А. Ю. Быков

Руководитель Научно-образовательного центра «Правовая защита бизнеса и предпринимательства» Московского государственного юридического университета им. О. Е. Кутафина (МГЮА)

Право цифровой экономики – некоторые народнохозяйственные и политические риски

В статье рассматриваются некоторые народнохозяйственные и политические риски, связанные с развитием цифровой экономики. Отмечается жизненная необходимость для России национальной кибергигиены. Делается вывод, что заполнить существующий сегодня в цифровой экономике правовой вакуум и устранить опасность возникновения беспредела может административно-правовая дорожная карта, которая на первом этапе реализации Стратегии научно-технологического развития Российской Федерации в 2017 – 2019 годах заложит в государственной политике России такие системные и правовые подходы, которые в теории и на практике сделают обман в цифровой экономике нашей страны бессмысленным.

Ключевые слова: цифровая экономика, правовая безопасность, Российская Федерация, международное право, правовое регулирование, стратегия, угроза, собственность, контроль.

1. Правовая безопасность Российской Федерации

Правовая безопасность Российской Федерации складывается из внешней и внутренней правовой безопасности государства, экономики, общества и граждан. При этом вопросы обеспечения правовой безопасности страны можно условно разделить на стратегические и тактические.

Вступление России в эпоху цифровой экономики, которое констатировала Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы, опубликованная на сайте Совета Безопасности РФ 13 декабря 2016 года[4], затронуло все аспекты правовой безопасности нашей страны.

В эпоху цифровой экономики при оценке уровня правовой безопасности Российской Федерации представляется необходимым учитывать правовую ситуацию в следующих сферах:

- международное право ЦЭ и практика его применения в РФ и для субъектов права РФ за рубежом;
- национальное право ЦЭ в РФ и практики его применения;
- работа уполномоченных органов государственного управления ЦЭ в РФ;
- государственные и частные аппаратные конструкции ЦЭ, в том числе архитектура облачных сервисов;
- применяемые программные продукты ЦЭ, в том числе в облачных сервисах;
- цифровые платформы бизнеса, общества и граждан в ЦЭ;
- федеральный и региональные информационные ресурсы по ЦЭ;
- специализированные форумы общения государственных чиновников, ученых и практикующих специалистов ЦЭ; ***сегодня в***

начале пути стране как воздух нужен критический голос науки и профессионалов из Российского союза промышленников и предпринимателей, Ассоциации европейского бизнеса, Ассоциации юристов России, Объединения корпоративных юристов России, Союза ИТ директоров России, всех без исключения интегральных, отраслевых и региональных объединений предпринимателей страны.

- технические, правовые и управленческие образовательные системы для ЦЭ, предлагаемые такими центрами, как Национальный центр компетенций в области цифровой экономики МГУ им. М.В.Ломоносова, Финансовый университет при Правительстве РФ, Университет ИТМО, Университет им. О.Е. Кутафина, МГИМО МИД РФ, НИУ ВШЭ, РАНХиГС, Санкт-Петербургский государственный экономический университет, Московский государственный университет путей сообщения Императора Николая II, Институт экономики роста им. Столыпина П.А., Институт развития интернета, Глобальная библиотека права цифровой экономики АНО Форт и др.

2. Международное право ЦЭ и практика его применения в РФ и для субъектов права РФ за рубежом.

На наших глазах выстраивается и самообновляется архитектура права цифровой экономики в США, Великобритании, Швеции, Китае, Японии, Евросоюзе, Южной Корее, Германии. Только продуманная концепция права может позволить правительствам создать здоровые и надежные аппаратные и программные решения для национальных цифровых экономик, а продуманные международные конвенции – для цифровой экономики всей планеты.

С учетом того, что международное право имеет приоритет над национальным правом, важен анализ того, в каком состоянии находится защита интересов российского бизнеса в ЦЭ за рубежом.

Не менее важен и тот аспект, что с учетом наступившей эры ЦЭ эффективность работы Федеральной налоговой службы, Федеральной антимонопольной службы и других федеральных учреждений в будущем в гораздо большей степени, чем до сих пор, будет зависеть от актуальности и качества международных конвенций, в которых участвует Российская Федерация.

В России применяется Конвенция ООН от 23 ноября 2005 года об использовании электронных сообщений в международных договорах.

Иных международных конвенций, напрямую посвященных ЦЭ, пока нет, равно как нет двусторонних соглашений по ЦЭ, ратифицированных РФ и действующих на территории РФ.

Ряд широко применяемых сегодня конвенций, например, Нью-Йоркской конвенции ООН о признании и приведении в исполнение иностранных арбитражных решений 1958 года, в эпоху цифровой экономики нуждаются в серьезной переработке.

Необходимо провести ревизию всех международных конвенций, в которых участвует Российская Федерация. Тут предстоит большая работа, в особенности для Министерства иностранных дел РФ, других федеральных ведомств и для юридической науки.

