Advances in Law Studies (2020). Vol. 8. Special issue: 25–32
DOI 10.29039/2409-5087-2020-8-5-25-32

ПРАВО, ГОСУДАРСТВО, ОБЩЕСТВО В XXI ВЕКЕ

Риски и угрозы цифровизации

УДК 34.02

Гайворонская Яна Владимировна
Кандидат юридических наук, доцент, доцент кафедры теории и истории государства и права, Дальневосточный федеральный университет, Юридическая школа; E-mail: yanavl@yandex.ru.

Статья получена: 17.03.2020. Рассмотрена: 14.04.2020. Одобрена: 19.05.2020. Опубликована онлайн: 04.06.2020. © РИОР

Работа выполнена при финансовой поддержке Гранта Президента РФ № НШ-2668-2020.6 «Национально-культурные и цифровые тренды социально-экономического и политико-правового развития Российской Федерации в XXI веке».

Аннотация. Целью исследования является систематизация рисков и угроз цифровой трансформации общества для последующей выработки опережающих правотворческих решений. Рассмотрев предложенные в науке классификации угроз и рисков цифровизации, автор предлагает разделить все угрозы цифровизации на три группы: гипотетические, реальные и гносеологические. Наибольшей актуальностью обладают реальные угрозы, которые проявляются на современном этапе технического развития и остро требуют юридических решений. В целом все реальные угрозы связаны с проблемами безопасности личности, бизнеса, общества и государства в цифровой среде.

Ключевые слова: цифровизация, цифровая трансформация общества, сквозные цифровые технологии, угрозы цифровизации, проблемы цифровизации, риски цифровизации

Цифровая трансформация общества неотвратимо захватывает всё новые социальные институты и сферы деятельности. Масштабность и скорость протекания этой трансформации позволяют именовать сегодняшний этап развития цифровых технологий цифровой революцией. Практически всё пространство вокруг, включая нас самих, непосредственно является объектом цифровой трансформации. Однако за видимыми на первый взгляд перспективами скрываются серьезные угрозы, которые необходимо прогнозировать и освещать в целях предотвращения возможных негативных последствий.

При столь высокой динамике технического прогресса естественным образом нарушаются системность и эволюционность социального развития. В результате многие социальные институты (особенно «гуманитарной» направленности) и имеющиеся регуляторы общественных отношений не успевают адаптироваться к происходящим изменениям, усиливая социальный кризис.

Тема рисков и угроз цифровизации активно осваивается учеными различных направлений: экономисты, политики, правоведы и многие

DIGITALIZATION RISKS AND THREATS

Gaivoronskaya Yana Vladimirovna
PhD in Law, Associate Professor, Associate Professor of the Department of Theory and History of State and Law, Far Eastern Federal University Law School; E-mail: yanavl@yandex.ru.

Manuscript received: 17.03.2020. Revised: 14.04.2020. Accepted: 19.05.2020. Published online: 04.06.2020. © RIOR
This work was financially supported by the Russian Federation Presidential Grant No. НШ-2668-2020.6 "National-Cultural and Digital Trends in the Socio-Economic, Political and Legal Development of the Russian Federation in the 21st Century".

Abstract. The aim of the study is to systematize risks and threats of digital transformation of the society for subsequent development of advanced law-making decisions. Having considered classification of digitalization threats and risks of proposed in science, the author proposes to divide all the threats of digitalization into 3 groups: hypothetical, real and epistemological. The most crucial are the real threats that appear at the present stage of technical development and urgently require legal solutions. In general, all the real threats are associated with security problems of individuals, businesses, society and the state in a digital environment.

Keywords: digitalization, digital transformation of the society, end-to-end digital technologies, digitalization threats, digitalization problems, digitalization risks

другие обеспокоены столь быстрым распространением цифровой волны.

