Ключевые риски развития цифровой экономики: новые вызовы для системы государственного управления

Шувалов С.С.,
кандидат экономических наук, старший научный сотрудник, Институт экономики РАН

Аннотация. В статье рассматриваются ключевые риски, связанные с развитием цифровой экономики в России и за рубежом, и порождаемые ими вызовы для системы государственного управления. Принимаются во внимание риски различной природы (технологические, институциональные, социально-экономические, геополитические и др.), характерные для разных этапов развития цифровой экономики. Выделяются ключевые направления государственного регулирования в части управления рисками развития цифровой экономики.
Ключевые слова: цифровая экономика, цифровое правительство, риски, государственное управление, вызовы, государственное регулирование.

The key risks of the digital economy: new challenges for the public administration

Shuvalov S.S.,
PhD in Economics, Senior Researcher, Institute of Economics of the Russian Academy of Sciences

Abstract. The paper deals with the key risks associated with the digital economy in Russia and other countries and the public administration challenges generated by the risks. The author takes into account various types of risks in accordance with their nature (technological, institutional, socioeconomic, geopolitical etc.) and the stage of the economy digitization. The urgent tracks of the governmental regulation for risk management in the digital economy are highlighted.
Keywords: digital economy, digital government, risks, public administration, challenges, governmental regulation.

Введение

В последние годы проблемы развития цифровой экономики находятся в фокусе внимания исследователей, аналитиков и практиков в большинстве стран мира, включая Россию. К настоящему времени опубликовано значительное количество работ, в которых рассматриваются различные положительные и отрицательные аспекты развития цифровой экономики, в том числе возможности и угрозы. Существуют также работы, посвященные анализу рисков, связанных с развитием цифровой экономики. Вместе с тем в большинстве опубликованных работ, как правило, рассматриваются отдельные риски развития цифровой экономики, входящие в круг научных интересов тех или иных авторов. Наблюдается определенный дефицит работ, в которых риски развития цифровой экономики рассматривались бы достаточно комплексно и в их взаимосвязи.

В настоящей работе на основе изучения значительного количества разнообразных источников предпринята попытка построения комплексной «кар-

тины рисков» развития цифровой экономики и порождаемых ими вызовов для системы государственного управления. Под риском в данной работе понимается вероятность наступления события, которое может оказать негативное влияние на государственную безопасность, состояние окружающей среды, социально-экономического развитие страны, безопасность, здоровье и благосостояние человека и пр. При этом под вызовом для системы государственного управления в данном контексте понимается необходимость создания условий, включая институты, направленных на управление соответствующими рисками, в том числе посредством предотвращения наступления неблагоприятного события или минимизации негативных последствий его наступления.

Следует подчеркнуть, что параллельно с процессами цифровизации экономики в России и за рубежом происходят процессы цифровизации государства, системы государственного управления. При этом одними исследователями процессы цифровизации государства рассматриваются как самостоятельный феномен, а другими — как неотъемлемая составляющая общего процесса цифровизации экономики. В данной работе предлагается различать процессы цифровизации и цифровой трансформации системы государственного управления. Под цифровизацией предлагается понимать использование цифровых технологий при производстве и реализации товаров и оказании услуг, в том числе государственных [5]. В такой логике процесс цифровизации системы государственного управления и связанные с ним риски предлагается рассматривать в контексте процесса цифровизации экономики. При этом под цифровой трансформацией системы государственного управления предлагается понимать более сложный и длительный процесс эволюции институтов, содержания, функций, концепций и даже парадигм государственного управления в процессе и (или) в результате цифровизации [9]. Данный процесс, с одной стороны, до некоторой степени является ответом на вызовы цифровизации, с другой стороны — характеризуется своими собственными рисками и вызовами, которые также необходимо принимать во внимание. В частности, одним из существенных барьеров на пути цифровой трансформации государства может стать отставание институциональных изменений от технологических [8].