Глобальная библиотека права ЦЭ предлагает нам целый ряд национальный законов и подзаконных актов, резолюций парламентов, итоговых документов «Большой двадцатки» и ОЭСР, которые могут в ближайшее время лечь в основу международных конвенций по ЦЭ и двусторонних соглашений с участием РФ.

«Большая двадцатка» 5 сентября 2016 года отметила, что в ЦЭ важную роль имеет соблюдение законов о конкуренции и защите прав потребителей[9]. Следствием может стать принятие Международной Конвенции по борьбе с картелями.

В 2017 года Г20 планирует принятие стратегических решений по ЦЭ.

6-7 апреля 2017 года на встрече в Дюссельдорфе министры цифровых экономик Г20, Испании, Норвегии, Нидерландов и Сингапура приняли стратегическую декларацию «Строительство дигитализации для взаимосвязанного мира» (Shaping Digitalisation for an Interconnected World) [5].

У G20 и ОЭСР существует план действий по борьбе с размыванием налогооблагаемой базы и уходом от налогообложения (Base Erosion and Profit Shifting). Россия активно участвует в этой работе. ОЭСР опубликовала уже 262 доклада по ЦЭ.

Параграф 10 «Дигитализация и правовые рамки» Доклада Генсека ОЭСР «Ключевые темы цифровой трансформации в G20», Берлин, 12 января 2017 года констатирует факт всеобщего отставания правового регулирования от темпов цифровой революции в мире [6].

Много внимания документ посвящает правовому регулированию защиты конкуренции. Однако авторы не пишут о том, что мощность современных гиперкомпьютеров достигается, в том числе, и такими программными решениями, которые носят ***принудительно картельный характер***. Действующее антимонопольное право просто не сможет противостоять картельному союзу аппаратных и программных решений.

Как не вспомнить фразу Кристофа Мартина Виланда «за деревьями не видно леса», когда анализируешь, какое число тем охватили 262 доклада ОЭСР по ЦЭ, какое число направлений, уже подвергшихся изменениям в правовом регулировании в ЦЭ, перечисляет доклад Гендиректора ОЭСР от 12 января 2017 года. Это:

- телекоммуникации (лицензирование спектров, всемирный доступ)
- защита личных данных
- защита критической информационной инфраструктуры
- цифровая идентичность (электронная подпись, электронное опознание)
- интеллектуальная собственность
- электронное правительство
- защита потребителей в электронной коммерции
- рециклирование электронных устройств
- онлайн безопасность людей и производства товаров
- торговля
- трудовые отношения
- налоги
- отраслевые законы (здравоохранение, энергетика, транспорт)

Упомянутый доклад Генерального директора ОЭСР констатирует отсутствие ясных подходов к правовому регулированию массово возникающих в ЦЭ конфликтных ситуаций. ***Доклад предсказывает, что цифровая революция быстро сделает устаревшей всеобъемлющую правовую основу дигитализации.*** Для движения вперед на данном фундаментальном направлении доклад предлагает найти баланс между двумя путями. Путем создания некоего экспериментального пространства, в котором могли бы действовать законы. И путем введения саморегулирования в промышленности при декларировании неких принципов и кодексов поведения.

Позвольте специально для юридического цеха полностью процитировать мысль Генерального директора ОЭСР, изложенную на стр.140 его доклада для «Большой двадцатки» от 12 января 2017 года.

«Хотя некоторые вопросы, возникающие в связи с дигитализацией, несомненно, нуждаются в юридическом ответе, а правовая определенность имеет решающее значение для многих аспектов дигитализации, менее ясно, как следует решать другие вопросы. В современных условиях быстрых цифровых инноваций и с учетом широкого применения цифровых технологий в экономике и обществе, всеобъемлющая правовая основа для дигитализации, скорее всего, устареет довольно быстро. Предоставление экспериментального пространства для законодательства и рассматривание саморегулирования в промышленности - это два варианта поиска путей обеспечения устойчивого баланса между дигитализацией невмешательства и жестким юридическим вмешательством. Кроме того, принципы высокого уровня могут служить руководством для политиков, деловых кругов и общества для ориентации и определения приоритетности решений на протяжении всего процесса дигитализации» [6].

В английском оригинале:

«While some issues raised by digitalisation clearly need a legal response and legal certainty is crucial for many aspects of digitalisation, it is less clear how other issues should be addressed. In today’s environment of rapid digital innovation and given the wide application of digital technologies in the economy and society, a comprehensive legal framework for digitalisation would likely become obsolete rather quickly. Providing an experimental space for legislation and considering industry self-regulation are two options for finding ways to strike a sustainable balance between laissez-faire digitalisation and heavy-handed legal intervention. In addition, high-level principles can serve as a guide

for policy makers, business and society to orient and prioritise decisions throughout the process of digitalisation.»