Появление любых изменений в экономике, политике, демографии, социальной жизни и т.д. связано с определенными вызовами и угрозами, что может проявиться в совокупности возможных проблем и отрицательных результатов. Каждый из этих нежелательных результатов (экономический, политический, демографический, социальный и т.д.) может быть представлен как риск, описываемый параметрами «размер возможного отрицательного результата» и «вероятность наступления отрицательного результата» [21, с. 53]. Однако, прежде чем оценивать потенциальные риски цифровой трансформации общественных отношений и разрабатывать превентивные правотворческие решения, необходимо определить сами нежелательные последствия, или проблемы цифровизации.

Термин «цифровизация» стал почти общепринятым, но при этом так и не обрел четкого смыслового значения. На уровне гуманитарных исследований и публицистики понятием цифровизации стали обозначать комплекс экономических, управленческих, социальных процессов, связанных с использованием и широким распространением, собственно, цифровых, компьютерных, информационных, электронных, сетевых, телекоммуникационных технологий в современной жизни. Представители общественных наук, рассуждая о плюсах и минусах цифровизации, используют понятия «цифровизация», «цифровые технологии», «информационные технологии», «автоматизация», «электронные технологии» и т.д. практически как синонимы.

В современном словоупотреблении термин «цифровые технологии» используется в узком смысле, т.е. применяется для обозначения последних достижений в области цифровых технологий и сквозных цифровых технологий. Ведь в широком смысле слова цифровая передача информации и цифровые машины были известны с прошлого века, именно на них основаны современные информационные и компьютерные технологии. Современный этап развития IT-технологий и сети Интернет называют цифровой революцией и связывают с цифровизацией производства, что выражается в создании глобальных промышленных сетей с использованием искусственного интеллекта, распространением Интернета вещей, сервисов автоматической идентификации, сбора и обработки глобальных баз данных, облачных технологий, социальных сетей, создании принципиально новых механизмов взаимодействия человека и машины [6, с. 13].

К проявлениям цифровизации как IV промышленной революции следует относить, прежде всего, так называемые сквозные цифровые технологии, которые затрагивают разные отрасли деятельности и в наибольшей степени влияют на развитие цифровой экономики. В федеральном проекте «Цифровые технологии», входящем в состав Национальной программы «Цифровая экономика Российской Федерации» [13; 10; 11], к сквозным цифровым технологиям отнесены: большие данные (Big Data), новые производственные технологии, промышленный интернет (Industrial Internet of Things, IIoT), искусственный интеллект (Artificial intelligence, AI, ИИ), технологии беспроводной связи, компоненты робототехники и сенсорика, квантовые технологии, системы распределенного реестра, технологии виртуальной (Virtual Reality, VR) и дополненной (Augmented Reality, AR) реальностей.

Целью нашего исследования является систематизация рисков и угроз цифровой трансформации общества для последующей выработки опережающих правотворческих решений. В данной работе мы будем использовать термин «цифровизация» в обобщающем смысле, для обозначения всех процессов цифровой трансформации общества и его отдельных институтов за счет внедрения информационных и сквозных цифровых технологий.

Большой пласт проблем цифровизации исследователи связывают с появлением и распространением искусственного интеллекта (потенциально — сильного ИИ) и как результат с возможным противостоянием человека и ИИ.

Однако, проводя проблематизацию вопроса о цифровой трансформации общества, его экономической, политической, правовой и культурной сферах, есть смысл разграничить уровни потенциальных рисков и угроз такой трансформации. Представляется разумным

разделить все потенциальные угрозы цифровизации на *гипотетические*, т.е. возможные в перспективе на высоком уровне технологического развития (уровне прогнозируемом, но в настоящий момент недоступном), и *реальные* (*насущные)*, т.е. очевидные и констатируемые в современном обществе на имеющемся уровне технологического развития.

Гипотетические угрозы связаны, прежде всего, с потенциально возможным появлением сильного ИИ, обладающего автономностью и сопоставимого с интеллектом человека. К гипотетическим угрозам относятся, в частности, возможное противостояние ИИ и человечества, конфликт ИИ с ноосферой, порождающие, в свою очередь, различные угрозы для существования человечества [18, с. 64]. В юридической плоскости к гипотетическим проблемам цифровизации относятся вопросы правосубъектности ИИ [8], распространения на юниты ИИ и автономные роботизированные аппараты (АРА) элементов правового статуса человека [5], в частности, прав человека [4].

