state.*

В-третьих, развитие и усложнение цифровых технологий позволило создать концепцию цифровой или электронной демократии (E-democracy, I- democracy, smart-democracy). Данная концепция основывается на широком развитии онлайн культуры граждан и инновационных технологиях организации политического и правового процесса с максимальным вовлечением граждан во все процессы подготовки, принятия и реализации управленческих решений. При этом коррупционный фактор снижается не только за счет последнего, но и переводом всех демократических процедур в электронно-цифровую форму, существенно снижая влияние человеческого фактора на функционирования тех или иных властных институций. В ряде государств создаются официальные публичные сети, организующие открытую коммуникацию в системе личность – общество – государство.

В-четвертых, это цифровые публичные сервисы (e-services), связанные с электронным форматом оказания государственных и муниципальных услуг, минимизирующие возможности для злоупотребления служебным положением и коррупционного взаимодействия. Во втором указанном аспекте дело обстоит сложнее, поскольку цифровые технологии сами порождают новые формы коррупционного взаимодействия. Остановимся здесь более подробно и дадим развернутые пояснения.

Проблематика цифровизации общественных отношений как в частной, так и в публичной деятельности сегодня выступает не только драйвером социально-экономического и политико-правового развития; но и ключевой мировоззренческой установкой, которая полностью трансформирует наши формы мыследеятельности, ключевые практики взаимодействия, изменяет ценностно-нормативные ориентации, установки и проч.

В настоящее время очевидны кардинальные изменения в юридическом мышлении, правовом регулировании, принципиально изменяется юридическая техника и правоприменительная деятельность. Сегодня, уже очевидно, что происходит трансформация некогда устойчивых культурных доминант и оснований различных традиционных социальных нормативных систем (обычая, традиции, право и т.д.). Данные изменения инициированы бурной разработкой и внедрением новых цифровых технологий, образующих принципиально новую связку человека и всевозможных инновационных

продуктов. Эти связи, сцепки, смеси новых технологий и социальных практик формируют и новую эпоху, новый образ мысли и действия. Последнее пока лишено четких ценностных, этических, духовных и других требований и стандартов, что открывает целый простор для злоупотреблений, теневого и внеправового взаимодействия. Это, безусловно почва и для развитие новых форм коррупционного мировоззрения и новых практик коррупционного взаимодействия. Так, имея в своём распоряжении лишь один, но достаточно богатый массив данных о прошлых происшествиях, правоохранительные органы имеют возможность с большой долей вероятности заранее предсказывать места совершения преступлений и даже личности преступников и предупреждать любые реальные правонарушения [76]. Соответственно, происходит обоснование новых абстрактных оснований порядка общественных систем, которые сменяют традиционные социальные институты и нормативные комплексы на цифро-алгоритмический «базис». В современном проектировании развития общественных организаций существуют и умеренные версии будущего, а именно конвергенционного или коэволюционного развития. Последние, предполагают сближение, адаптацию и последующую интеграцию традиционных и цифро-алгоритмических оснований [77].

В соответствие с вышеизложенным необходимо отметить, что инновационные технологии и цифро-алгоритмические решения не только решают вопросы по минимизации традиционных форм и практик коррупционного взаимодействия, но и формируют новые скрытые формы власти и теневые сектора принятия управленческих решений, связанные с разработкой исходных кодов и изначальных алгоритмических решений. В настоящее время «лучший способ получить ответ на вопрос о контроле в мире, полном умных машин, - понять ценности тех, кто фактически создает эти системы» [78].

1.4. Правовая институционализация цифровых технологий противодействия коррупционным отношениям

Использование информационных технологий в правовой политики по противодействии коррупции представляет собой систему комплексных взаимосвязанных программных средств, позволяющих реализовать сложные системные механики динамического отслеживания причин и условий формирования коррупции, признаков коррупционной деятельности, оценки коррупционных рисков, прогнозирование развитие коррупционных правонарушений, комплексной оценки эффективности применяемых средств противодействия. Современные программные средства, телекоммуникационные

системы, базы данных позволяют вести учет множественной информации не имеющий в фрагментарном состоянии какой-либо ценности для реализации правовой политик по противодействию коррупции. Между тем сопоставление отдельных элементов юридически значимых действий, информации во взаимосвязи с субъектами контролируемых государственной системой противодействия коррупции позволяет определить общую картину коррупционных проявлений. Уникальный характер таких технологий стал позволять осуществлять реально эффективные меры не карательного характера как для предотвращения, так и не допущения коррупционных отношений в государственном аппарате и бизнес-среде. Оценивая сегодня систему разработанных и принятых нормативных актов, учреждающих отдельные антикоррупционные институты, можно утверждать, что сегодня сформированы достаточные предпосылки для создания системной цифровой платформы позволяющей объединить разрозненные институциональные решения в единый цифровой комплекс. Очевидно, что такая программная конструкция должна быть представлена модульной структурой, позволяя наращивать потенциал единой цифровой платформы.

В этом ключе следует констатировать естественную связь между модульной конструкцией программных средств и реализуемой в России правовой политикой по противодействию коррупции, в том смысле, что под каждый институциональный программный модуль необходима разработка соответствующих средств правового регулирования, определяющих порядок функционирования каждого института по противодействию коррупции в цифровом формате. Таким образом, актуализируется проблема правовой адаптации существующих институтов по противодействию коррупции к информационной среде, а также разработка новых институциональных решений позволяющих осуществить системную государственную политику по противодействию коррупции программными средствами с применением технологий нейро сетей AI, Big data, интернет-вещей и т.п.

Ключевой антикоррупционный эффект– это формирование условий максимально допустимой прозрачности публичной деятельности должностных лиц. Здесь следует обратить внимание на важную несущую конструкцию концепции, определяющую приоритет формирования условий, при которых коррупционная деятельность госслужащих становится невозможной или с высокой вероятностью изобличаемой за счет информированности общества. По сути речь идет не о последующем, а превентивном антикоррупционном контроле, снижающем как распространённость коррупционных проявлений, так и объем применимости карательных юридических мер, что имеет

потенциал позитивного влияния на развития национальной экономики и правовой культуры населения.

Сегодня результаты общественного контроля во многом подвергаются обоснованной критике со стороны госслужащих в части доминирования субъективных начал в результатах общественного контроля. Со стороны гражданского общества так же формируется устойчивая убежденность в том, что результаты общественного контроля государственной системой контроля не используются, что провоцирует постепенное сворачивание данного гражданского института.

Между тем, разрешению данного противоречия во многом может способствовать формирования комплексного федерального программного решения позволяющего сформировать рефлексивную систему взаимодействия граждан и органов власти по противодействию коррупции.

Важным модульным элементом, обладающим потенциалом интеграции в общую систему антикоррупционной платформы является сервисное решение частных компаний по проверке благонадежности контрагентов. Данные программные продукты, интегрированные в федеральную систему данных фиксирующих коррупционные связи учредителей и работников юридических лиц, позволяют опосредованно воздействовать на коррупционные факторы, создавая антикоррупционные тренды в бизнес-среде.

Соответственно, разрозненный характер таких программных инициатив, разная степень качества их проработки, требует законодательного закрепления и общей регламентации подобных цифровых решений, их лицензирования, объединение в единую модульную федеральную платформу и использование результатов общественного контроля как неотъемлемой части государственного контроля всеми уполномоченными органами власти.

2. Противодействие коррупции в условиях цифровизации государства, права и экономики: технологии, институты и юридические механизмы

2.1 Big Date и коррупция: прогностический анализ основных сфер взаимовлияния и мер противодействия им

2.1.1 Большие данные как экономический ресурс

Большие Данные (англ. bigdata) представляют собой современный экономический ресурс, используемый в сфере информационных технологий при получении, накоплении, систематизации, хранении и использовании значительных объемов структурированной и

неоднородной информации, которые формируются из корпоративных архивов государственных и муниципальных органов, общественных организаций, частного сектора, материалов социальных сетей, форумов, блогов, из показаний датчиков, приборов, средств видеоконтроля и проч.

Исходя из смысла п.1 ст.5 закона «Об информации» Большие Данные следует рассматривать в качестве объекта публичных, гражданских и иных правоотношений.

К числу основных сфер, где активно используются Большие Данные, следует отнести:

- социальные сети, блоги, форумы, текстовый контент, фотографии, презентации, картинки и проч.;

- банковскую сферу, в которой вкладываются значительные средства в оценку возможных коррупционных рисков, в дискретное производство, в аналитические услуги, в работу с клиентскими профилями, направленную на повышение маржинальности, в прогнозировании потоков клиентов в отделениях банков, а также в отслеживание подозрительных транзакций и выявление закономерностей, сигнализирующих о возможной преступной деятельности;

- сферу страхования, где использование Больших Данных позволит в короткие сроки проверить историю страхователя, автоматизировать обработку заявлений и заявок, систематизировать личную информацию о клиентах, группировать их по установленным категориям риска, анализировать статистику страховых случаев, прогнозировать объем и структуру страховых случаев, оптимально рассчитывать суммы страховых выплат, а также моделировать целевую аудиторию для реализации предложений о страховых услугах;

- сферу биомедицины и здравоохранения, где в связи с пандемией коронавируса наиболее остро встала проблема разработки новых программно-технических средств, необходимых для анализа больших объемов информации, с которыми не справляются традиционные алгоритмы анализа;

- сферу мобильной связи, где использование больших данных направлено на формирование портрета клиента, который требует постоянной корректировки, так как в течение короткого времени многие его черты становятся неактуальными;

- энергетическую промышленность, которая, опираясь на Bigdata, рассчитывает энергопотоки в целях повышения эффективности энергоснабжения, путем анализа показаний датчиков повышает надежность энергоснабжения, предупреждает аварии и катастрофы;

- сферу транспорта, где анализ Больших Данных предоставляет возможность рассчитывать грузо- и пассажиропотоки, прогнозировать их изменение, адаптировать логистические потребности к оперативным возможностям, эффективно реализовывать билеты для перевозки пассажиров, изучать рынок в поисках резервов, повышать эффективность использования оборотных средств, обеспечивать безопасность перевозок и защищенность объектов транспорта и граждан от террористических угроз;

- нефтегазовую промышленность, где Большие Данные помогают оптимизировать бизнес-процессы, обеспечить учёт продукции и расчёт цен с учетом конъюнктуры международного рынка, организовать контроль за обеспечением безопасности нефте-газопроводов, антитеррористическую устойчивость инфраструктуры отрасли;

- городскую среду, общественный транспорт, сферу жилищно-коммунального хозяйства, в которых широко применятся цифровые технологии, обеспечивающие экономию бюджетных средств при закупках и прозрачность экономических решений, устраняющих факторы, детерминирующие коррупцию;

- розничную торговлю, где Bigdata позволяют активно проводить маркетинговые мероприятия и алгоритмы рекламы, накапливать, анализировать и использовать большие объемы информации в целях разработки (корректировки) стратегии повышения эффективности бизнеса, продвижения бренда, прогнозирования направлений развития, освоения новых рынков сбыта.

В современной России, по мнению экспертов, цифровизация бизнес-проектов охватила большинство отраслей, однако внедрение этих технологий, в связи с проблемами инвестиционных рисков, находится на начальном этапе, достигая в лучшем случае стадии пилотного проекта. При этом, несмотря на низкую возвратность инвестиций, в ближайшие годы ожидается существенный рост числа проектов и спектра инструментария Больших Данных.