Постановка Генеральным директором ОЭСР вопроса о балансе этих двух путей представляется разумной. Однако, стабильный баланс может быть найден только в том случае, если два предлагаемых пути будут находиться не в одной плоскости, а подчинены друг другу. ***Саморегулирование должно быть разрешенным легальным сектором правового поля. Иначе оно может стать сектором беспредела, картелей и теневой экономики.***

О принципах высокого уровня и кодексах поведения в ЦЭ говорит не только ОЭСР. Европарламент, например, в резолюции о роботах и искусственном интеллекте от 16 февраля 2017 года предлагает дизайнерам и производителям роботов присягать на кодексе нравственных ценностей для роботов Исаака Азимова. В этой резолюции Еврокомиссии предложено учредить Агентство ЕС по роботам и искусственному интеллекту, ввести обязательное страхование ответственности роботов, создать специальный фонд для покрытия убытков, которые могут оказаться не застрахованными.

В целом в Евросоюзе цифровая экономика неуклонно сливается с реальной. Еврокомиссия планирует инвестировать 500 млрд. евро в серию хабов ЦЭ, где бизнес будет получать новые компетенции. Приоритетами ЕС является стандартизация в пяти областях: 5G, облачных технологиях, интернете вещей, информационных технологиях и кибербезопасности. Действует программа Единого европейского цифрового рынка. Все торговые реестры и государственные вестники стран ЕС о несостоятельности будут сведены в единый портал электронной юстиции.

Основные инициативы Евросоюза в ЦЭ – Индустриальная политика в эру глобализации (Industrial Policy for the Globalization Era), Цифровая повестка дня для Европы (Digital Agenda for Europe 2015), Инновационный союз (the Innovation Union); Акт о малом бизнесе Европы (The Small Business Act for Europe, 2008); Коммюнике Комиссии «Адаптация политики по электронному бизнесу в меняющейся среде: уроки инициативы Go Digital и задачи на будущее» (“Adapting e-business policies in a changing environment: the lessons of the Go Digital initiative and the challenges ahead”, 2003).

В цифровой экономике в мире в настоящее время лидируют США. За ними идут Южная Корея, Великобритания, Швеция, Финляндия, Япония, Китай, Германия, Франция, Испания и Индия. США лидируют в вопросе создания правовой базы для национальной ЦЭ, им в этом вопросе «в затылок дышат» Великобритания и Китай.

1 декабря 2016 года, в день утверждения Президентом РФ указом N 642 Стратегии научно-технологического развития Российской Федерации Комиссия по усилению национальной кибербезопасности США опубликовала свой 100 страничный доклад по безопасности и росту цифровой экономики в США.

В состав Комиссии по усилению кибербезопасности США, созданной 9 февраля 2016 года указом Президента США N 13718 как подразделение Министерства торговли США, входят, например, генерал Кейт Александер, бывший директор Агентства национальной безопасности США и бывший командующий Командования кибероперациий Минобороны США, Самуэль Пальмисано, бывший гендиректор АйБиЭм, Петер Ли, директор корпорации Майкрософт, Айя Банга, президент Мастер Кард, Джозеф Салливан, директор по безопасности компании Юбер, то есть руководители американских корпораций, работающих по всей России.

Доклад от 1 декабря 2016 года показывает, что цифровая экономика США является частью системы кибербезопасности США. Именно так, а не наоборот. У Президента США есть специальный помощник по вопросам кибербезопасности. Он работает вместе с главным федеральным исполнительным директором по вопросам информации и главным федеральным исполнительным директором по вопросам информационной безопасности. Они руководят Фондом развития информационной безопасности, размер которого в 2016 году составил 3,1 млрд. долларов.

США полагают, что достигли достаточного уровня кибербезопасности своих федеральных ведомств и в настоящее время переносят акцент на обеспечение кибербезопасности своего бизнеса.

Президенту США Трампу рекомендовано назначить специального посла США по

кибербезопасности, который бы отвечал за продвижение американских правовых и технологических стандартов в этой области во всем мире.

К началу 2017 года администрация США опиралась в своей работе по национальной кибербезопасности и цифровой экономике на мощную правовую базу, построенную за прошедшие 30 лет.

Еще 12 апреля 1984 года Конгресс США принял закон N 98-473, запрещающий пользование чужими компьютерами и компьютерными сетями без разрешения.

Заслуживают быть упомянутыми указ N 13010 президента Клинтона от 15 июля 1996 года «О защите критической инфраструктуры» [5]; Доклад от июля 1997 года «О мерах по защите критической инфраструктуры» [5]; Директива Президента «О защите критической инфраструктуры» от 4 августа 1998 года[5]; «Национальный план защиты информационных систем» 2000 года[5]; «Национальная стратегия безопасного киберпространства» президента Буша от февраля 2003 года[5]; Президентская директива по национальной безопасности N 7 от 17 декабря 2003 года «По определению, приоритезации и защите объектов критической инфраструктуры» [5]; «План защиты национальной инфраструктуры» 2006 года[5]; Президентская директива по национальной безопасности N 54 от января 2008 года «О политике кибербезопасности»[5].