Обобщая, можно сказать, что искусственный интеллект порождает угрозы и вызовы, «сопряженные с крайне сложно просчитываемыми рисками и поливариантностями, создает беспрецедентно много неопределенностей» [15, с. 105]. Иными словами, одной из наибольших проблем распространения ИИ является невозможность четко предугадать и спрогнозировать возможные угрозы и риски, связанные с этой технологией в будущем. Большая часть прогнозируемых на сегодняшний день угроз в сфере ИИ касается этических вопросов, точнее, возможных конфликтов современной антропоцентричной морали и логики функционирования будущих автономных носителей сильного ИИ. Исследователи констатируют, что «... развитие тех или иных опасных технологий без учета вопросов этики может привести человечество к совершенно катастрофическому результату» [17, с. 248]. С другой стороны, жесткие ограничения, сформулированные на заре формирования новой технологии, могут препятствовать технологическому и, следовательно, социально-экономическому и политическому развитию общности, что само по себе также можно признать одной из угроз цифровой эпохи (искусственное торможение развития, связанное с невозможностью деонтологического, правового и культурного опосредования происходящих изменений).

К *реальным* угрозам цифровизации, в полной мере осознаваемым и актуальным уже сегодня, относятся незащищенность персональных данных в киберпространстве и связанная с этим неспособность современных правовых средств осуществить регулирование и защиту общественных отношений; интеллектуализация военной робототехники и связанные с этим последствия, в частности, угроза потери людьми контроля над военными компьютерными системами; изменение рынка труда и технологическая безработица; распространение киберпреступности и неспособность правоохранительных органов обеспечить безопасность личности в интернет-пространстве; отсутствие правового регулирования Интернета и механизмов действенного государственно-правового контроля в интернет-среде и т.д.

Особняком хотелось бы поставить *гносеологические* проблемы цифровизации: угрозы классическим научным теориям и моделям, лежащим в основе действующих сейчас политических, правовых, экономических и иных социальных институтов. Например, в предметной области юриспруденции цифровизация несет угрозы классическим теориям государственного суверенитета [22], правосубъектности, лиц, правоотношений, которые становятся нереализуемыми в условиях киберпространства и/или с участием принципиально новых квазиакторов (юнитов ИИ, роботов-агентов и т.д.).

Право как регулятор общественных отношений претерпевает некоторые сущностные изменения, а выделяемые в теории основные признаки права в цифровую эпоху теряют прежний смысл [20, с. 15]. Новая цифровая реальность требует нового понимания всего механизма правового регулирования и, что особенно важно, нового понимания места права в стремительно меняющемся цифровом обществе [1, с. 324]. Требует модификации теория прав человека (как минимум в части расширения перечня официально закрепленных и гарантированных государством прав в цифровом обществе), что

повлечет за собой изменения в идеологии, основанной на этой теории. Смарт-контракт как новая форма договора [24], интернет-портал как официальный источник опубликования нормативно-правовых актов [1, с. 359] и многие другие нововведения подводят нас к тому, что именно трансформацией права как важнейшего института гражданского общества обусловлены технологические изменения, происходящие в юридической профессии.

Понятие информации образует отдельную междисциплинарную область, имеющую массу прикладных аспектов. Правовое регулирование информации как универсального объекта права является крайне сложным и устаревает еще до момента появления законопроекта (этим отчасти объясняется совершенно неудовлетворительное с точки зрения современных достижений технического прогресса состояние понятия информации в современном правовом поле). Эта ситуация, кстати, сама по себе становится одной из угроз цифровизации: перманентное отставание законодательства об информационных технологиях от реального уровня технологий, и отсутствие опережающих правотворческих решений.

Изменения категориального аппарата науки, методологии и предметной области исследований под влиянием цифровизации затрагивает, естественно, не только юриспруденцию, а практически все виды и области научного знания.