2.1.2. Антикоррупционный потенциал Больших данных

Во многих научных статьях, посвященных вопросам цифровизации социально-экономических отношений, подчеркивается антикоррупционный потенциал цифровизации [79]. Для реализации этого потенциала в Российской Федерации разработана и введена в эксплуатацию специальная программа по созданию сети многофункциональных центров. Поставлена задача перевести в цифровую форму документооборот между государственными (муниципальными) структурами. Это важно не только для органов государственной власти и органов местного самоуправления, но и

для населения, так как цифровизация всей системы государственного управления, повышение ее прозрачности одновременно представляет собой «мощный фактор противодействия коррупции»[80].

Любое обращение индивида к Большим Данным, отраженное в цифровой форме, оставляет цифровой след. И чем больше таких обращений, тем больше информации, позволяющей судить о личности индивида, уровне его образования, целях, мотивах, предпочтениях, материальном положении, его связях, изменении географии проявления его цифровых следов и проч. Таким образом, Большие Данные содержат цифровые следы, характеризующие практически всех физических и юридических лиц, вступающих в коммуникативные отношения в информационной сфере. Однажды возникнув как отражение коммуникации, цифровые следы сохраняются в Больших Данных и при обращении к ним могут способствовать идентификации объекта, оставившего эти следы. Последнее обстоятельство создает реальные условия получения информации в отношении граждан (организаций), совершающих, совершивших или подготавливающих правонарушения коррупционного характера практически во всех сферах жизнедеятельности государства и общества, охватываемых BigData. Возможность получения подобной информации должно позволить не только принимать предусмотренные законом меры для выявления и пресечения вскрытых коррупционных правонарушений и привлечения к ответственности адекватной содеянному лиц, к ним причастных, но и формировать условия для осуществления мер упреждающего характера, направленных на профилактику и устранение (минимизацию) причин и факторов, детерминирующих коррупцию.

Методы выявления преступлений коррупционного характера в сфере Больших Данных, в ряде случаев, могут приобретать интрузивный (проникающий) характер, затрагивающий неотъемлемые права граждан, установленные Конституцией Российской Федерации, такие как право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений[81]. Подобные методы (оперативно-розыскные мероприятия) допускается использовать на основании судебного решения и при наличии условий, оговоренных в статье 8 оперативно-розыскного закона. При этом проводимые мероприятия по своей процедуре должны соответствовать нормам действующего антикоррупционного законодательства.

Указанные методы содержат значительный антикоррупционный потенциал, который содержится как в массивах информации, формируемых уполномоченными законом

субъектами в сферах своей деятельности, так и отражается в социальных сетях, публикациях и репортажах в средствах массовой информации и информационных массивах, относящихся к Большим Данным.

Технология анализа и проверки сведений, представляемых физическими и юридическими лицами в сфере противодействия коррупции, с использованием инструментария Больших Данных, может быть представлена в виде следующего алгоритма:

- представление сведений о доходах, об имуществе и обязательствах имущественного характера;

- анализ представленных сведений с использованием методических рекомендаций Министерства труда и социальной защиты Российской Федерации:

- получение информации от уполномоченных лиц;

- в случае наличия оснований принятие решения о проверке и проведение проверки путем направления соответствующих запросов и получения объяснений;

- по результатам проверки, при наличии оснований, принятие решения о применении взыскания с отражением в соответствующем акте;

- в случае наличия признаков преступления или административного правонарушения, направление материалов в правоохранительные органы.

При реализации данного алгоритма технологии Больших данных используются при первичной оценке представленных сведений с точки зрения полноты и своевременности предоставления. Затем осуществляется сопоставление предоставленных материалов с материалами, которые данное лицо предоставляло в предыдущие периоды и выявление внутренних противоречий. Далее материалы сопоставляются с иными полученными сведениями и результатами анализа открытых источников, имеющих отношение к данному лицу.

Антикоррупционная проверка, осуществляемая с использованием Больших Данных, включает проверку сведений о доходах, об имуществе и обязательствах имущественного характера, анализ достоверности и полноты сведений, представленных гражданами при поступлении на службу, соблюдении ими ограничений и запретов, требований о предотвращении или урегулировании конфликта интересов, а также проверку достоверности и полноты сведений о расходах, соблюдении требований антикоррупционного законодательства бывшими служащими.

В целях проверки полноты и достоверности представленных лицами, указанными в нормативных правовых актах, указанных выше сведений, подразделения и лица,

наделенные соответствующими полномочиями вправе направлять в установленном порядке с использованием инструментария Больших Данных, запросы в правоохранительные и иные федеральные государственные органы, органы местного самоуправления, на предприятия, в учреждения, организации и общественные объединения запросы об имеющихся у них сведениях: о доходах, расходах и имуществе гражданина, его супруги (супруга) и несовершеннолетних детей; о достоверности и полноте сведений, представленных гражданином; о соблюдении им требований к служебному поведению.

В Российской Федерации анализ Больших Данных, характеризуемых высокой степенью интеграции информационных систем и баз данных государственных и коммерческих структур, дает возможность на основе информационных технологий выявлять лиц, причастных к совершению и подготовке правонарушений коррупционного характера:

- оценить объективность сведений о доходах и расходах, представленных государственным (муниципальным служащим, гражданином), оценить адекватность (соразмерность) имущественного положения рассматриваемых категорий лиц их доходам;

- установить признаки представления недостоверных (неполных) сведений, что может свидетельствовать о наличии конфликта интересов либо других правонарушений коррупционного характера;

- вскрыть факты несоблюдения запретов, ограничений и обязанностей, установленных антикоррупционным законодательством для служащих и иных лиц;

- обеспечить реализацию прокурорскими работниками, возложенной на них законом обязанности по обнаружению в ходе анализа сообщений средств массовой информации, сведений о возможных коррупционных правонарушениях;

- обеспечить обмен данными между кредитными организациями и операторами сотовой связи для предотвращения мошеннических и коррупционных схем;

- повысить объективность замеров уровня восприятия коррупции путем применения более совершенных технологий.

- повысить эффективность отслеживания финансовых потоков, укрываемых от налогообложения.

2.1.3. Коррупционные риски в сфере Больших данных

Взаимовлияние BigDate и коррупции может иметь не только антикоррупционную направленность, но и существенно повысить эффективность коррупционных правонарушений, осуществляемых представителями криминальной среды и чиновниками, пытающимися использовать цифровые технологии для извлечения неправомерных выгод, хищений, мошенничества. Цифровизация повлекла за собой рост киберпреступности, появление новых видов преступлений и способов сокрытия следов преступной активности. В.Д. Зорькин прогнозирует ситуацию, при которой группа коррумпированных участников сети сконцентрировашая в своих руках 51% вычислительных мощностей, сможет действовать в собственных интересах, подтверждая только выгодные для себя транзакции [82].

Характерной особенностью многих видов информации, используемой при реализации технологий Больших Данных является то, что она не всегда и не в полном объеме, может быть использована непосредственно после получения, так как:

- во-первых, человек, в силу ограниченности восприятия значительного объема сведений не способен произвести качественный анализ полученной информации, выделить проявляющиеся тенденции, сформулировать выводы, дающие основания для принятия оптимальных решений;

- во-вторых, необходимо не только подвергать анализу возрастающие в геометрической прогрессии объемы поступающей информации, но и сопоставлять выявляемые тенденции и выводы с ранее полученными сведениями, что весьма затруднительно для человеческого интеллекта;

- в-третьих, различные субъекты, заинтересованные в осуществлении анализа BigData, имеют разные формы доступа к информации в силу ее относимости к государственной либо коммерческой тайне, содержания персональных данных и проч., поэтому анализ всей совокупности поступающих сведений доступен далеко не каждому пользователю.

Учитывая изложенное, эффективная обработка значительных объемов накопленной и продолжающей поступать информации может быть реализована лишь в рамках, установленных действующим законодательством и при использовании современных информационных технологий анализа Больших Данных, что позволит получить результаты в форме, доступной восприятию человеческого интеллекта.

2.2. Коррупция на этапе создания «умных городов» и использование потенциала цифровизации городской среды в борьбе с коррупцией

2.2.1 Смарт-города и технологическая зависимость

Определенные риски суверенитету государства, безопасности личности, общества и государства возникают и в связи с развитием «умных городов» (Smart City). Разрабатываемые в Великобритании и США унифицированные и стандартизированные шаблоны моделирования и развития «умных городов», первоначально возникшие на уровне национальных проектов, постепенно становятся образцами на международном уровне.

«Умные города» критически зависят от систем сбора данных, распределения информационных потоков, поступающих с огромного количества датчиков, обрабатываемых с помощью программных алгоритмов искусственного интеллекта, используемых в благих целях обеспечения безопасности граждан, решения и предупреждения экологических, экономических, социальных, инфраструктурных и иных проблем. Стандарты кибербезопасности разработаны в Великобритании, ставшей лидером по развитию технологического и нормативного сопровождения умных городов [83]. Существует специальный словарь, определяющий термины в системах управления «умным городом», формирующий концептуальные основы, виды данных и многое другое. Эта система нацеливает на необходимость наличия общегородского хранилища данных о жителях города и информационных объектах из самых различных источников – начиная от медицинских учреждений и заканчивая правоохранительными органами. Данная база данных называется «Открытые данные» и она может быть использована для различных нужд и потребностей [84].

Типичный умный город состоит из четырех ключевых компонентов, а именно: «Умные сети», Системы автоматизации зданий (BAS), Беспилотные летательные аппараты (БЛА), Smart Vehicles; с включением датчиков Интернета вещей (IoT) и облачной платформы [85]. Сочетание каждого из этих элементов могут порождать новые виды преступлений, причем их круг имеет тенденцию к расширению, поэтому обеспечение надежной и сквозной безопасности является непростой задачей. Трудности ожидают и с позиции уязвимости элементов умных городов от трансграничных воздействий и кибератак со стороны стран-противников.

2.2.2. Идентификация личности и право на без цифровую среду

Основой умных городов является система биометрической идентификации личности. На сегодняшний день идентификация личности осуществляется либо по биометрическим признакам человека, либо с помощью специальных устройств, в том числе и имплантируемых. Здесь могут возникать серьезные риски коррупциогенного характера со стороны инженеров и имплантологов, так как на этапе закладки уже возможны махинации с чипами и номерами. Кроме того, всеобщий и обязательный для всех сбор биометрических параметров человека для хранения и идентификации недопустим с точки зрения прав человека на частную жизнь: принцип добровольности, точнее принцип «неприкосновенности частной жизни, недопустимости сбора, хранения, использования и распространения информации о частной жизни лица без его согласия», закрепленный в ст.3 Федерального закона от 27 июля 2006 года N 149-ФЗ "Об информации, информационных технологиях и о защите информации"[86].

В этой связи возникает вопрос о перспективах безопасности единой системы цифровой аутентичности и идентичности человека, о доступе к этой системе различных государственных организаций и должностных лиц. Большую опасность вызывает и возможность доступа к этим системам зарубежных государственных организаций и транснациональных корпораций, что в условиях вовлечения банков в процесс биометрической идентификации населения трудно ограничить. Кроме того, данная система является важным узлом внедряемой в РФ модели электронного правительства, что представляет собой одну из задач в построении единого глобального информационного общества. Решение видится в нормативном ограничении возможности доступа к этим системам различным структурам, включая уголовную ответственность за нарушение правил работы с ними.