Президент Обама принял свой «План защиты национальной инфраструктуры» 2009 года[5]. Обзор политики в киберпространстве от мая 2009 года[5]. В апреле 2011 года была принята «Национальная стратегия проверенных личностей в киберпространстве» [5]. В мая 2011 года – «Международная стратегия для киберпространства» [5]. В октябре 2011 годы был принят указ Президента N 13587 «Структурные реформы по улучшению безопасности зашифрованных информационных сетей» [5]. 12 февраля 2013 года был принят указ N 13636 «Об усилении кибербезопасности критической инфраструктуры» [5]. В тот же день была принята президентская директива «Об усилении координации правительства и частного сектора в области кибербезопасности» [5]. В 2013 году был принят уже третий «План защиты национальной инфраструктуры» [5]. В феврале 2014 годы была утверждена «Конструкция усиления кибербезопасности критической инфраструктуры» [5]. Заслуживают также упоминания «Национальный план действий по кибербезопасности» от 9 февраля 2016 года[5] и Президентская директива N 41 от 26 июля 2016 года «О координации действий при инцидентах в киберпространстве Соединенных Штатов» [5].

Великобритания принимает «Билль о цифровой экономике» [5], реализует свою «Стратегию национальной кибербезопасности 2016-2021гг.» [5], частью которой является цифровая экономика страны. Правительство реализует «Стратегию цифровой экономики 2015-2018 годов»[5]. В Великобритании более 100 000 компаний - разработчиков программного обеспечения. Создан Национальный центр кибербезопасности с бюджетом в 1,9 млрд. фунтов на 5 лет. 16 февраля 2017 года при официальном открытии королевой Великобритании Елизаветой II Национального центра кибербезопасности канцлер казначейства Великобритании Филипп Хэммонд заявил, что за последний год 65% крупных компаний сообщили правительству о попытках взлома и попытках кибератак. Это только известные факты. А 90% британских компаний не имеют плана действий на случай кибернападения. Национальный центр кибербезопасности является частью Центра правительственной связи Великобритании, отвечающего за электронную разведку и безопасность. Его функцией является защита как правительственный учреждений, так и британского бизнеса от всех видов киберугроз [8].

В Китае активно действует государственная Канцелярия по интернет-информации. Среди всех мировых технологических компаний с капитализацией более $1 млрд. по темпам роста капитализации все 50 первых мест занимают китайские компании. Гиганты национального ИКТ-комплекса Alibaba, Xiaomi, Tencent, Baidu, Lenovo, Huawei, ZTE и др., продолжают активно развиваться на инновационной основе, гибко реагируя на новые hi-tech-вызовы, соответственно диверсифицируя свой бизнес и расширяя его географию [14].

Федеральное министерство экономики и энергетики Германии издает ежегодный доклад по ЦЭ. Экономика Германии прохо-

дит через настоящую цифровую революцию, почитает себя однако, отстающей от Китая, Японии и Южной Кореи. 51% немецких компаний пользуются «интернетом вещей». В сфере ИКТ в Германии работает 1 млн. человек. Каждый работающий создает еще одно рабочее место в сфере обслуживания отрасли ИКТ. Оборот отрасли ИКТ в 2016 году составил 223 млрд. евро. Председатель СвДП Германии Стефан Линднер пообещал добиться создания федерального министерства цифровой экономики Германии, если его партия сможет войти в правительство Германии по итогам выборов в Бундестаг 24 сентября 2017 года.

В ноябре 2016 года премьер – министр Индии Нарендра Моди вывел из оборота банкноты достоинством 500 рупий (7 долларов США) и 1000 рупий (14 долларов США), составлявших вместе по стоимости 86% наличных денег страны. Индия подготовилась и перешла на безналичные расчеты. Это рассматривается экспертами как безвозвратный поворот страны к цифровой экономике.

В поставленном Всемирным экономическим форумом на первое место среди цифровых экономик мира Сингапуре действует Закон 1993 года «О запрете злоупотреблений компьютерами», Закон «Об электронных сделках» 2010 года, заменивший аналогичный закон 1998 года. В Сингапуре действует Агентство кибербезопасности, Комиссия по защите персональных данных.

3. В России многие важные стратегические и тактические вопросы правового регулирования цифровой экономики осознаны и очерчены.

Известна оценка, приводимая в докладе Бостон Консалтинг Групп 2016 года о цифровой экономике России о том, что в ближайшие 10-20 лет в мире в результате цифровой революции исчезнут 50% профессий. Цифровая экономика, таким образом, касается буквально каждого [10].

Успехи цифровой экономики в США, Китае, Японии, Великобритании, Сингапуре и других странах впечатляют. Цифровая экономика позволяет любому существующему бизнесу развивать большое количество принципиально новых бизнес-моделей. Об этом книга профессора Клауса Шваба «Четвертая промышленная революция» [13]. Цифровая экономика имеет потенциал стать основой национальной безопасности России и благосостояния ее граждан. Необходимо поставить цифровую экономику на правовые рельсы и сделать ее надежной для ведения бизнеса.