Основной упор в настоящее время нужно делать на предотвращение реальных угроз цифровизации (по терминологии нашей условной классификации). Не умаляя значимости других научных изысканий, хочется подчеркнуть срочный прикладной характер исследований в области реальных угроз цифровой трансформации общества. Уровень риска этой группы угроз высок, а для некоторых нерешенных вопросов является критическим, в то время как уровень риска гипотетических проблем цифровизации в настоящий момент является низким (или средним), что позволяет отсрочить их разрешение на уровне принятия правотворческих решений. Исследования группы насущных угроз цифровизации должны дать концепции и модели правового регулирования имеющихся общественных отношений, закрывая регулятивный вакуум и создавая возможности для дальнейшего развития, технического прогресса и научных исследований цифровизации.

Экономисты выделяют следующие группы проблем экономической безопасности цифрового общества: системные, структурные, отраслевые, деятельности отдельных предприятий, проблемы отдельных граждан. Проблематизация в данном случае осуществляется по критерию субъекта/института, в отношении интересов которого формируется угроза в связи с распространением цифровых технологий. К системным проблемам экономической безопасности отнесены проблемы, касающиеся экономики в целом или ее значительных частей (зависимость от цифровых технологий других государств, отсутствие собственной элементарной базы, проблема «цифрового неравенства»). Структурные проблемы, вызванные цифровизацией, связаны с изменением отдельных социальных институтов или системообразующих процессов в обществе (например, существенные изменения на рынке труда и рост безработицы). К отраслевым проблемам относится отсутствие цифровых решений для отдельных отраслей (например, отсутствие собственной платежной системы). Проблемы экономической безопасности деятельности отдельных предприятий затрагивают конкретных участников бизнеса (кража корпоративных данных, промышленный шпионаж, хакерские атаки, недостаточная обеспеченность цифровыми технологиями, компетентными кадрами и т.д.). К проблемам цифровой безопасности отдельных граждан относятся кража, манипулирование личными данными [16, с. 1088–1101].

Интересная обобщающая классификация предложена в исследовании А.И. Пискунова, посвященном цифровизации промышленности. В основу классификация глобальных вызовов и угроз цифровой трансформации общества, определенных на базе изучения материалов экономических форумов Давос-2016 и Давос-2017, положено определение сфер распространения потенциальных угроз. Вызовы и угрозы цифровизации разделены на 5 групп: I группа — угрозы, которые могут спровоцировать социальную и экономическую нестабильность (технологическая безработица и все ее

проявления); II группа — угрозы разрыва в уровнях технологического развития между странами, а также между различными экономическими группами в зависимости от доступа и эффективности использования интеллектуальных ресурсов; III группа — вероятность техногенных катастроф, неспособность человека лидировать в принятии управленческих решений по сравнению с интеллектуальными системами; IV группа — экологические риски и угрозы (интенсификация производства может привести к существенному изменению климата); V группа — угрозы снижения уровня национальной безопасности страны (риски усиления терроризма, сложность обеспечения конфиденциальности информации, угроза создания новых моделей кибероружия) [14, с. 12].

Сейчас мир переживает переломный момент — переход от «индустриального общества» к «обществу информационному». Развитие информационных технологий ставит ряд новых задач, требующих эффективного и качественного разрешения. Источником угроз и опасностей в этих условиях становится глобальная киберпреступность [9, с. 175].

В отчете ВЭФ по глобальным рискам (The Global Risks Report, 2018) такие общемировые угрозы, как киберпреступность и кража данных, расположены на третьем и четвертом месте по их значимости [25].

Интернет знает о человеке больше, чем он сам, его друзья и родные — в эпоху развития информационных технологий это уже не является шуткой. «Автоматическое исследование информационных запросов пользователей в Интернете, сведения с личных гаджетов, операции по банковским картам, электронная переписка и мессенджеры формируют блок информации о человеке, которую он и сам о себе может не знать», — указывают исследователи, объясняя суть угрозы хищения личных данных и использования их в корыстных целях [2, с. 146].