В Великобритании реализация прав человеком не зависит от наличия у него единого документа (паспорта): паспорта граждане этой страны обязаны получать только в случае перемещения за рубеж [87]. В ФРГ правительство отказалось от идеи концентрации сведений о персональных данных на одном сервере или в одной базе данных из соображений национальной безопасности и безопасности человека, жителей страны: «Федеральный Конституционный суд - высший суд ФРГ, следящий за соблюдением Основного закона, еще 30 лет назад постановил: единого средства сохранения всех данных о личности не должно быть. Ведь каждый гражданин по конституции имеет право на информационную тайну, а государство, в свою очередь,

неправомерно следить за гражданами, собирать и в централизованном порядке сохранять данные о них. Во Франции также единый электронный документ отказались внедрять, назвав его прямо тоталитарным и в высшей степени вредным [88]. В США паспорта требуется при выезде за границу, нет единого документа, который обязательно выдается каждому гражданину [89].

В Стратегии развития электронной промышленности России на период до 2025 года фиксируется совсем иной подход – в качестве цели видится единство человека и цифровой реальности: «Внедрение нанотехнологий должно еще больше расширить глубину ее проникновения в повседневную жизнь населения. Должна быть обеспечена постоянная связь каждого индивидуума с глобальными информационно- управляющими сетями типа Internet. Наноэлектроника будет интегрироваться с биообъектами и обеспечивать непрерывный контроль за поддержанием их жизнедеятельности, улучшением качества жизни, и таким образом сокращать социальные расходы государства» [90]. Данная программа развития наряду с созданием единого федерального информационного ресурса, содержащего сведения о населении, порождает новые угрозы и риски в сфере прав человека [91]. Для России риски тоталитарного контроля неизмеримо выше в силу ее исторического опыта и привычного пренебрежения правами человека.

К основным задачам применения информационных и коммуникационных технологий для развития социальной сферы, системы государственного управления, взаимодействия граждан и государства следует отнести сохранение возможности взаимодействия граждан с государственными и муниципальными организациями без применения информационных технологий [92].

2.2.3. Интернет вещей и роботизация

Умные города представляют собой не только городское пространство, построенное в виртуальном мире и оптимизированное с помощью математических систем и алгоритмов. Умные города – это еще и внутридомовые технологии, обеспечивающие безопасную и комфортную среду. «Интернет вещей» или «умные вещи» представляют собой высоко-технологичные, интеллектуализированные устройства, подключенные к Интернету, прежде всего, промышленные и потребительские товары, бытовая техника, видеонаблюдение и т.п. Одно из определений термина "Интернет вещей" было представлено в п. 3.2.2 Рекомендации Международного союза электросвязи Y.2060 (06/2012): это "глобальная инфраструктура для информационного общества, которая обеспечивает возможность предоставления более сложных услуг путем соединения друг с

другом (физических и виртуальных) вещей на основе существующих и развивающихся функционально совместимых информационно-коммуникационных технологий"[93]. Эти устройства легко уязвимы для кибератак, несанкционированного сбора данных для спецслужб зарубежных государств, корпораций, мошенничества и злоупотребления, недобросовестной конкуренции поставщиков товаров и услуг. Например, холодильник с функцией дозаказа продуктов и их покупки в автоматическом режиме может выбирать определенных поставщиков не без помощи удаленного взлома или программирования на этапе производства. При этом программное обеспечение и электронные схемы скрыты от контроля: они защищены как секрет производства (ст. 1465 ГК РФ). По всей видимости потребуется внесение изменений в ФЗ "Об информации, информационных технологиях и о защите информации", "О коммерческой тайне", "О персональных данных"[94] с целью защитить пользователей «интернет вещей» от недобросовестной конкуренции участников рынка. Следует отметить, что весьма спорной выглядит концепция некоторых авторов, предлагающих строго концептуальное отделение личных (персональных) данных от личной информации и оспаривание применимости концепции собственности к личной информации в контексте Интернета вещей (IoT)[95]. Особенно важно определиться с личной информацией в сфере медицинских интернет-вещей: это медицинские изделия, которые с помощью специальных датчиков собирают информацию о пациенте и воздействуют на его здоровье. Это не только фитнес-браслеты, но и устройства, предназначенные для мониторинга, контроля и поддержания состояния здоровья, в том числе инсулиновые и инфузионные помпы, кардиостимуляторы, аппараты искусственного дыхания, электрокардиографы. «Умные устройства данного сегмента позволяют обеспечивать бесперебойный мониторинг уровня кровяного давления, могут в автоматическом режиме вводить необходимые лекарства (в частности, инсулин, химиотерапевтические препараты), снимать кардиограммы и т.д.» [96].

Быстрый рост таких устройств, а также роботизированных и алгоритмизированных киберфизических систем в условиях трансграничной торговли, используемой вне доступа государства в сфере частной собственности, может стать большой угрозой личной безопасности. Системы «умного дома», собирающие и хранящие личные данные, обрабатывающие их для обслуживания клиентов с помощью искусственного интеллекта являются весьма легкими целями для взлома и сбора информации. Законодательно необходимо обязать производителей защищать эти устройства специальными программами защиты. Кроме того, необходимо законодательно определить сферы, в которых применение интернет-вещей и искусственного интеллекта неприемлемо:

вызывает опасения тенденция устранения человека из ряда видов деятельности, как, например, образования, медицины, транспорта, связи, правосудия.

Право вполне эффективно может регулировать и определять каналы внедрений технологических инноваций. Опасаться заурегулированности или торможения технологического развития не стоит, как показывает законотворческий опыт других стран, весьма эффективно регулирующих вопросы анонимности в Интернете, идентификации пользователей, взаимодействия спецслужб и разработчиков программного обеспечения, использования роботов в тех сферах, где их применение нежелательно в силу ряда причин, например, общественной значимости тех или иных профессий, видов деятельности или технологической безработицы.

2.3 Коррупция в условиях цифровизации валютного рынка

В научной литературе достаточно много публикаций посвящено становлению рынка криптовалют, и рискам их использования с целью обхода законодательных ограничений. Основной проблемой формируемого рынка виртуальной валюты называется особый характер ее природы: анонимность владельцев, немонетарная природа, децентрализованный, экстерриториальный алгоритм и т.п. препятствующие традиционным способам государственного контроля за получением имущественных благ государственными служащими и тем самым, многократно возрастающий потенциал коррупционных рисков. Отсюда в научном сообществе и в среде представителей органов государственной власти звучат призывы о полном запрете криптовалюты, как экономического явления, природа которого носит мошеннический характер, или же вообще криптовалюта наделяется статусом экономического оружия.

Анализируя природу криптовалюты, исследователи отмечают, что по своему фактическому использованию ее в экономике она отвечает признакам фиатных денег (используется в качестве средства платежа) [97]. Однако законопроект федерального закона «о цифровых финансовых активах», не меняет общей концепции монополии государства на денежные средства, установленной ст. 140 ГК РФ и ст. 9 Федеральный закон от 10.12.2003 N 173-ФЗ (ред. от 27.12.2019) "О валютном регулировании и валютном контроле" (с изм. и доп., вступ. в силу с 31.05.2020). Как в этой связи отмечают исследователи, - «из системного толкования законопроекта становится очевидным, что цифровые финансовые активы не являются законным средством платежа» [98].

Отсюда возникает проблема, уголовного преследования по преступлениям связанным с криптовалютами, как непризнанного средства платежа [99]. Между тем,

правовая позиция Верховного Суда РФ по вопросам взяток, построена на понимании того что под взяткой следует понимать не только передачу денег, ценных бумаг, или иного имущества, но и любой имущественной выгоды, том числе «цифровых прав»[100] введенных в качестве объекта гражданских прав ст. 141.1 Гражданского кодекса Российской Федерации (часть первая) от 30.11.1994 N 51-ФЗ. Использование законодателем конструкции «цифровых прав», обусловленное принципом технологической нейтральности, тем не менее, включает в себя и понятие критовалюты, как одной из технологий цифрового выражения гражданских прав [101]. В этом же ключе мы видим судебную позицию в отношении отмывания денежных средств, полученных преступным путем, где одной из форм легализации теневых доходов Верховным Судом РФ признана криптовалюта [102]. Продолжая логику выстраиваемой политики финансовой прозрачности оборота криптовалюты аналогичную позицию по декларированию дохода от курсовой разницы криптовалют и майнинга занимает ФНС и Минфин России. В частности в своем Письме ФНС России от 04.06.2018 N БС-4-11/10685 "О порядке налогообложения доходов физических лиц" (вместе с <Письмом> Минфина России от 17.05.2018 N 03-04-07/33234) сообщает об обязанности физических лиц декларировать такие доходы, самостоятельно исчислять суммы налога и осуществлять декларирования дохода от криптовалют.

Важным аспектом, рассматриваемой проблемы является вопрос правового контроля за криптовалютами: ведь их правовое признание или не признание, не устраняет проблемы использования цифровой технологии криминальной средой, в том числе с целью сокрытия коррупционных сделок.

Все криптовалюты основаны на технологии распределенной сети (распределение всей цифровой инфраструктуры между множеством пользователей сети). Это позволяет обеспечить уникальную устойчивость программной инфраструктуре, объединить беспрецедентные вычислительные мощности. На основании этой технологии была разработана технология blockchain, основанная на распределенных реестрах между всеми участниками сети, последовательно записываемыми блоками цифровых операций. На основе blockchain создаются алгоритмы конкретных криптовалют, каждая из которых может подчинятся определенным правилам, установленных программой. В том числе, криптовалюты могут иметь анонимные и персонифицированные алгоритмы. В ситуации елм криптовалюта предусматривает идентификацию лица, технология «blockchain» обеспечивает полную прозрачность, и такая валюта позволяет достоверно изобличить обе стороны коррупционной сделки [103].

Таким образом, можно сделать следующие выводы:

- во-первых, развитие рынка криптавалют в России требует правового регулирования в части идентификации владельцев крипто кошельков, что в настоящее время отражено в ст. 4 проекта федерального закона «о цифровых финансовых активах»[104].

- во-вторых, использование технологии «blockchain» в системе любых расчетов, при условии идентификации пользователей, позволит полностью контролировать любые финансовые операции, не препятствуя свободному рынку.

В правовом пространстве России имеются все предпосылки к созданию эффективной системы противодействия коррупции на активно развивающемся рынке криптовалюты: идет проектирование правовых регуляторов, сформирована правоприменительная позиция Верховного Суда РФ по вопросам легализации (отмывании) денежных средств приобретенных преступным путем посредством криптовалюты и др. Представляется, что следующим шагом должно стать формулирование технических требований, стандартов, сертификации алгоритмов легальных криптовалют, технологических разработок по внедрению национальной криптовалюты.

Обобщая в целом выше сказанное отметим, что, наиболее важным является сбалансированная антикоррупционная политика в вопросах, ограничения формируемого рынка криптовалют, который является не только источником финансирования цифровой экономики России, но и потенциальным средством обеспечивающим экономическую стабильность страны. В этой связи, вряд ли обоснованным представляется позиция изъятия из гражданско-правового оборота криптовалюты, как цифровой формы закрепления имущественных прав граждан и юридических лиц.