Документ Евразийской экономической комиссии «Платформа отраслевых экосистем цифровой экономики» предлагает подробно проработанный вариант архитектуры ЦЭ ЕАЭС на базе крупных игроков ИКТ рынка [11].

Стратегия научно-технологического развития Российской Федерации, утвержденная Указом Президента России N 642 от 1 декабря 2016 года, со смирением констатирует проблемы невосприимчивости нашей экономики и нашего общества к инновациям, существенного отставания эффективности российских исследовательских организаций со сравнению со странами-лидерами, слабое взаимодействие сектора исследований и разработок с реальным сектором экономики, разомкнутость инновационного цикла, несогласованность приоритетов и инструментов научно-технологического развития Российской Федерации на национальном, региональном, отраслевом и корпоративном уровнях, риск отставания России от стран - мировых технологических лидеров и обесценивания внутренних инвестиций в сферу науки и технологий и целый ряд других угроз для национальной безопасности и благосостояния страны [1].

39-й пункт Стратегии предусматривает создание на первом этапе реализации Стратегии (2017-2019 годы) организационных, финансовых и законодательных механизмов, обеспечивающих гармонизацию научной, научно-технической, инновационной, промышленной, экономической и социальной политики и готовность Российской Федерации к большим вызовам.

Правительству Российской Федерации в Стратегии поручен, в том числе, мониторинг качества государственного регулирования и сервисного обеспечения научной, научно-технической и инновационной деятельности. 5 декабря 2016 года Указом Президента N646 была принята Доктрина информационной безопасности РФ [2].

13 декабря 2016 года на сайте Совета Безопасности был опубликован проект Стра-

тегии развития информационного общества в Российской Федерации на 2017 – 2030 годы [4].

1 января 2017 года вступил в силу Федеральный закон N 244-ФЗ от 3 июля 2016 года «О внесении изменений в части первую и вторую налогового кодекса Российской Федерации», известный как «налог на Гугл». Он ввел в РФ устоявшуюся в мире практику взимания НДС при оказании электронных услуг иностранными компаниями.

5 марта 2017 года Председатель Правительства РФ поручил Минсвязи и Минэкономразвития рассмотреть вопрос применения технологии блокчейн в условиях российской экономики. По мнению ряда юристов, эта новация неминуемо потребует серьезных изменений в действующем законодательстве, поскольку средства шифрования будут теперь в обязательном порядке использоваться в проектировании, производстве, внешней и внутренней торговле электронными устройствами.

21 марта 2017 года Председатель Правительства РФ провел совещание о государственной инфраструктуре облачных вычислений.

3 апреля 2017 года Президент РФ издал Распоряжение N 96-рп «Об утверждении Положения о рабочей группе Экономического совета при Президенте Российской Федерации по направлению «Цифровая экономика». Рабочую группу возглавили два помощника Президента – Андрей Белоусов и Игорь Щеголев. В состав группы помимо сопредседателей вошли 26 экспертов высокого уровня [3].

Правительство РФ во исполнение указа Президента N 624 разрабатывает программу «Цифровая экономика». Бизнес и экспертное сообщество ждут доклад рабочей группы Правительства РФ «Цифровая экономика», который должен быть сдан 11 мая 2017 года.

Правовой режим информации в РФ в настоящее время также регулируется Федеральным законом от 27 07 2006 года N 149-ФЗ «Об информации, информационных технологиях, и о защите информации» и Федеральным законом от 27 07 2006 года N 152-ФЗ ФЗ 152 «О персональных данных».

Важен проект Федерального закона N 47571-7 «О безопасности критической информационной инфраструктуры Российской Федерации».

В Государственной Думе весной 2017 года приступил к работе Совет по цифровой экономике.

Минпромторг России завершает работу над «Стратегией развития электронной торговли на 2017-2018 годы и на период до 2015 года».

ФАС РФ заявляет о подготовке изменений в законодательство о защите конкуренции, которые бы отражали реалии цифровой экономики. Принят Базовый документ по сетевой нейтральности, подготовленный членами рабочей группы по сетевой нейтральности ФАС РФ.

Роспотребнадзор ведет работу над законом, устанавливающим наказание товарным агрегаторам за размещение недостоверной информации в сети интернет.