По данным правоохранительных органов только в 2019 г. число зарегистрированных в России IT-преступлений выросло на 70% (294 тыс.), они составляют уже 15% от всех регистрируемых в стране преступлений. По словам главы МВД, их раскрываемость выросла в 1,5 раза [3].

Одной из главных угроз для информационной безопасности на сегодняшний день специалисты называют киберпреступность с использованием вирусов-шифровальщиков. Опасность связана с тем, что такие «высокие технологии» проникают не только в персональные компьютеры, но и в засекреченные данные стратегических объектов, аэропортов, нефтепроводов, космодромов, оборонных предприятий, военных баз, АЭС, что грозит техногенными катастрофами и огромным ущербом [2, с. 146].

Попадание персональных данных в руки мошенников и сторонних лиц возможно как через кибератаки, так и через утечку информации из-за слабой защиты хранилища данных. Так, в 2018 г. кибератаке подвергся израильский сервис MyHetitage, в числе прочего позволяющий по ДНК-тесту установить родственные связи. Таким образом, в руки злоумышленников попала информация о биологических данных более 92 млн человек [23]. Самыми громкими случаями утечек в России являются выставление на продажу в 2019 г. персональных данных клиентов, включая кредитную историю и данные документов, «Альфа-Банка» и Сбербанка. Из зарубежных примеров можно назвать ошибку в коде взаимодействия между онлайн-магазином Apple и сервером T-Mobile, повлекшую утечку финансовой информации [12].

По статистике Президента компании InfoWatch в 2018 г. в мире утекло 7,28 млрд записей. А за первое полугодие 2019 — уже 8,74 млрд [7]. И связано это, прежде всего, со слишком быстрым внедрением цифровых технологий.

Кроме этого, всё более серьезными становятся риски, связанные с порчей и утратой информации вследствие вирусных заражений коммуникационных каналов и баз данных [19]. В эпоху промышленного интернета вещей всё больше данных будет оказываться в сети, а значит, всё более уязвимым будет становиться промышленное производство: злоумышленники удаленно могут вносить изменения в коды, на основе которых машины общаются между собой, принимая решения без участия человека. Негативные последствия в таких случаях могут быть катастрофическими: от хищения данных,

потери интеллектуальной собственности, порчи репутации компании и коммерческих убытков до остановки производств, техногенных или экологических катастроф [14, с. 11].

Подводя итоги, можно сказать, что основной проблемой цифровизации на сегодняшний день является обеспечение безопасности личности, бизнеса, общества и государства в цифровую эпоху. Проблема безопасности в условиях развития информационных технологий имеет множество проявлений, выступающих в качестве угроз либо отдельным социальным институтам, либо защищаемым законом правам и интересам лиц. По мнению исследователей, решение проблемы возможно только через активную деятельность государства. Именно государство должно создавать определенные правила и регулировать рынок [18]. Обеспечение безопасности персональных данных в сети эксперты связывают с установлением жестких мер ответственности со стороны государства за допущение потери данных [12]. Последовательная политика государства в этом направлении, в частности, введение юридических процедур, позволяющих пользователям в подобных случаях получать возмещение ущерба в заявительном порядке, могла бы повысить социальную ответственность бизнеса.

С точки зрения здравого смысла в разных сферах жизни применяется формула «если потенциальный риск от реализации некой идеи выше, чем предполагаемая польза, то от идеи надо отказаться». В случае с цифровизацией можно сказать, что ожидаемая польза может существенно превысить неудобства переходного периода, но только в случае контроля над процессами цифровой трансформации общества. Зная риски, можно минимизировать негативные последствия, но нельзя пускать технологическое развитие на самотек: потенциальные угрозы слишком серьезны и многоплановы.