2.4. Использование AI в борьбе с коррупцией

2.4.1. Искусственный интеллект и правоприменение: риски и ограничения

Нельзя не обратить внимание на угрозы безопасности человека, дегуманизации и технократизации правоприменения, возникающие в связи с внедрением искусственного интеллекта в правоприменительную деятельность. Этот путь развития права и правосудия будет только усугублять недостатки явно ошибочного, логоцентристского, позитивистского восприятия права, формально-догматического правопонимания. Еще в середине XX века ученые фиксировали кризис права: юридический формализм стал

господствовать над содержательной гранью права. Задолго до цифровизации представители западной интеллектуальной элиты фиксировали нарастающий кризис европейской традиции права, вызванный избыточной формальной рациональностью, механистическим мировосприятием права и правосудия, доминированием формальной законности над справедливостью. Расцвет юридического формализма следует рассматривать как процесс отчуждения человека от права. Его также можно считать «перерождением формальной рациональности»: формально-рациональное начало, обязанное своим появлением проблеме поиска справедливости «не взирая на лица» в рамках «здорового» формализма, призванного в качестве средства обеспечить справедливость на началах равенства, обернулось и заняло место цели, то есть достижения этой справедливости. Творческий аспект деятельности юристов редуцируется и вообще утрачивает свою силу. Происходит эмпирически фиксируемое превращение юридического процесса в нечто “аналогичное производству”, где все сводится к формально-логическому подведению индивидуального под всеобщее» [105]. Объективность в правоприменении посредством искусственного интеллекта достигнуть невозможно и не нужно, так как система правовых норм представляет собой, прежде всего, систему ценностей, защищенных этими нормами. К тому же, эта система носит иерархический характер, что предполагает постоянное сопоставление средств и целей, то есть целеполагание, оценку, субъективность.

Дело в том, что возможность использования искусственного интеллекта на современном этапе его проектирования, точнее сказать, обоснование этой возможности и пределы его использования, должны быть связаны с изучением эпистемологических характеристик правового мышления, логических аспектов правоприменительной деятельности, логическим анализом правового мышления, правоприменительного познания. Искусственный интеллект не обладает важнейшими предпосылками, свойствами и качествами человеческого интеллекта и сознания. Именно в юриспруденции особенно важным является творческий компонент мышления, иррациональная основа принятия решений.

Евросоюз уже принял «Этическую хартию искусственного интеллекта в судебных системах» [106]. Однако, искусственные судьи еще более чем люди зависят от различных предустановок, например, расовых, социально-экономических, конфессиональных и иных предрассудков, так как прогнозируют поведение человека, исходя из таких фактов как личный статус, уровень образования, занятость и т.д.

Внедрение искусственного интеллекта в правосудие влечет за собой дальнейшую дегуманизацию права, увеличивает риски неправосудных и несправедливых решений.

Право на безопасность в условиях цифровой эпохи может исследоваться в двух парадигмах: «безопасности цифры» и «безопасности от цифры». Эти две парадигмы тесно связаны, так как ряд угроз и вызовов совпадают или не могут быть устранены без решения одной из этих задач. Однако искусственное стимулирование цифровизации увеличивает риски.

Полагаем, что в ближайшее время возникнет необходимость в корректировке Доктрины информационной безопасности РФ и разработке Доктрины цифровой безопасности, которая зафиксирует угрозы и риски цифровизации различных сфер социального взаимодействия, сформирует ключевые приоритеты и направления правовой политики государства в сфере цифровой безопасности как отдельной личности, так и государства и общества в целом, а также безопасности государственного управления, правовой, экономической, политической и других общественных систем.

На доктринально-правовом уровне является важным формирование государственно-правового механизма и правовых режимов цифровой безопасности общества, гарантированности и защиты прав граждан и человека в цифровой среде, формирование системы ограничений и запретов, обеспечивающих данную безопасность, которые может в последствие стать особым разделом кодифицированного нормативного правового акта – Цифрового кодекса Российской Федерации.

2.4.2 Нейросети и искусственный интеллект в борьбе с коррупцией

В настоящее время ведущими государствами разрабатываются системы и технологии мониторинга и прогнозирования различным правонарушений, основанные на нейронных сетях и систем искусственного интеллекта. В рамках противодействия и превенции коррупционного взаимодействия можно выделить следующие основные направления.

Во-первых, это использование систем искусственного интеллекта в мониторинге и обработки больших данных, ориентированные, с одной стороны, на прогнозирование возможных мест, сфер и форм коррупционного взаимодействия, с другой – это выставление индивидам индекса криминогенности, склонности того или иного субъекта вступить в коррупционные связи (системы так называемой предикативной полиции [107].

Во-вторых, это системный мониторинг больших данных, направленный на выявление или прогнозирование потенциальных конфликтов интересов.

В-третьих, на основании вышеобозначенных систем и роботизированных комплексов в настоящее время в развитых странах (Италия, Германия, Китай и т.д.) строится мобильные коррупционные матрицы/карты [108].

В-четвертых, нейронные сети и технологии, основанные на системах искусственного интеллекта используются и в отслеживание перемещений и деятельности, например, сбежав коррупционеров за границу, их связи и контакты из заграницы с людьми, чиновниками, финансовыми и другими институтами на родине [109].

В-пятых, это технологии, которые работают также в качестве экспертных систем, прогнозирующих и блокирующих социальную, экономическую, политическую и другую активность коррупционера. На основании баз данных осуществляется блокировка лиц, компаний и организаций, участвовавших в коррупционных делах [110].

3. Стратегия антикоррупционной безопасности в условиях цифровой экономики

3.1. Моделирование антикоррупционной правовой политики в условиях цифрового государства

Анализ роста влияния коррупции на состояние национальной безопасности порождает необходимость исследования такой важной составляющей системы национальной безопасности, как антикоррупционная безопасность.

Антикоррупционная безопасность представляет собой «состояние защищенности жизненно важных интересов личности, общества, государства от коррупционной деятельности» [111].

Существенный вклад в исследование сущности безопасности внес Абрахам Гарольда Маслоу, который в XX веке определил безопасность как одну из жизненно важных потребностей человека, указав, что представления о безопасности возникают на уровне чувств, а не на уровне рефлексии, как считалось ранее. Маслоу указал, что безопасность представляет собой внешний, отсутствующий в организме человека феномен, потому последний испытывает в нем нужду. Важный вывод, который следует из рассуждений Маслоу, заключается в том, что безопасность представляющее собой свойство не субъекта или объекта каких-либо отношений, а метода взаимодействия субъекта и объекта. Изложенное позволяет раскрыть сущность безопасности как качество, присущее различным способам предотвращения опасности, в контексте настоящей НИР, возможности избежать (минимизировать) опасность коррупции.

Анализируя понятие «антикоррупционная безопасность», мы может его раскрыть:

- как конечный результат *реализации комплекса мер по обеспечению антикоррупционной безопасности;*

- как процесс реализации уполномоченными на то законом субъектами мер по обеспечению антикоррупционной безопасности, включающий определение правовых принципов отношений между участниками данного процесса, разработку правовой основы их деятельности, выявление и предупреждение причин и условий, детерминирующих угрозы антикоррупционной безопасности;

- непрерывный выбор, осуществляемый государством и обществом между стремлением к повышению эффективности экономики, росту прибыли и противодействием коррупционным проявлениям, затрудняющим (исключающим) возможность реализации интересов не только представителей криминальной среды, но и правопослушных предпринимателей.

Задача обеспечения антикоррупционной безопасности следует из Концепции общественной безопасности в Российской Федерации, в которой коррупция отмечена в числе угроз России. В Стратегии национальной безопасности Российской Федерации коррупция уде фигурирует в числе наиболее существенных внутренних угроз национальной безопасности. Общая норма об ответственности граждан и юридических лиц за совершение коррупционных правонарушений, прописана в части 1 статьи 13 Федерального закона «О противодействии коррупции», из которой следует, что граждане Российской Федерации, иностранные граждане и лица без гражданства за совершение коррупционных правонарушений несут уголовную, административную, гражданско-правовую, дисциплинарную ответственность.

В то же время, несмотря на пристальное внимание к проблеме обеспечения антикоррупционной безопасности со стороны государства и общества, реальная жизнь свидетельствует о необходимости корректировки основных подходов к формированию целостной системы обеспечения данного вида безопасности, прежде всего, на региональном уровне, который учитывая размеры нашей страны, приобретает ключевое значение, как фактор социально-политической стабильности государства.

Технология совершенствования антикоррупционной безопасности, по нашему мнению, должна включать:

- анализ, оценку и прогноз угроз личности, обществу, государству со стороны возможных коррупционных проявлений;

- планирование антикоррупционных мер, осуществляемых уполномоченными законом субъектами;

- совершенствование нормативно-правовой и методологической основы противодействия коррупции;

- разработку и внедрение специальных экономических мер, направленных на противодействие коррупции;

- организацию финансирования научно-исследовательской работы в сфере обеспечения антикоррупционной безопасности;

- координацию деятельности по обеспечению антикоррупционной безопасности на федеральном и региональном уровнях власти, с местным самоуправлением и общественными организациями;

- повышение роли российских духовно-нравственных ценностей, благодаря которым у населения формируется уважительное отношение к своему Отечеству, при реализации положений антикоррупционной безопасности;

- проведение продуманной информационной политики при обеспечении антикоррупционной безопасности.

Таким образом задача разработки системы обеспечения антикоррупционной безопасности приобретает на современном этапе развития Российской Федерации первоочередное значение.

3.2. Новые сферы коррупции и финансовая теневизация коррупции

Развитие теневых форм социального взаимодействия в цифровую эпоху наиболее опасное условие для развитие антикоррупционных практик, которые, с одной стороны, весьма активно стимулирует развитие вредоносных для общества и государства форм отношений, а, с другой – создают пространство для масштабного вовлечение новых субъектов публично-властных отношений в коррупционного взаимодействие. Этому способствуют два ключевых фактора:

Первый фактор является вполне традиционным для государственно-правовой сферы, тем не менее, исследованию последнего отводится достаточно мало внимания. Кроме того, сегодня практически не разрабатываются правовые режимы и социально-правовые механизмы противодействия данному фактору.

Второй фактор, о котором речь шла выше, связан со спецификой цифровой трансформации общества. И, что совершенно очевидно, не учитывался до последнего времени, не становился объектом комплексного и всестороннего исследования, а, тем

более, областью предметом правового регулирования. Речь идёт о теневом пространстве разработки исходных кодов и первоначальных алгоритмических решений при создании конкретных информационно-коммуникативных систем, роботизированных технологий, автономных цифровых программ, цифровых технологий (например, блокчейн), систем слабого и сильного искусственного (или спроектированного) интеллекта и т.д.

В настоящий момент вся эта деятельность находится «за пространством» нормативного правового регулирования, общественного контроля, не нормируется ни этическими кодексами и нравственными стандартами, ни иными ценностно-нормативными и идеологическими регуляторами. При необходимо учитывать тот факт, что разработка вышеобозначенных сквозных цифровых технологий, реализуется в теневом пространстве и сегодня общество не имеет механизмов контроля и влияния на данный процесс. Соответственно, внеправовые формы публично-властной деятельности, а также теневизация процессов разработки и внедрения современных цифровых технологий и алгоритмических решений формируют новые угрозы и риски для развития современных общественных систем.

В рамках формирования адекватной антикоррупционой политики следует подчеркнуть, что сфера отношений, связанная с разработкой и внедрением цифровых форм и роботизированных технологий постоянно изменчивая и слабо прогнозируемая. Поэтому, в стратегическом плане здесь важны не только негативные эффекты, которые могут появится от развития неправовых и теневых практик, но и возможные позитивные следствия, значимые для формирования нового правопорядка в цифровую эпоху.