В данной работе рассматриваются две принципиально разные группы рисков развития цифровой экономики. Первая группа рисков представлена рисками, возникающими на начальном этапе формирования цифровой экономики и ставящими под угрозу саму возможность формирования эффективной цифровой экономики на национальном уровне и суверенного цифрового государства. Вторая группа рисков включает в себя риски, связанные с дальнейшим распространением цифровых технологий и функционированием цифровой экономики.

Кроме того, риски развития цифровой экономики можно разделить на универсальные (характерные для большинства стран мира) и национальные (характерные для конкретных стран). В данной работе рассматриваются как универсальные риски, так и риски, специфичные для развития цифровой экономики в России.

1. Риски, связанные с формированием цифровой экономики

Центром стратегических разработок (ЦСР) выделяются шесть ключевых рисков, которые могут оказать серьезное негативное влияние на темпы и результаты цифровизации российской экономики [7].

Первый риск — недостаточно оперативная подготовка необходимой нормативной базы, несвоевременное изменение существующих и (или) принятие новых нормативных актов, в том числе определяющих принципиальную возможность использования тех или иных цифровых технологий.

Второй риск — сопротивление цифровой трансформации со стороны сложившихся управленческих структур, отсутствие необходимой поддержки изменений на уровне среднего управленческого звена.

Третий риск — недостаток государственных и частных инвестиций в развитие цифровой экономики.

Четвертый риск — недостаток технологических и управленческих компетенций, в том числе в сфере разработки, развертывания и поддержки функционирования платформенных решений государственного уровня.

В контексте перечисленных рисков следует отметить, что консервативность бюрократии и ее неготовность к применению передовых технологий, а также отсутствие должного внимания к обновлению инфраструктуры в некоторых случаях тормозит развитие цифрового правительства, особенно на региональном и местном уровнях, даже в странах — лидерах технологического развития. Например, в США многие ведомства до сих пор заказывают разработку программного обеспечения на базе устаревших языков компьютерного программирования, некоторые из которых были созданы еще в конце 1950-х гг., а средний возраст компьютеров в некоторых американских ведомствах приближается к 30 годам [20].

Пятый риск — консервативность населения, недостаточная информированность конечных пользователей о возможностях и преимуществах использования цифровых технологий и (или) отсутствие достаточного уровня заинтересованности в их использовании.

Шестой риск — несоответствующее качество данных в существующих хранилищах, технические проблемы объединения данных из различных хранилищ, проблемы корректной классификации данных по уровням доступа и защиты, наличие административных барьеров, препятствующих совместному использованию отдельных массивов данных.

Кроме того, по мнению Натальи Касперской, на этапе формирования цифровой экономики в России возникают риски поспешного заимствования иностранных технологий с последующей деградацией собственных цифровых компетенций и вытекающие из этого риски захвата российского рынка и российской экономики транснациональными и зарубежными игроками [10]. Данные риски во многом связаны с рисками неверного определения технологических приоритетов бюджетных инвестиций в развитие цифровой экономики с сопутствующей дезориентацией частных инвесторов относительно приоритетов инвестирования. Высокая вероятность соответствующих рисков во многом определяется недостаточной квалификацией государственного аппарата и окружающего его экспертного сообщества, зачастую не обладаю-

щих необходимыми техническими и экономическими знаниями и попросту попадающих под влияние медийного «хайпа». В результате нагнетается атмосфера нервозности, боязни опоздать, алармистские призывы развивать и внедрять те или иные технологии без внятных оценок их реальной необходимости, обществу и бизнесу навязывается неактуальная повестка, деньги тратятся на тупиковые или неактуальные для страны технологии.