Литература

1. Баранов П.П., Мамычев А.Ю., Мордовцев А.Ю. Права и свободы человека в цифровую эпоху: проблемы и перспективы политико-правовой динамики // Балтийский гуманитарный журнал. — 2019. — № 4(29). — С. 320–324, 359.
2. Бехер В.В., Зеленых Е.В. Цифровые технологии: угрозы и риски внедрения [Электронный ресурс] // Евразийское научное объединение. — 2019. — № 1–3(47). — С. 145–146. — URL: https://www.elibrary.ru/item.asp?id=36993290 (дата обращения: 15.03.2020).
3. В СК создан отдел по расследованию киберпреступлений [Электронный ресурс] // Tass.ru. — 03.03.2020. — URL: https://tass.ru/proisshestviya/7889859 (дата обращения: 15.03.2020).
4. Гайворонская Я.В., Мирошниченко О.И. Правовые проблемы цифровизации: теоретико-правовой аспект // Legal Concept = Pravovaya paradigma. — 2019. — № 18(4). — С. 27–34.
5. Дремлюга Р.И., Дремлюга О.А. Искусственный интеллект — субъект права: аргументы за и против // Правовая политика и правовая жизнь. — 2019. — № 2. — С. 120–125.
6. Карцхия А.А. Цифровая революция: новые технологии и новая реальность // Правовая информатика. — 2017. — № 1. — С. 13–18.
7. Касперская Н. Утечки конфиденциальной информации: почему их все больше и как с ними бороться [Электронный ресурс] // Tass.ru. — 21.11.2019. — URL: https://tass.ru/opinions/7164059 (дата обращения: 15.03.2020).
8. 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 жизнь. — 2019. — № 2. — С. 125–133.
9. Мартьянов Н.Р. Уголовно-правовая борьба с киберпреступлениями на современном этапе // Государственная служба и кадры. — 2020. — № 1. — С. 175–177.
10. Национальная программа «Цифровая экономика Российской Федерации» (включает 6 федеральных проектов): утв. Протоколом заседания президиума Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности от 28.05.2019 г. № 9 [Электронный ресурс] // Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций РФ. — URL: https://digital.gov.ru/ru/activity/directions/858/.
11. О системе управления реализации национальной программы «Цифровая экономика Российской Федерации»: Постановление Правительства РФ от 02.03.2019 № 234 [Электронный ресурс] // Официальный интернет-портал правовой информации. — URL: http://publication.pravo.gov.ru/Document/View/0001201903070015.
12. Оганесян А. Болезнь цифрового мира: как защититься от утечек персональных данных [Электронный ресурс] // Forbes. — 23.05.2019. — URL: https://yandex.ru/turbo?text=https%3A%2F%2Fwww.forbes.ru%2Ftehnologii%2F376499-bolezn-cifrovogo-mira-kak-zashchititsya-ot-utechek-personalnyh-dannyh.
13. Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”»: утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 04.06.2019 № 7 // СПС КонсультантПлюс.
14. Пискунов А.И. Вызовы, угрозы и ожидания цифровизации для промышленных предприятий // Организатор производства. — 2019. — № 27(2). — С. 7–14.
15. Понкин И.В., Редькина А.И. Искусственный интеллект с точки зрения права // Вестник РУДН. — Серия: Юридические науки. — 2018. — № 22(1). — С. 91–109.
16. Попов Е.В., Семячков А.А. Проблемы экономической безопасности цифрового общества в условиях глобализации // Экономика региона. — 2018. — № 14(4). — С. 1088–1101.