Речь идёт главным образом том, что внеправовая деятельность и теневые практики могут выступить в качестве апробации и легитимации будущих государственно-правовых форм воздействия и управления цифровыми формами взаимодействия людей друг с другом, человека и машины. Например, сформированные в рамках пандемии формы государственного воздействия или управления, с помощью цифровых технологий могут в силу своей эффективности, адекватности и социальной приемлемости (т.е. результаты управленческого воздействия были признаны обществом в качестве приемлемых) быть «переведены в юридическую оболочку», зафиксированы в действующем законодательстве и войти в устойчивую юридическую практику. Кроме того, важный аспект деформации правого и, прежде всего, профессионального правосознания связан и с проблематикой автоматизации бюрократических процедур профессиональной деятельности, в процессе которой содержание и смысл той или иной деятельности полностью выхолащивается рутинными и автоматическими процедурами. При этом не важно реализуются последние

через алгоритмические системы (например, цифровые формы обработки обращений граждан, их учете и классификации) или непосредственно должностным лицом (например, выполнение рутинных и типичных операций).

Цифровые коммуникационные технологии и различные алгоритмические решения, используемые на скрытых цифровых платформах теневых сетях (например платформы темной стороны интернета, так называемый darknet) ведут к институционализации и распространению в системе публично-властных отношений теневых практик и структур. С помощью цифровых форм коммуникации и «теневого аппаратного обеспечения» создаются скрытые формы и теневые правила сетевого коррупционного взаимодействия. При этом данные сквозные цифровые технологии стимулирует не только количественное, но и качественное развитие коррупционных сетей.

Развитее коррупционных сетей активизирует также процессы системной деформализации официальных норм и требований, а теневые практики и правила начинают замещать нормативно-правовые модели и официальные этические кодексы служебного поведения.

В большинстве случаев частные системы, конфликтующие с системой официальной, возникают из-за вакуума власти, отсутствия должной либо адекватной урегулированости определенного сектора общественного взаимодействия.

3.3. Коррупционные риски в процессах цифровизации правосудия и использования AI в механизме правового регулирования

Правовая политика государства должна своевременно реагировать на цифровизацию традиционных форм коррупции и появления новых феноменов – e-corruptions (электронной, цифровой коррупции) [112].

С точки зрения адекватного моделирования правовой политики государства, что понятия цифровая трансформация и четвертая промышленная революция, это *концептуально широкие понятия*, используемые, как правило, в качестве научных метафор. Очевидно, что «размытое» видение объекта и предметного поля исследования не позволяет сформировать адекватную систему управленческого воздействия, что не только не гарантирует, но и весьма затрудняет выработку эффективной правовой политики в сфере цифровой трансформации различных сфер общественного взаимодействия.

Четвертую промышленную революцию в современной литературе содержательно описывают в качестве процесса повсеместной цифровизации всех созданных человечеством артефактов, социокультурных материалов и информации, перевод в цифру

различных форм взаимодействия и видов коммуникативной активности, а также тотальная виртуализация разнобразных связей (отсюда и появление таких специфичных явлений как е-коррупция, проекционное коррупционное взаимодействие и др.).

Процессы цифровизации связаны также с переводом различных социальных ресурсов физических и материальных объектов, символических ресурсов в виртуализированную (цифровую) среду. При этом революционность цифровизации заключается еще и в том, любое взаимодействие, обмен, накопление и проч. генерируется, контролируется и реализуется через системы алгоритмических решений и автономных цифровых систем.

Аналитически можно выделить пять основных уровней развертывания данного феномена, каждый из которых может при более содержательном рассмотрение дифференцирован. Моделирование антикоррупционной политики необходимо формировать по этим уровням, для адекватного эффективного противодействия развитию коррупционного взаимодействия в цифровую эпоху развития общественных систем.

Первый уровень условно можно обозначить в качестве *базисного, изначального уровня цифровой трансформации*. В качестве цифрового базиса выступают изначальные цифровые коды и алгоритмические решения, которые, закладываются в системы машинного обучения и спроектированных интеллектуальных систем (более известно в качестве популярного, но далекого от реальности понятия – искусственный интеллект). Именно последние закладывают перспективу развертывания как отдельных цифровых систем, так и траекторию развития различных инновационных технологий.

Этот уровень сегодня находится *вне какого-либо социального контроля и нормирования*. Как следствие, в дельнейшем формируются и развертываются специфические формы и режимы публично-властной деятельности, при которые реальные центры принятия решения и влияния размещаются за действующей системой общественного контроля [113].

Второй уровень отражает реальные повседневные практики, связанные с переходом в общественном взаимодействии от аналоговых технологий к цифровым. Содержание данного уровня сегодня находится «под пристальным вниманием» всего корпуса социально-гуманитарных наук (юриспруденции, политологии, социологии, философии, экономики и т.д.). Этот уровень можно обозначить также в качестве инструментального, поскольку здесь разворачиваются процессы, связанные со сменой основных инструментов и технологий в человеческой жизнедеятельности [114].

Третий уровень связан, прежде всего с институциональными практиками и их изменениями под воздействием «оцифрофизации» социальной коммуникации и общественной организации. Именно на этом уровне разворачивается целая серия противоречий между традиционными общественными основаниями порядка и новыми институциональными изменениями, вызванными политикой внедрения цифровых форм и алгоритмических решений в разнообразные социальные практики. В рамках антикоррупционой политики необходимо прогнозировать активное действующее участие разнообразных автономных, алгоритимических и интеллектуальных систем в противоправном взаимодействие и коррупционном обмене.

Четвертый уровень, это институциональное измерение современной общественной организации, уровень действующих институциональных структур (экономических, политических, юридических, культурных).

Пятый уровень, отражает ценностно-нормативные, культурные и этические основания цифровой трансформации государства, права, общества. В рамках данного уровня формируется и реализуется общая система национальной безопасности, воплощается и гарантируется национальный интерес (сбалансированная система гарантий и защиты интересов личности, общества и государства).

Отправной точкой системной политики государственной поддержки развития технологий искусственного интеллекта (далее AI) является Указ Президента РФ "О развитии искусственного интеллекта в Российской Федерации" [115]. Применение технологии AI в системе противодействия коррупции, согласно Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации", имеет определенные ограничения, определяемые через ключевые принципы развития технологии AI.

В реализации политики противодействия коррупции посредством технологий AI необходимо также учитывать, что сама технология AI основана на ряде сопутствующих технологических решений, развитие которых неразрывно связанно с самой технологией нейросетей, в том числе это технология малых и больших данных, технология blockchain, которая позволяет выявлять нейронным сетям не удаляемые следовые характеристики юридически значимых решений, транзакций, таким образом, многократно увеличивая вероятность выявления признаков коррупционных правонарушений, доказуемость коррупционных актов [116].

4. Программа профилактики и противодействия коррупции в условиях цифровой экономики Правительства РФ

1.Основные принципы профилактики и противодействия коррупции в условиях цифровой экономики

Профилактика и противодействие коррупции в условиях цифровизации государственного управления и общественной жизни осуществляется в соответствии со следующими принципами:

1) Принцип верховенства прав человека и гарантий цифровой безопасности личности;

2) Принцип справедливости в отношениях между органами государственной власти, осуществляющих антикоррупционную деятельность и гражданином;

3) Принцип обеспечения национальной безопасности в процессах цифрового контроля за деятельностью органов публичной власти при обеспечении их транспарентности и открытости;

4) Принцип информационной поддержки в сети Интернет и социальных сетях принимаемых антикоррупционных решений в цифровой среде;

5) Принцип соразмерности при использовании цифровых мер контроля за деятельность государственных служащих с обеспечением права на частную жизнь граждан;

6) Принцип взаимодействия органов государственной власти и структур гражданского общества в процессах цифровизации антикоррупционной деятельности государства;

7) Принцип международного сотрудничества с международными структурами, правоохранительными органами иностранных государства в целях обнаружения граждан, совершивших преступления либо подозреваемых в них, их имущества, связей и отношений с иностранными коммерческими и иными структурами, получения необходимой для цифрового контроля информации и согласования взаимных действий;

8) Принцип соответствия всех принимаемых мер цифрового противодействия коррупции традиционным духовно-нравственным ценностям народов Российской Федерации.

2. Основные направления цифрового противодействия коррупции государственных и иных структур, в том числе институтов гражданского общества:

2.1. В сфере технологического развития:

- разработка программно-аппаратных комплексов, позволяющих минимизировать контакты чиновников и граждан – потребителей госуслуг;

- создание специальных сервисов, достигающих максимальной прозрачности управленческой деятельности в сфере финансовых процессов;

- оптимальная и полноценная цифровизация наиболее коррупциогенных сфер;

- разработка специальных технологий, гарантирующих цифровую и информационную безопасность личности, общества и государства;

- устранение административных барьеров для бизнеса с помощью автоматических порталов регистрации субъектов экономической деятельности;

- создание новых программно-аппаратных комплексов на основе технологии блокчейн для проведения электронного голосования;

- разработка систем искусственного интеллекта с целью поиска и выявления конфликтов интересов, выявление коррупционных отношений с помощью специальных программных поисковых систем и «больших данных».

2.2. В сфере нормативно-правового обеспечения:

- борьба с монополизацией цифровых рынков, особенно в сфере образования и финансовых услуг посредством налогового стимулирования;

- разработка законодательных ограничений использования искусственного интеллекта без институтов общественного контроля;

- принятие уголовно-правовых норм, предусматривающих ответственность разработчиков программного и аппаратного обеспечения за предустановленные скрытые программы – шпионы, программы сбора информации, торговлю данными и «закладки» на уровне антикоррупционных норм;

- создание специального портала антикоррупционного омбудсмена.

3. Основные меры, направленные на профилактику и противодействие коррупции в условиях цифровой экономики и цифровизации государственного управления

3.1. Профилактические меры в сфере коррупционных связей и отношений в условиях цифровизации предполагают:

- разработку стратегии развития цифровых технологий противодействия коррупции с учетом как естественных, социальных, экономических, правовых, культурных пределов применения цифровых технологий, так и оценки их потенциальной разработки, перспективного определения этапов их внедрения, в том числе с учетом мероприятий, направленных на преодоление существующих ограничений их внедрения;

- осуществление комплекса мероприятий, сочетающих технологические меры с социально-экономическими и политико-правовыми методами воздействия: формирование в обществе нетерпимости к коррупционному поведению;

- антикоррупционная экспертиза всех технологических инноваций;

- формирование с помощью цифровых технологий специальных цифровых досье на всех кандидатов, претендующих на замещение государственных или муниципальных должностей, поиск подтверждений сведений, представляемых указанными гражданами.

- использование институтов общественного контроля за реализацией антикоррупционных норм в цифровой среде.

3.2. Осуществление комплексной политики в сфере противодействия коррупции в цифровой среде:

- внедрение цифровых платформ совместной деятельности государственных и не государственных органов и институтов по проблемам противодействия коррупции в цифровых сферах;

- использование методов правового стимулирования для активного вовлечения всех граждан к борьбе с коррупцией;

- обеспечение широкого и полноценного доступа граждан к информации об исполнении наказания в отношении коррупционеров

- реализация специальных интеллектуальных технологий отслеживания реализации принципов добросовестности, открытости, добросовестной конкуренции и объективности при осуществлении закупок товаров, работ, услуг для обеспечения государственных или муниципальных нужд;

- взаимодействие с иностранными государствами в сфере совместного цифрового контроля в ходе борьбы с коррупцией;

- автоматизация контроля в сфере разрешения конфликтов и споров, изложенных в обращениях различных лиц;

- установление ответственности и создание специальных подразделений определение подразделений или должностных лиц, ответственных за профилактику коррупционных и иных правонарушений;

- использование сетевых интеллектуальных технологий по поиску конфликта интересов и ошибок при сдаче поддельных документов и отчетности.