Аналитический центр при Правительстве РФ приводит следующий список государственных программ в области ЦЭ:

- Концепция долгосрочного социально-экономического развития Российской Федерации на период до 2020 года;
- Прогноз долгосрочного социально-экономического развития Российской Федерации на период до 2030 года;
- Прогноз социально-экономического развития Российской Федерации на 2016 год и на плановый период 2017 и 2018 годов;
- Прогноз научно-технологического развития до 2030 года;
- Стратегия научно-технологического развития Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года;
- Государственная программа Российской Федерации «Информационное общество (2011-2020 годы)»;
- План мероприятий («дорожная карта») «Развитие отрасли информационных технологий»;
- Концепция региональной информатизации;
- План мероприятий («дорожная карта») в области инжиниринга и промышленного дизайна»;
- План мероприятий («дорожная карта») по созданию единой федеральной меж-

ведомственной системы учета обучающихся по основным образовательным программам и дополнительным образовательным программам»;

- Энергетическая стратегия России на период до 2030 года;
- План мероприятий («дорожная карта») «Повышение доступности энергетической инфраструктуры»
- «Дорожные карты» Национальной технологической инициативы – «Хелснет», «Нейронет», «Аэронет», «Аэронет» и «Маринет»;
- План мероприятий («дорожная карта») «Развитие лазерных, оптических и оптоэлектронных технологий (фотоники)»;
- План мероприятий («дорожная карта») по развитию электронного взаимодействия на финансовом рынке;
- План мероприятий («дорожная карта») по повышению эффективности расходов на развитие автомобильных дорог общего пользования;
- Стратегия национальной безопасности;
- Стратегия противодействия экстремизму в Российской федерации до 2025 года;
- Концепция общественной безопасности Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года [12].

Следует отметить, что стране еще предстоит придти к единым понятиям в ЦЭ и дать каждому из этих понятий правовое определение. В ЦЭ недопустимо отсутствие системности, которое пока, к сожалению, характерно для правоотношений, вытекающих из более чем тысячи подзаконных актов, на основании которых в настоящее функционируют федеральные и региональные информационные ресурсы.

4. Некоторые стратегические вопросы правового регулирования цифровой экономики.

Изучая путь, пройденный ведущими цифровыми экономиками мира за последние 30 лет, важно овладеть их понятийным инструментарием и стандартами, понять объявляемые акценты, познакомиться с архитектурой и правовым регулированием в ЦЭ. Но не менее важно для России сегодня ***глубоко разобраться с теми фундаментальными темами, которые в большинстве анализов, докладов, указов и законов мировых лидеров цифровой экономики затрагиваются лишь по касательной либо блещут своим отсутствием***. Обозначим некоторые из них.

Правоотношения «машина с машиной».

Время заключения контрактов на современных биржах между роботами сократилось до одной десятой секунды. Однако четкое правовое описание юридически значимых действий в отношениях между роботами есть далеко не всегда. Нет однозначного правового определения самих роботов. Обсуждаются варианты, что робот – это имущество, юридическое лицо, электронное лицо и другие. Признание роботов юридическими лицами может подогреть тему уголовной ответственности для юридических лиц.

В мире есть компании, продающие тысячи продуктов, предлагающие каждый из этих продуктов по десяткам и сотням вариантов стандартных контрактов, и при этом работающих с сотнями тысяч партнеров. Вариантность правоотношений в таких отраслях измеряется десятками и сотнями миллионов. Если не разработать и ввести понятные и лаконичные правовые нормы цифровой экономики, судьям можно будет только посочувствовать.

Угроза объектам критической инфраструктуры

В мировой ЦЭ существует понятие Критическая национальная инфраструктура. Электросети являются ее частью. Предлагаю каждому примерить конкретно на свой бизнес успешную атаку киберпреступников на украинские электросети 23 декабря 2015 года. Преступники за 6 месяцев до этой атаки разослали в офисы коммунальных электрических сетей Украины вредоносные электронные письма. Им удалось собрать такие данные, которые позволили им получить прямое дистанционное управление электрическими сетями и на несколько часов отключить 50 подстанций распределительных сетей.

Мы хорошо помним блэкаут в Москве 25 мая 2005 года. Десятки тысяч людей выходили из вагонов метро и по рельсам в темноте шли к станциям и далее поднимались на поверхность. Тогда только решительные действия Министерства обороны РФ предотвратили попадание канализационных вод в водопроводную систему Москвы, что могло привести к санитарной катастрофе с непредсказуемыми последствиями. Ясно, что преступники и террористы рвутся к организации подобных техногенных катастроф. Рвутся они и к оружию. Министр обороны Германии Урсула фон дер Ляйен, например, сообщила газете «Ди Вельт», что ее ведомство отражает 4500 кибератак ежедневно[7].

России жизненно необходима национальная кибергигиена. Уровень технических навыков и ***электронной правовой грамотности*** населения должен стремиться к 100%. Все сотрудники каждой компаний, в первую очередь из состава критической национальной инфраструктуры, должны проходить подготовку по кибербезопасности. Ошибка одного сотрудника может стоить любой компании полной потери бизнеса, а ее акционерам потери своих капиталовложений. Но следует помнить, что инсайдерское предательство представляет собой наибольшую угрозу и может по своим последствиям быть страшнее любой хакерской атаки. На первом месте по темпу прироста числа правонарушений в США сейчас находится «кража идентичности человека». Этот вид преступлений предельно опасен, пересекается со сферами терроризма и коррупции, и заслуживает специального обсуждения. Нужны меры уголовного преследования за новые виды правонарушений.