17. Ройзензон Г.В. Проблемы формализации понятия этики в искусственном интеллекте [Электронный ресурс] // Шестнадцатая национальная конференция по искусственному интеллекту с международным участием КИИ-2018. Труды конференции: в 2 томах. — М.: Издательство: Федеральное государственное предприятие «Информационное телеграфное агентство России (ИТАР-ТАСС)» филиал «Российская книжная палата», 2018. — С. 245–252. — URL: https://elibrary.ru/item.asp?id=35568660 (дата обращения: 25.09.2019).
18. Самсонова А. Российский IoT не справляется с киберугрозами [Электронный ресурс] // COMNEWS: новости цифровой трансформации, телекоммуникаций, вещания и ИТ. — URL: https://www.comnews.ru/content/204931/2020-03-10/2020-w11/rossiyskiy-iot-nespravlyaetsya-kiberugrozami?utm_source=telegram&utm_medium=general&utm_campaign=general (дата обращения: 31.03.2020).
19. Стерледев Р.К., Стерледева Т.Д. Искусственный интеллект в аспекте ноосферы: почти фантастика? // Вестник ПНИПУ. Культура. История. Философия. Право. — 2017. — № 2. — С. 61–65.
20. Сулейманов М.Д. Цифровизация: угрозы или прорывная трансформация экономики? [Электронный ресурс] // Фонд науки и образования: официальный сайт. — URL: http://фонд-науки.рф/menu/novosti-fonda/558-tsifrovizatsiya-ugroza-ili-proryvnaya-transformatsiya-ekonomiki.html (дата обращения: 15.03.2020).
21. Талапина Э.В. Право и цифровизация: новые вызовы и перспективы // Журнал российского права. — 2018. — № 2. — С. 5–17, 53.
22. Халин В.Г., Чернов Г.В. Цифровизация и ее влияние на российскую экономику и общество: преимущества, вызовы, угрозы и риски // Управленческое консультирование. — 2018. — № 10. — С. 46–63.
23. Шестопал С.С., Мамычев А.Ю. Суверенитет в глобальном цифровом измерении: современные тренды // Балтийский гуманитарный журнал. — 2020. — № 1(30). — С. 398–403.
24. MyHeritage Statement About a Cybersecurity Incident. URL: https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/.
25. Rusakova E.P., Frolova E.E., Gorbacheva A., Kupchina E.V. Implementation of the smart-contract construction in the legal system. *6th international conference on education, social sciences and humanities*. 2019, pp. 748–753.
26. The Global Risks Report 2018 13th Edition. URL: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (accessed 26 March 2020).

References

1. Baranov P.P., Mamychev A.Yu., Mordovtsev A.Yu. Human rights and freedoms in the digital age: problems and prospects of political and legal dynamics. *Baltic humanitarian journal*. 2019, no. 4(29), pp. 320–324, 359.
2. Beher V.V., Zelenykh E.V. Digital technologies: threats and risks of implementation. *Eurasian scientific association*. 2019, no. 1–3(47), pp. 145–146. URL: https://www.elibrary.ru/item.asp?id=36993290 (accessed 15 March 2020).
3. In the UK created the Department for the investigation of cybercrime. *Tass.ru*. 3 March 2020. URL: https://tass.ru/proisshestviya/7889859 (accessed 15 March 2020).
4. Gaivoronskaya Ya.V., Miroshnichenko O.I. Legal problems of digitalization: theoretical and legal aspect. *Legal concept = legal paradigm*. 2019, no. 18(4), pp. 27–34.
5. Dremlyuga R.I., Dremlyuga O.A. Artificial intelligence — the subject of law: arguments for and against. *Legal policy and legal life*. 2019, no. 2, pp. 120–125.
6. Carchia A.A. the Digital revolution: new technologies and the new reality. *Legal Informatics*. 2017, no. 1, pp. 13–18.
7. Kaspersky N. Leaks of confidential information: why are there more and more of them and how to deal with them. *Tass.ru*. 21 November 2019. URL: https://tass.ru/opinions/7164059 (accessed 15 March 2020).
8. Mamychev A.Yu., Miroshnichenko O.I. Modelling the future of law: problems and contradictions of legal policy in the sphere of regulatory regulation of artificial intelligence systems and robotic technologies. *Legal policy and legal life*. 2019, no. 2, pp. 125–133.
9. Martianov N.R. Criminal and legal fight against cybercrime at the present stage. *State service and personnel*. 2020, no. 1, pp. 175–177.
10. The national programme "Digital economy of the Russian Federation" (includes 6 Federal projects): approved by the report of presidium of the government commission on digital development, use of information technologies for improvement of quality of life and conditions of conducting business activity from the 28th of May 2019 no. 9. *Official website of the Ministry of digital development, communications and mass communications of the Russian Federation*. URL: https://digital.gov.ru/ru/activity/directions/858/.
11. The control system implementation of the national programme "Digital economy of the Russian Federation": Resolution of the Russian Federation Government from the 2nd of March 2019 no. 234. *Official web portal of legal information*. URL: http://publication.pravo.gov.ru/Document/View/0001201903070015.
12. Oganesyan A. The disease of the digital world: how to protect yourself from personal data leaks. *Forbes*. 23 May 2019. URL: https://yandex.ru/turbo?text=https%3A%2F%2Fwww.forbes.ru%2Ftehnologii%2F376499-bolezn-cifrovogo-mira-kak-zashchititsya-ot-utechek-personalnyh-dannyh.
13. Passport of the national project "National program of the digital economy of the Russian Federation": approved by the presidium of the Presidential Council for Strategy Development and National Projects, report no. 7 from the 4th of June 2019. *ConsultantPlus*.
14. Piskunov A.I. Challenges, threats and expectations of digitalization for industrial enterprises. *Organizer of production*. 2019, no. 27(2), pp. 7–14.
15. Ponkin I.V., Redkina A.I. Artificial intelligence from the point of view of law. *Vestnik RUDN*. Series: Legal Sciences. 2018, no. 22(1), pp. 91–109.
16. Popov E.V., Semyachkov A.A. Problems of economic security of digital society in the conditions of globalization. *Regional economy*. 2018, no. 14(4), pp. 1088–1101.
17. Roizenzon G.V. Problems of formalization of the concept of ethics in artificial intelligence. Shestnadczataya nacional`naya konferenciya po iskusstvennomu intellektu s mezhdunarodny`m uchastiem KII-2018. Trudy` konferencii: v 2 tomax [Sixteenth national conference on artificial intelligence with international participation CII-2018. Proceedings of the conference: in 2 volumes]. Moscow, publishing House: federal state unitary enterprise "Information Telegraph Agency of Russia (ITAR-TASS)" branch "the Russian book chamber", 2018, pp. 245–252. URL: https://elibrary.ru/item.asp?id=35568660 (accessed 25 September 2019).
18. Samsonova A. Russian IOT does not cope with cyber threats. *COMNEWS: news of digital transformation, telecommunications, broadcasting and IT*. URL: https://www.comnews.ru/content/204931/2020-03-10/2020-w11/