ЗАКЛЮЧЕНИЕ

В связи с развитием цифровых технологий государство активно развивает и стимулирует программу цифровизации и технологической модернизации экономики, государственного управления, правового регулирования. Особенно это влияние очевидно на фоне проблем обеспечения национальной безопасности Российской Федерации. Риски и вызовы национальной безопасности в эпоху цифрового мира становятся особенно явными в контексте цифровой глобализации, под которой следует понимать формирование нового миропорядка, конструируемого и управляемого с помощью цифровых технологий в единстве сетевой, коммуникационной и мировоззренческо-смысловой структуры. Представляется правильным говорить в таком случае о цифровой безопасности как важнейшем элементе национальной безопасности, но не в смысле технологической защиты информации.

В современном мире появляется всё больше разнообразных исследований самых различных направлений, отраслей и научных дисциплин, анализирующих современные подходы и способы внедрения цифровых решений в систему противодействия коррупции как в повседневной бытовой жизни, так и в комплексе мер антикоррупционной правовой политики. Популярность цифровых технологий обусловлена серьёзным увеличением гласности и открытости в деятельности органов государственной власти. Помимо этого, информационно-цифровые технологии позволяют ограничить и минимизировать разнообразные формы взаимоотношений между гражданами и должностными лицами, четко контролировать расходы и доходы представителей органов государственной власти, должностных лиц сотрудников правоохранительных органов. Увеличение степени

прозрачности в деятельности представителей чиновничества определена различными нормативными актами, в которых фиксируется принцип публичности и открытости деятельности органов государственной власти.

Коррупция наряду с другими преступлениями анализируется в юридико-криминологическом аспекте, как исторически эволюционирующее явление, которое существенно трансформируется и приобретает новые черты, качественные характеристики и траектории развития под воздействием внедрения информационных технологий в противоправных целях. Отмечается, что благодаря бесчисленным способам злоупотребления информационными технологиями, сегодня наблюдается технологический сдвиг в характере преступлений.

Использование информационных технологий в правовой политики по противодействии коррупции представляет собой систему комплексных взаимосвязанных программных средств, позволяющих реализовать сложные системные механики динамического отслеживания причин и условий формирования коррупции, признаков коррупционной деятельности, оценки коррупционных рисков, прогнозирование развитие коррупционных правонарушений, комплексной оценки эффективности применяемых средств противодействия. Современные программные средства, телекоммуникационные системы, базы данных позволяют вести учет множественной информации не имеющий в фрагментарном состоянии какой-либо ценности для реализации правовой политики по противодействию коррупции. Оценивая систему разработанных и принятых нормативных актов, учреждающих отдельные антикоррупционные институты, можно утверждать, что сегодня сформированы достаточные предпосылки для создания системной цифровой платформы позволяющей объединить разрозненные институциональные решения в единый цифровой комплекс. Очевидно, что такая программная конструкция должна быть представлена модульной структурой, позволяя наращивать потенциал единой цифровой платформы.

В национальной правовой доктрине сложилось общее понимание антикоррупционной политики как многовекторного правотворческого и правоприменительного процесса, видится обоснованным указать на тот факт, что исследователи не вкладывают в данную дефиницию концептуальных конструкций исключающих человеческий фактор. Между тем, ставка на идеальную личность, отвечающую высоким морально-этическим требованиям правопорядка не приносит своих результатов. С другой стороны, развитие технологий администрирования построенного на

принципе «Zero Trust» (нулевого доверия) к государственному служащему, посредством процедурных конструкций, средств объективного контроля демонстрирует высокую эффективность.

В рамках формирования антикоррупционой политики следует подчеркнуть, что сфера отношений, связанная с разработкой и внедрением цифровых форм и роботизированных технологий постоянно изменчивая и слабо прогнозируемая. Поэтому, в стратегическом плане здесь важны не только негативные эффекты, которые могут появится от развития неправовых и теневых практик, но и возможные позитивные следствия, значимые для формирования нового правопорядка в цифровую эпоху.

Всё выше изложенное, позволяет прогнозировать, что цифровая трансформация общественного взаимодействия очевидным образом приведёт к содержательному расширению и видоизменению теории правовых отношений, конкретизации новых объектов (а возможно и субъектов – например, цифровых субъектов) и содержания правоотношений. Думается все структурные элементы правовых отношений будут содержательно расширены и конкретизированы исходя из новой цифровой реальности. Следовательно, в рамках антикоррупционой политики необходимо прогнозировать активное действующее участие разнообразных автономных, алгоритимических и интеллектуальных систем в противоправном взаимодействие и коррупционном обмене. Возникают и будут соответственно еще более активно возникать сложный состав фактов, не вписывающие в традиционную классификацию юридических фактов и сложных фактических составов.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Баранова Н. Что такое цифровая безопасность: термины и технологии. URL на дату 01.07.19: // https://te-st.ru/2018/05/25/digital-security-terms/

2. Ефремов А.А. Проблемы реализации концепции управления рисками цифровой безопасности ОЭСР в российском законодательстве // Информационное право. 2016. № 4. С. 25 - 28.

3. Овчинников А.И., Самарин А.А. Перспективы развития современного права: экстерриториальность, трансграничность, сетевая множественность // Философия права. 2015. № 3 (70). С. 8-14.

4. Саломатин К., Буртин Ш. Заводной мандарин. Узники китайских лагерей рассказывают про общество будущего // Русский репортер. №10 (475). 2019. С.34-47.

5. Указ Президента РФ от 05.12.2016 N 646 "Об утверждении Доктрины информационной безопасности Российской Федерации" // СЗ РФ. 12.12.2016. № 50. Ст. 7074.

6. Соколов И.А., Куприяновский В.П., Аленьков В.В., Покусаев О.Н., Ярцев Д.И., Акимов А.В., Намиот Д.Е., Куприяновская Ю.В. Цифровая безопасность умных городов // International Journal of Open Information Technologies. №1. 2018г. С.104-116.

7. Ellison D., Venter H. An ontology for digital security and digital forensics investigative techniques (Conference Paper) // Proceedings of The 11th International Conference on Cyber Warfare and Security (ICCWS2016). Boston, 2016. P. 120 – 128.

8. Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document. Published on October 01, 2015. URL: http://www.oecd.org/publications/digital-security-risk-management-for-economic-and-social-prosperity-9789264245471-en.htm.

9. Сухаренко А.Н. Законодательное обеспечение информационной безопасности в России // Российская юстиция. 2018. № 2. С. 2.

10. McKinsey Global Institute. Digital Globalization: the new era of global flows. Executive Summary, march 2016. URL: http://www.mckinsey.com

11. Kadar M., Moise I.A., Colomba C. Innovation Management in the Globalized Digital Society. Procedia - Social and Behavioral Sciences, Volume 143, 2014, Pages 1083-1089, ISSN 1877-0428, https://doi.org/10.1016/j.sbspro.2014.07.560 ; Dufva T., Dufva M. Grasping the future of the digital society, Futures, Volume 107, 2019, Pages 17-28, ISSN 0016-3287, https://doi.org/10.1016/j.futures.2018.11.001 ; Jean-Sébastien Guy. Digital technology, digital culture and the metric/nonmetric distinction, Technological Forecasting and Social Change, Volume 145, 2019, Pages 55-61, ISSN 0040-1625, https://doi.org/10.1016/j.techfore.2019.05.005.

12. Holtel S. Artificial Intelligence Creates a Wicked Problem for the Enterprise // Procedia Computer Science. Volume 99, 2016, P. 171. URL: https://doi.org/10.1016/j.procs.2016.09.109

13. Лапшин А.О. Глобализация и цифровое общество: заметки на полях // Власть. 2019. №1. С.64.

14. Аббасова Е.В., Васильев В.А. Трудовое право в цифровой реальности: проблемы интеграции // Российская юстиция. 2019. N 4. С. 17.

15. Злобин Н. Правило «мягкой силы». Российская газета от 29.03.2013. URL на дату 01.07.19: https://rg.ru/2013/05/29/zlobin.html

16. Документ WSIS-03/GENEVA/DOC/5-R от 12 декабря 2003 года - Женевский «План действий по построению глобального информационного общества» https://docplayer.ru/33746414-Dokument-wsis-03-geneva-doc-5-r-12-dekabrya-2003-goda-original-angliyskiy-plan-deystviy.html

17. Балашова А. Oracle установила рекорд продаж в России на фоне импортозамещения софта. Почему госструктуры и госкомпании продолжают закупать американское ПО // URL на дату 01.07.19: https://www.rbc.ru/technology_and_media/29/04/2019/5cc48a549a79475b870c850e?from=newsfeed

18. Декларация лидеров «Группы двадцати» // URL: http://www.kremlin.ru/supplement/5373

19. Форум ВВУИО 2019 года // URL: https://www.itu.int/net4/wsis/forum/2019/ru

20. Орлов П. Электронный начальник // Российская газета. URL на дату 01.07.19: https://rg.ru/2009/12/14/electron-pravitelstvo-site.html

21. Кольдина А. Свежая голова. Российская газета от 20.02.2018. URL на дату 01.07.19: https://rg.ru/2018/02/20/valentina-petrenko-obshchaia-baza-dokumentov-v-razy-uprostit-zhizn.html

22. Послание Президента Федеральному Собранию 1 марта 2018 года. URL: http://kremlin.ru/events/president/news/56957 (дата обращения: 10.06.2019)

23. Греф Г. Цифровизация - единственный способ борьбы с коррупцией. URL: https://www.vestifinance.ru/articles/113176 (дата обращения: 10.06.2019).

24. Бессонова В.В., Жукова А.С. К вопросу об участии институтов гражданского общества в противодействии коррупции // Государственная власть и местное самоуправление. 2012. № 10. С. 9 - 13. Васильев В.И. Борьба с коррупцией и местное самоуправление // Журнал российского права. 2012. № 4. С. 5 - 17.

25. Andersen T. B. E-Government as an anti-corruption strategy // Information Economics and Policy, 21(3), 201–210. URL на дату 10.06.19: https://doi.org/10.1016/j.infoecopol.2008.11.003 (дата обращения: 10.06.2019).

26. "Конвенция Организации Объединенных Наций против коррупции" (принята в г. Нью-Йорке 31.10.2003 Резолюцией 58/4 на 51-ом пленарном заседании 58-ой сессии Генеральной Ассамблеи ООН) // Бюллетень международных договоров, 2006, N 10, октябрь, С. 7 - 54

27. Камалова Г.Г. О современном состоянии законодательства о служебной тайне // Актуальные проблемы российского права. 2014. № 9. С. 1893 - 1898.

28. Библия. Второзаконие. Гл. 27. Стих 25; Сборник «Сады благонравных» имама Ан-Навави; Торы, Дварим, 16.19-20 и др.

29. Памятники русского права. Вып. 3. М. 1955. С. 208; Судебники XV-XVI вв. Под ред. Б.Д. Грекова. М.-Л.: АН СССР, 1952. С. 19; Грамоты Великого Новгорода н Пскова. Под ред. С.Н. Валка. М.-Л., 1949. С. 145. № 88; Судебники XV-XVI вв. С. 141 и др.