Сегодня взаимодействие правовых, налоговых и антимонопольных органов России в регулировании ими экономики осложнено постоянными новациями уголовного и другого законодательства и нестыковкой между программными продуктами, применяемыми различными ведомствами. По мере перехода экономики в цифру и резкого роста числа трансакций эти проблемы могут нарастать в геометрической прогрессии. При ухудшении делового климата гиперкомпьютеры позволят бизнесу уходить из-под контроля государственных органов в облачные юрисдикции.

Угроза всем видам частной собственности

На тему киберугроз в мире издано много книг, принято немало нормативных документов правительств, безусловно, лидируют США и Великобритания. Хакерство из протестного движения и вида интеллектуального спорта становится глобальной проблемой. Но дело не только в хакерах. ***Всей цифровой экономике необходим нравственный юридический стиль мышления и правовое регулирование.*** На программные угрозы необходимы системные программные ответы.

Опасность состоит прежде всего в том, что сегодня буквально каждый гражданин и буквально каждая компания в цифровой экономике каждой страны могут быть, сами того не ведая, неожиданно для себя разорены. Сегодня можно в одно мгновенье потерять все, что имеешь, и нет той силы, которая могла бы найти преступника, наказать его и вернуть украденное. Государство сегодня имеет ресурсы помочь лишь единицам из многих тысяч обворованных электронными жуликами. Что будет, если задачу воровства злоумышленники поставят гиперкомпьютерам с искусственным интеллектом?

Для иллюстрации приведу самый банальный вариант из нашей действительности далеко не уровня цифровой экономики. Это когда, например, ***в недвижимости вдруг официальные документы становятся недействительными, а ложные и подставные становятся действительными и законными, и затем подтверждаются судами. Такой уровень опасности сегодня в цифровой экономике существует практически повсеместно. Отсюда необходима фундаментальная юридическая защита российского бизнеса, как в России, так и за рубежом не ниже уровня новых угроз.***

Ровно год тому назад на Ялтинском экономическом форуме мы выдвинули концепцию принятия в России ***конституционного закона «О правовой защите бизнеса в Российской Федерации»***. Эта инициатива вызвала интерес в деловых кругах страны. В данной теме сегодня с нами сотрудничает целый ряд уважаемых объединений предпринимателей и корпораций. Мы по крупицам составляем типологию случаев нарушения прав предпринимателей, благодарны за

материалы, которые нам присылают из различных отраслей и регионов.

Угроза потери государством контроля над экономикой.

В целом в цифровой экономике пока наблюдается полное отсутствие ответственности. Преступления есть, а наказать их очень трудно. Отсутствие правого регулирования провоцирует положение, когда преступления становятся нормой, практикой, и даже образом жизни. ***Сегодня в России и во всем мире целые большие коллективы талантливых и честных людей трудятся в пока еще преступной системе, не понимая, что эта система преступна.*** Это предельно опасно не только для России, но для всего вступившего в эру «четвертой промышленной революции» человечества. За несколько лет вся наша экономика станет цифровой. Государство должно решительно не допустить правовой беспредел в цифровой экономике именно сейчас, пока наша страна находится в самом начале пути. Иначе государство может потерять контроль над экономикой как своим важнейшим инструментом.

Кому выгодна потеря нашим государством контроля над экономикой России? Есть два варианта ответа на этот вопрос. В области экономики - тем, кто стремится к экономической колонизации России. В области политики – тем, кто стремится к смене политического строя в России.

Ураганный рост в цифровой экономике есть недвусмысленное штормовое предупреждение государству. Опасность представляет собой «синдром Понтия Пилата», когда чиновник хоть и понимает масштаб чрезвычайной ситуации, подвергающей опасности всех и вся, но действует по служебной инструкции иногда и «ледникового периода», строго в своем узком секторе ответственности. Сегодня в ЦЭ вызовы таковы, что остро востребованы стратегические аналитики и наделенные властью высококомпетентные интеграторы исполнительных решений. Нужна ответственность и сосредоточение на решение проблем. Предпочтительно проектное управление темами ЦЭ.

5. Выводы

Отставание в России в цифровой экономике, а известное исследование Бостон Консалтинг Групп 2016 года разместило Россию на 39-ом месте среди цифровых экономик мира, для юристов - это не в последнюю очередь шанс избежать чужих ошибок.

По моему убеждению, заполнить существующий сегодня в цифровой экономике правовой вакуум и устранить опасность возникновения беспредела может административно-правовая дорожная карта, которая на первом этапе реализации Стратегии научно-технологического развития Российской Федерации в 2017 – 2019 годах заложит в государственной политике России ***такие системные и правовые подходы, которые в теории и на практике сделают обман в цифровой экономике нашей страны бессмысленным.***

Существует опасность того, что, если этого не сделать незамедлительно, то уже в ближайшие 5-7 лет существенная ***часть бизнеса вынужденно уйдет в облачные юрисдикции и по парадигме «облако с облаком» станет недоступной для регуляторов, налоговой службы и силовых структур страны***. И наоборот, именно решительное установление государством твердого порядка в цифровой экономике может стать тем долгожданным среди предпринимателей рычагом, который зачистит порочную практику заказных дел, оздоровит в стране деловой климат, вернет ушедшие капиталы и привлечет новые.