rossiyskiy-iot-ne-spravlyaetsya-kiberugrozami?utm_source=telegram&utm_medium=general&utm_campaign=general (accessed 31 March 2020).
19. Sterledev R.K., Sterledeva T.D. Artificial intelligence in the aspect of the noosphere: almost fiction? *PNRPU Mechanics Bulletin. Culture. History. Philosophy. Right*. 2017, no. 2, pp. 61–65.
20. Suleymanov M.D. Digitalization: threats or breakthrough transformation of the economy? *Foundation of science and education: official website*. URL: http://фонд-науки.рф/menu/novosti-fonda/558-tsifrovizatsiya-ugroza-ili-proryvnaya-transformatsiya-ekonomiki.html (accessed 15 March 2020).
21. Talapina E.V. Law and digitalization: new challenges and prospects. *Journal of Russian law*. 2018, no. 2, pp. 5–17, 53.
22. Khalin V.G., Chernov G.V. Digitalization and its impact on the Russian economy and society: advantages, challenges, threats and risks. *Management consulting*. 2018, no. 10, pp. 46–63.
23. Shestopal S.S., Mamychev A.Yu. Sovereignty in the global digital dimension: modern trends. *Baltic humanitarian journal*. 2020, no. 1(30), pp. 398–403.
24. MyHeritage Statement About a Cybersecurity Incident. URL: https://blog.myheritage.com/2018/06/myheritage-statement-about-a-cybersecurity-incident/.
25. Rusakova E.P., Frolova E.E., Gorbacheva A., Kupchina E.V. Implementation of the smart-contract construction in the legal system. *6th international conference on education, social sciences and humanities*. 2019, pp. 748–753.
26. The Global Risks Report 2018 13th Edition. URL: http://www3.weforum.org/docs/WEF_GRR18_Report.pdf (accessed 26 March 2020).