30. Аристотель. Сочинения: пер. с древнегреч. В 4 т. Т. 4 / Аристотель. – М. : Мысль, 1983. – С. 631.

31. Россияне назвали самые коррумпированные сферы в России. НОВОСТИ РОССИИ. 22 октября 2019. Доступ: https://www.business-gazeta.ru/news/443475

32. Воронцов, С.А., Понеделков, А.В. О слабых звеньях коммуникационной деятельности по противодействию коррупции // Коммуникология. 2018. - Т. 6. №1. - С. 143-154.

33. Толковый словарь иностранных слов Л. П. Крысина.- М: Русский язык, 1998.

34. Указ Президента РФ от 01.04.2016 N 147 «О Национальном плане противодействия коррупции на 2016 - 2017 годы». Доступ: http://www.consultant.ru/document/cons_doc_LAW_196138/

35. Андреева Л.А. К вопросу определения понятия и причин коррупции // Вопросы современной юриспруденции: сб. ст. по матер. XIV междунар. науч.-практ. конф. – Новосибирск: СибАК, 2012.; Чечуров А.В. Коррупция: историко-философская ретроспектива // Вестник Волгоградского гос. Ун-та. Сер. 7. Филос. 2010. №2 (12). – С. 158-163.; Гуляева Э.В. Понятие коррупционного правонарушения по законодательству РФ // Молодой учёный. – 2018. №15 (201). – С. 53-56.; Сердюк Л.В. К вопросу о понятии коррупции и мерах ее предупреждения // Российская юстиция. 2011. N 2. С. 41-44.; Цирин А.М. Перспективные направления развития законодательства Российской Федерации о противодействии коррупции // Журнал российского права. 2011. N 2. С. 12-24 и др.

36. Воронцов С.А., Понеделков А.В., Зырянов С.Г. Индикаторы коррупционной деятельности в системе государственной власти и местного самоуправления РФ // Социум и власть. 2017. № 1 (63). С. 30-37.

37. Источник (печатная версия): Словарь русского языка: В 4-х т. / РАН, Ин-т лингвистич. исследований; Под ред. А. П. Евгеньевой. — 4-е изд., стер. — М.: Рус. яз.; Полиграфресурсы, 1999; (электронная версия): Фундаментальная электронная библиотека.

38. Чечуров А.В. Коррупция: историко-философская ретроспектива // Вестник Волгоградского гос. Ун-та. Сер. 7. Филос. 2010. №2 (12). – С. 158-163.

39. Фрагменты ранних греческих философов.Ч. 1. От эпических теокосмогоний до возникновения атомистики / изд. подг. А. В. Лебедев. – М. : Наука, 1989. – С. 34.

40. Фрагменты ранних греческих философов. Ч. 1. От эпических теокосмогоний до возникновения атомистики / изд. подг. А. В. Лебедев. – М. : Наука, 1989. – 176 с.

41. Аристотель. Сочинения : пер. с древнегреч. В 4 т. Т. 4 / Аристотель. – М. : Мысль, 1983. – С. 631.

42. Гегель, Г. В. Ф. Философия права : пер. с нем. / Г. В. Ф. Гегель. – М. : Мысль, 1990. – С. 116.

43. Реале, Д. Западная философия от истоков до наших дней. В 4 т. Т. 1. Античность / Д. Реале, Д. Антисери. – М. : Петрополис, 1994. – С. 262.

44. Макиавелли, Н. Государь : Сочинения / Н. Макиавелли. – М. : ЭКСМО-Пресс, 2001. – 286 с.

45. Вебер М. Политические работы (1895-1919) / Перевод с нем. В.М. Скуратова. М.: Праксис. 3003. С. 141.

46. Хантингтон, С. Политический порядок в меняющихся обществах / С. Хантингтон. – М. : Прогресс-Традиция, 2004. – 480 с.

47. Коррупция: тормоз или смазка экономики? 29.09.2015. Доступ: https://www.mql5.com/ru/blogs/post/650488

48. Myrdal G. 1968. Asian Drama: An Inquiry into the Poverty of Nations. — N.Y.

49. Кузьмин Н.А. К вопросу о понятии и природе коррупции. // Административное и муниципальное право. 2010. № 6 // КонсультантПлюс Версия Проф. [электронный ресурс] — Режим доступа. - URL: http // www/consultant.ru/

50. Большой юридический словарь / Под ред. А.Я. Сухарева, В.Е. Крутских. – М., 2000. [–] С. 288–289.

51. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. – М.: Азбуковник, 1999. – С. 298.

52. Горный М.Б. Коррупция в России: системная проблема и системное решение. [Электронный ресурс]— Режим доступа. — URL: http://www.strategy-spb.ru/Koi8/Proekt/Proekt_antikorup/otchet_arhangelsk.htm

53. Марлухина, Е. О. Криминология : учебное пособие / Е. О. Марлухина. - Москва : Дашков и К°, 2007. – 370.

54. Русецкий Е.А. Понятие, сущность и особенности современной коррупции [электронный ресурс] — Режим доступа. — URL: rusetskiy.ru

55. Кузьмин Н.А. К вопросу о понятии и природе коррупции. // Административное и муниципальное право. 2010. № 6 // КонсультантПлюс Версия Проф. [электронный ресурс] — Режим доступа. - URL: http // www/consultant.ru/

56. Конвенция по борьбе с подкупом иностранных должностных лиц при осуществлении международных коммерческих сделок, принятая Организацией экономического сотрудничества и развития (ОЭСР) 21 ноября 1997 года. Доступ: http://www.consultant.ru/law/hotdocs/16996.html/

57. Конвенция об уголовной ответственности за коррупцию" (заключена в г. Страсбурге 27.01.1999). Доступ: http://www.consultant.ru/document/cons_doc_LAW_121544/

58. Конвенция Организации Объединенных Наций против коррупции" (принята в г. Нью-Йорке 31.10.2003 Резолюцией 58/4 на 51-ом пленарном заседании 58-ой сессии Генеральной Ассамблеи ООН)

59. Модельный закон "Основы законодательства об антикоррупционной политике" (принят постановлением Межпарламентской Ассамблеи государств - участников СНГ от 15 ноября 2003 г. N 22-15). Доступ: https://base.garant.ru/2569543/

60. Цирин А.М. Перспективные направления развития законодательства Российской Федерации о противодействии коррупции // Журнал российского права. 2011. N 2. С. 12-24.

61. Купрещенко Н.П. Влияние коррупции на экономические отношения в Российской Федерации // Налоги. 2008. Спец. вып. Январь.

62. Противодействие коррупции на государственном и муниципальном уровне в современной России. Материалы Всероссийской научно-практической конференции с международным участием 17 апреля 2020г., Ростов-на-Дону: Изд-во ЮРИУ РАНХиГС, 2020. – 320 с.

83. Противодействие коррупции на государственном и муниципальном уровне в современной России. Информационно-аналитические материалы Всероссийской научно-практической конференции с международным участием 17 апреля 2020г., Ростов-на-Дону: Изд-во ЮРИУ РАНХиГС, 2020. – 240 с.

64. Федеральный закон от 25 декабря 2008 г. N 273-ФЗ "О противодействии коррупции" (с изм. от 30.10.2018) // СЗ РФ. 2008. N 52 (часть 1). Ст. 6228.

65. Воронцов С.А., Понеделков А.В. Проблемы противодействия коррупции на государственной и муниципальной службе и пути их решения в современной России

(обзор материалов круглого стола) // Северо-Кавказский юридический вестник. 2018. № 1. С. 145-154.

66. Артемьев А.А., Зайковский В.Н., Лепехин И.А. К вопросу о необходимости корректировки определения коррупции в современном российском законодательстве // Российская юстиция. №7. 2019. С. 50-51.

67. Augenbaum S. The Secret to Cybersecurity: A Simple Plan to Protect Your Family and Business from Cybercrime. Forefront Books. 2019. 192 p.

68. Joshua B. Hill, Nancy E. Marion. Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century. Praeger Security International, 2016. 290 p.

69. Samuel C. McQuade. Encyclopedia of Cybercrime. London: Westport, Connecticut. 2009. 2010 p.

70. Kremling J., Parker A.M. Sh. Cyberspace, Cybersecurity, and Cybercrime. SAGE Publications, Inc, 2016. 296 p.; Mehan J.E. Cyberwar, Cyberterror, Cybercrime and Cyberactivism (2nd Edition): An in-depth guide to the role of standards in the cybersecurity environment. Published by: IT Governance Publishing. 2014. 376 p.; Clough J. Principles of Cybercrime. Cambridge University Press, 2010. 505 p.; Chawki M., Darwish A., Ayoub M., Tyagi K.S. Cybercrime, Digital Forensics and Jurisdiction. Springer, 2015.151 p.; Tropina T., Callanan C. Self- and Co-regulation in Cybercrime, Cybersecurity and National Security. Springer, 2015. 100 p.; Castiglione, A., Pop, F., Ficco, M., Palmieri, F. Cyberspace Safety and Security. Springer, 2018. 326 p.; Kostopoulos G. Cyberspace and Cybersecurity. 2nd Edition. CRC Press, Taylor & Francis Group, LLC, 2018. 316 p.

71. Болдуин Р. Великая конвергенция: информационные технологии и новая глобализация. М.: Издательский дом «Дело» РАНХиГС, 2018. 416 с.; Гринфилд А. Радикальные технологии: устройство повседневной жизни. М.: Издательский дом «Дело» РАНХиГС, 2018. 424 с.; Каку М. Будущее разума. 4-е изд. М.: Альпина нон-фикшн, 2018. 646 с.; Келли К. Неизбежно. 12 технологических трендов, которые определяют наше будущее. М.: Манн, Иванов и Фербер, 2017. 347 с.; Шваб К. Четвертая промышленная революция. М.: Изд-во Эксом, 2019. 208 с. ; Darrel Menthe, Jurisdiction In Cyberspace: A Theory of International Spaces 4 Mich.Tel.Tech.L.Rev.3 April 23, 1998 URL: https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1163&context=mttlr; David R. Johnson and David G. Post, Law and Borders—The Rise of Law in Cyberspace // Stanford Law Review, 1996, vol. 48, 1367, 1378–9. и др.

72. Bernik I. Cybercrime and Cyber Warfare. 2014. 176 p.; Lilienthal G. & Nehaluddin A. Cyber-attack as Inevitable Kinetic War // Computer Law & Security Review. 2015. Vol. 31, Iss.

3. pp. 390-400; Dinstein Y. War, Aggression and Self-Defence, 3rd ed. United Kingdom: Cambridge University Press. 2001.; Brownlie L. International Law and the Use of Force by States. UK: Clarendon, 1963; Bergsmo M., Ling Y. (2012) State Sovereignty and International Criminal Law . Oslo : TOAEP), а также кибертерроризма от хакерства и хактивизма (см., например, Jordan T., Taylor O. Hacktivism and Cyberwars: Rebels with a Cause? London: Routledge, 2004. 193 p.; Sauter M., Zuckerman E. The Coming Swarm: DDOS Actions, Hacktivism, and Civil Disobedience on the Internet. Bloomsbury Academic, 2014. 193 p.; Busch O., Palmas K. Abstract Hacktivism: The Making of a Hacker Culture. OpenMute, 2006. 132 p. и др.

73. Tsagourias N., Buchan R. Research Handbook on International Law and Cyberspace || Cyber terrorism [Электронный ресурс]. Режим доступа: https://booksc.xyz/book/73098906/566da2 ; Harrison D., Heather A. The Threat of Cyber Terrorism and What International Law Should (Try To) Do about It // Georgetown Journal of International. 2018. Vol.19; Orji U.J. ExaminingMissing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection // Computer Law Review International. 2014. Vol. 15.