В России необходимо создать цифровое министерство обороны, цифровое министерство промышленности, цифровое министерство экономики, цифровое министерство науки и образования, цифровую полицию, цифровую налоговую службу и цифровую антимонопольную службу. Эти и другие цифровые структуры правительства должны ***а) аппаратно и б) программно надежно обеспечить кибербезопасность всей страны, в) право должно стать третьей несущей опорой кибербезопасности и цифровой экономики России.***

Сегодня достаточно посмотреть на число изменений в действующее законодательство, принимаемых каждый год, и судебных решений и комментариев по ним, чтобы увидеть право в роли служанки потребностей текущего дня. Это порождает недоверие к праву и государству. Даже профессора юридических ВУЗов не поспевают за нововведе-

ниями. В Российской Империи на разработку новых законов нередко уходило не менее 20 лет. Такого срока у нас в эпоху цифровой экономики нет. Но вернуть уважение и доверие к праву необходимо.

Вопрос господствующего в стране менталитета не менее важен, чем дух и буква законов и практики судов, ибо все мы - люди. Менталитет хозяина должен вернуться в Россию, указав на дверь менталитету временщика. Только тогда мы сможем говорить о системе правовой безопасности Российской Федерации как якоре стабильности, фундаменте инноваций и экономического роста в стране. Цифровая экономика может быть плодоносной только на почве триединой платформы, в которой сольются лаконичное бизнес-ориентированное правовое регулирование, грамотные аппаратные решения и пиковые достижения российских программистов.

Библиографический список:

Документы:

1. Указ Президента Российской Федерации от 01.12.2016 г. № 642 «О Стратегии научно-технологического развития Российской Федерации» http://www.kremlin.ru/acts/bank/41449 (дата обращения 15.01.2017 года).
2. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» http://www.kremlin.ru/acts/bank/41460 (дата обращения 15.01.2017 года).
3. Распоряжение Президента Российской Федерации от 03.04.2017 г. № 96-рп «Об утверждении Положения о рабочей группе Экономического совета при Президенте Российской Федерации по направлению «Цифровая экономика» http://www.kremlin.ru/acts/bank/41826 (дата обращения 10.04.2017 года).
4. Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы http://www.scrf.gov.ru/documents/6/136.html (дата обращения 15.12.2016 года).

Электронные библиотеки:

5. Глобальная библиотека права цифровой экономики АНО Форт.

Исследования и публикации:

6. KEY ISSUES FOR DIGITAL TRANSFORMATION IN THE G20. Report prepared for a joint G20 German Presidency/ OECD conference BERLIN, GERMANY. 12 JANUARY 2017. http://www.ranepa.ru/images/media/g20/2017hamburg/keyissues.pdf (дата обращения 10 апреля 2017 года).
7. „Wir wehren 4500 Cyberangriffe am Tag ab“ https://www.welt.de/politik/deutschland/article163733870/Wir-wehren-4500-Cyberangriffe-am-Tag-ab.html (дата обращения 15.04.2017 года).
8. Елизавета II открыла центр кибербезопасности в Лондоне http://www.kommersant.ru/doc/3219821 (дата обращения 16.02.2017 года).
9. Инициатива «Группы двадцати» по развитию и сотрудничеству в области цифровой экономики http://kremlin.ru/supplement/5111 (дата обращения 18.04.2017 года)
10. Россия онлайн? ДОГНАТЬ НЕЛЬЗЯ ОТСТАТЬ http://www.bcg.ru/documents/file210280.pdf (дата обращения 10.01.2017 года).
11. Платформа отраслевых экосистем цифровой экономики http://www.eurasiancommission.org/ru/act/dmi/workgroup/Documents/3.%20%D0%91%D0%B0%D0%B1%D0%B0%D1%8F%D0%BD%20%D0%95.%D0%91._%D0%9F%D0%BB%D0%B0%D1%82%D1%84%D0%BE%D1%80%D0%BC%D0%B0%20%D0%%D0%B5%D0%BC.pdf (дата обращения 10.02.2017 года).
12. Цифровая экономика http://ac.gov.ru/files/content/11704/cifrovaya-ekonomika-pushkin-v-1-6-dlya-mozgovogo-shturma-pdf.pdf (дата обращения 10.04.2017 года).
13. Шваб К. Четвертая промышленная революция. М., 2017.
14. Шульцева В.К. ЦИФРОВАЯ ЭКОНОМИКА КИТАЯ: "АССИМИЛЯЦИЯ! СОПРОТИВЛЕНИЕ БЕСПОЛЕЗНО!" Часть 1. ИМЭМО РАН, http://www.lastmile.su/journal/article/4702 (дата обращения 10.04.2017 года).