74. Tabansky, L., Ben Israel, I. Cybersecurity in Israel. Springer, 2015; Cutler L. President Obama's Counterterrorism Strategy in the War on Terror. An Assessment Springer, 2017; Schünemann, Wolf J., Baumann, Max-Otto (Eds.) Privacy, Data Protection and Cybersecurity in Europe. Springer, 2017; Austin G. Cybersecurity in China. The Next Wave. Springer, 2017; Schallbruch, M., Skierka, I. Cybersecurity in Germany. Springer, 2017; Baumard, Ph. Cybersecurity in France. Springer, 2017; Tropina, T. Callanan, CormacSelf- and Co-regulation in Cybercrime, Cybersecurity and National Security; Almeida G. M. Cybersecurity Policy and LawMaking in the EU, US and Brazil // Computer Law Review International. 2016. Vol.17; Fidler D.P. The U.S. Election Hacks, Cybersecurity, and International Law // AJIL Unbound. 2016. Vol. 110. и др.

75. Fountain J. Building the Virtual State. Information Technology and Institutional Change. Washington: Brooking Institution Press, 2001; SAGA: Standards and Architectures for e-government Application. KBSt. 2003.; E-Government Strategy: Implementing the President's Management Agenda for E-Government. Office of Management and Budget, 2002; UN Global E-Government Survey 2003. UN, 2003; Evansa D., Yenb D. E-government: An analysis for implementation: Framework for understanding cultural and social impact Government Information Quarterly. No22. 2005.; Extending the Public Sphere through Cyberspace: The Case of Minnesota E-Democracy by Lincoln Dahlberg First Monday, Volume 6, Number 3-5 March

2001 // http://journals.uic.edu/ojs/index.php/fm/article/view/838/747; A Public Service-Oriented Gov- ernment Building Path in Chinese City: An Example From Public Rental Housing of Chongq- ing. Canadian Social Science. Vol. 9, No 4. 2013.

76. Гринфилд А. Радикальные технологии: устройство повседневной жизни. М.: Издательский дом «Дело» РАНХиГС, 2018. С. 324

77. Критика цифрового разума / Главн. Редактор В.В. Савчук. СПб.: Академия исследования культуры, 2020. 295 с.

78. Брокман Дж. Что мы думаем о машинах, которые думают: Ведущие мировые ученые об искусственном интеллекте. М.: Альпина-Нон-фикшин, 2017. 552 с. [электронный ресурс]. Режим доступа: https://www.litmir.me/br/?b=592732&p=1 (дата обращения 30.04.2020 г.)

79. Корякин В.М. «Цифровизация» общественных отношений и ее влияние на состояние коррупции в военной организации государства // Военное право. 2019. № 1 (53). С. 217-228

80. Послание Президента РФ Федеральному Собранию от 01.03.2018 "Послание Президента Федеральному Собранию". Доступ: http://www.consultant.ru/document/cons_doc_LAW_291976/

81. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993). Доступ: http://constrf.ru/

82. Зорькин В.Д. Право в цифровом мире: размышления на полях Петербургского международного юридического форума // Российская газета. 2018. 29 мая.

83. Соколов И.А., Куприяновский В.П., Аленьков В.В., Покусаев О.Н., Ярцев Д.И., Акимов А.В., Намиот Д.Е., Куприяновская Ю.В. Цифровая безопасность умных городов // International Journal of Open Information Technologies. №1. 2018г. С.105.

84. Куприяновский В.П., Уткин Н.А., Николаев Д.Е., Ярцев Д.И., Синягов С.А., Намиот Д.Е.. О локализации британских стандартов для Умного города // International Journal of Open Information Technologies. 2016. Vol.4, №7. P.14.

85. Baig, Z. A., Szewczyk, P., Valli, C., Rabadia, P., Hannay, P., Chernyshev, M., ... & Syed, N. (2017). Future challenges for smart cities: Cyber-security and digital forensics. Digital Investigation, 22, P.3. https://doi.org/10.1016/j.diin.2017.06.015

86. Федеральный закон от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации" Собрание законодательства РФ" // СЗ РФ. 31.07.2006, № 31 (1 ч.). Ст. 3448.

87. Дмитриева О. Без "бумажки" – человек. Российская газета. URL на дату 01.07.19: https://rg.ru/2011/02/11/dokumenty-site.html

88. Там же.

89. Купцова М. Права - всем голова. Российская газета. URL на дату 01.07.19: https://rg.ru/2013/12/02/pasporta.html

90. Приказ Минпромэнерго РФ от 07.08.2007 N 311 "Об утверждении Стратегии развития электронной промышленности России на период до 2025 года" // "Еженедельник промышленного роста", № 31, 24 - 30.09.2007. СПС «КонсультантПлюс».

91. Распоряжение Правительства РФ от 04.07.2017 N 1418-р (ред. от 18.10.2018) «Об утверждении Концепции формирования и ведения единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации» (вместе с "Планом мероприятий ("дорожной картой") по формированию и ведению единого федерального информационного ресурса, содержащего сведения о населении Российской Федерации") // СЗ РФ. 17.07.2017, № 29, Ст. 4390.

92. Указ Президента РФ от 09.05.2017 N 203 "О Стратегии развития информационного общества в Российской Федерации на 2017 - 2030 годы" // "Собрание законодательства РФ", 15.05.2017, N 20, ст. 2901.

93. Багоян Е.Г. Информационная безопасность и применение технологии блокчейн: зарубежный ыт и необходимость правового регулирования в Российской Федерации // Юрист. 2019. N 3. С. 42. DOI: 10.18572/1812-3929-2019-3-42-49 (www.doi.org).

94. Федеральный закон от 27.07.2006 № 149-ФЗ "Об информации, информационных технологиях и о защите информации" // СЗ РФ, 31.07.2006, № 31 (1 ч.), Ст. 3448; Федеральный закон от 29.07.2004 N 98-ФЗ "О коммерческой тайне" // СЗ РФ, 09.08.2004, N 32, Ст. 3283; Федеральный закон от 27.07.2006 N 152-ФЗ "О персональных данных" // СЗ РФ, 31.07.2006, N 31 (1 ч.), Ст. 3451.

95. Janeček V. Ownership of personal data in the Internet of Things, Computer Law & Security Review, Volume 34, Issue 5, 2018, P. 1040, ISSN 0267-3649, https://doi.org/10.1016/j.clsr.2018.04.007.

96. Смирнова К.М. Проблема информационной безопасности в контексте использования "Интернета вещей" в медицине // Медицинское право. 2019. № 1. С. 31.

97. Егорова М. А., Ефимова Л. Г. Понятие криптовалют в контексте совершенствования российского законодательства // Lex Russica (Русский закон). — 2019. — № 7. — С. 130–140.

98. Белых В. С., Егорова М. А. Криптовалюта как средство платежа: новые подходы и правовое регулирование // Вестник Университета имени О.Е. Кутафина. — 2019. — № 2.

99. Аветисян А.Д., Диденко Н.С. Отдельные проблемы противодействия преступлениям с использованием криптовалют в Российской Федерации // Юристъ-Правоведъ, 2020, №1. С. 63-67

100. Постановление Пленума Верховного Суда РФ от 09.07.2013 N 24 (ред. от 24.12.2019) "О судебной практике по делам о взяточничестве и об иных коррупционных преступлениях" // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=341481&dst=1000000001&date=01.05.2020

101. 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. С. 330-334. БО!: https://doi.org/10.18500/1994-2540-2019-19-3-330-334

102. Постановление Пленума Верховного Суда РФ от 07.07.2015 N 32 (ред. от 26.02.2019) "О судебной практике по делам о легализации (отмывании) денежных средств или иного имущества, приобретенных преступным путем, и о приобретении или сбыте имущества, заведомо добытого преступным путем" // http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=319280&dst=1000000001&date=14.06.2020

103. Утакаева И.Х., Никитенко В.О., Тутаев И.А. Особенности внедрения технологии блокчейн в цифровую экономику // Вестник Алтайской академии экономики и права. – 2019. – № 7-1. – С. 91-95; URL: https://www.vaael.ru/ru/article/view?id=637 (дата обращения: 13.06.2020).

104. Информационный ресурс Государственной Думы. Доступ: https://sozd.duma.gov.ru/bill/419059-7

105. Гайденко П.П., Давыдов Ю.Н. История и рациональность: Социология М. Вебера и веберовский ренессанс. М.: Политиздат, 1991. С.311.

106. Бекетов А. Искусственный интеллект в суде. URL на дату 01.07.19: https://ru.euronews.com/2019/01/28/eu-robojudge-courts

107. Гринфилд А. Радикальные технологии: устройство повседневной жизни. М.: Издательский дом «Дело» РАНХиГС, 2018.

108. Lopez-Iturriaga, Felix & Pastor Sanz, Iván. (2017). Predicting Public Corruption with Neural Networks: An Analysis of Spanish Provinces. Social Indicators Research. 140. 975-998. 10.1007/s11205-017-1802-2. URL:

https://www.researchgate.net/publication/321222117_Predicting_Public_Corruption_with_Neural_Networks_An_Analysis_of_Spanish_Provinces (дата обращения: 10.06.2019).

109. Трунцевский Ю.В., Севальнев В.В. Перспективы международного сотрудничества Российской Федерации и Китайской Народной Республики в сфере противодействия коррупции // Международное публичное и частное право. 2016. № 6. С. 30 - 34.

110. Хабриева Т.Я. Научно-правовые проблемы противодействия коррупции // Журнал российского права. 2012. № 7. С. 7 - 14.

111. Бикмухаметов А.В. и др. Под. общ. ред. П.А. Кабанова. Коррупция и антикоррупционная политика. Словарь-справочник. М. 2008.

112. Basel Institute on Governance, New perspectives in e-government and the prevention of corruption. Working Paper 23 (2017). URL: https://www.baselgovernance.org/publications/working-paper-23-new-perspectives-e-governmentand-prevention-corruption. Accessed: 10.10.20; E-government in support of sustainable development (2016). URL: http://workspace.unpan.org/sites/Internet/Documents/UNPAN97453.pdf. Accessed: 10.10.20 и др.

113. Роботы заявляют о своих правах: доктринально-правовые основы и нравственно-этические стандарты применения автономных роботизированных технологий и аппаратов : коллективная монография / Под ред. А.Ю. Мамычева, А.Ю. Мордовцева, Г.В. Петрук. Москва : РИОР, 2020. 349 с.; Pasquale F. The Black Box Society: The Secret Algorithms Behind Money and Information. Cambridge, MA: Harvard University Press, 2015; Salthouse T.A. When Does Age-Related Cognitive Decline Begin? // Neurobiology of Aging. 2009. Vol. 30. № 4 (April). P. 507 – 514.

114. Мамычев А.Ю., Мирошниченко О.И. Моделируя будущее права: проблемы и противоречия правовой политики в сфере нормативного регулирования систем искусственного интеллекта и роботизированных технологий // Правовая политика и правовая жизнью. 2019. № 2. С. 125-133.

115. Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации" // https://www.garant.ru/products/ipo/prime/doc/72738946/

116. Маринкин Д. Н., Плотников Р. В. Информационные технологии блокчейн как способ борьбы с коррупцией в современной России // Вестник Прикамского социального института. 2019. № 1 (82). С. 61-64.