В этом контексте примечательно, что существуют научные работы, в которых на основе эмпирических наблюдений показано, что форсированная цифровизация системы государственного управления, несмотря на наличие политической воли, технологий и финансовых ресурсов, не всегда возможна и целесообразна, и в общем случае цифровизация системы государственного управления представляет собой достаточно длительный эволюционный процесс, состоящий из последовательно сменяющих друг друга стадий, каждая из которых характеризуется своими целями, задачами и вызовами. Кроме того, констатируется, что истории успеха в области цифровой трансформации системы государственного управления, как правило, возникают не тогда, когда ее тотальная цифровизация ставится в качестве самоцели, а тогда, когда конкретные цифровые решения в системе государственного управления рассматриваются как средство преодоления конкретных социально-экономических, политических и других вызовов [16].

Наличие существенных проблем и рисков, связанных с недостаточным уровнем развития и внедрения собственных цифровых технологий и кадрового обеспечения для формирования цифровой экономики, подчеркивается значительным числом российских исследователей. Причем последняя проблема характерна не только для России — например, около 90% международных компаний признают, что испытывают серьезный дефицит «цифровых талантов» [6]. Таким образом, на этапе становления российской цифровой экономики ключевыми вызовами для системы государственного управления становятся необходимость развития цифровой инфраструктуры, совершенствование регуляторной среды, преодоление дефицита «цифровых талантов», развитие цифровых компетенций у работников государственного аппарата и широких слоев населения [11].

2. Риски, связанные с функционированием цифровой экономики

В Докладе о глобальных рисках, подготовленном Всемирным экономическим форумом (ВЭФ) в 2017 г., выделяются ключевые глобальные тренды и определяемые ими риски, а также технологии, под влиянием которых формируются данные тренды и риски [21]. В Докладе выделяются 12 ключевых технологий, развитие и распространение которых уже сейчас начинает оказывать значительное влияние, а в среднесрочной перспективе будет оказывать решающее влияние на развитие мировой экономики и формирование соответствующих трендов и сопутствующих рисков. Примечательно, что в той или иной степени все выделенные технологии имеют «цифровую составляющую», а само их развитие и внедрение будет во многом зависеть от прогресса в развитии технологий цифрового блока. При этом ровно половину из выделенных технологий можно отнести к цифровым технологиям «в чистом виде»:

- искусственный интеллект и робототехника;
- блокчейн и технологии распределенного реестра;
- технологии «Интернета вещей»;
- нейротехнологии;
- новые технологии компьютерных вычислений, в том числе в области облачных, оптических и квантовых вычислений, обработки нейронных сетей и др.;
- технологии виртуальной и дополненной реальности.

Из 13 выделенных в Докладе ВЭФ ключевых глобальных трендов два прямо или опосредованно определяются развитием цифровых технологий:

- возрастание цифровой зависимости под влиянием развития цифровых технологий, в том числе в силу возрастающей цифровой взаимосвязи между индивидами, активами и организациями;
- изменение ландшафта международного управления, глобальных и региональных институтов, соглашений и сетей, в том числе под воздействием цифровых технологий.

В числе ключевых рисков, вероятность и значимость которых повышается в связи с развитием рассмотренных цифровых технологий и глобальных трендов, в Докладе ВЭФ выделяются следующие:

- риски сбоев в работе критической инфраструктуры, в том числе энергетической, транспортной и коммуникационной, вследствие недостатка инвестиций в ее обновление и обеспечение безопасности;
- риски возникновения рукотворных экологических и иных катастроф;
- риски эскалации межгосударственных конфликтов, в ходе которых могут быть использованы кибератаки и другие достижения цифровых технологий;
- риски непредвиденных негативных последствий развития и внедрения цифровых технологий, в том числе искусственного интеллекта, для человека, окружающей среды и экономики;
- риски сбоев в работе критической информационной инфраструктуры, разрушительный эффект которых особенно велик в условиях возрастающей цифровой зависимости;
- риски масштабных кибератак, способных привести в том числе к серьезным экономическим последствиям, геополитическим конфликтам и утрате доверия к интернету;
- риски кражи государственных, корпоративных или персональных данных и мошенничества с ними;
- риски террористических атак;
- риски роста незаконной торговли, в том числе трансграничной;
- риски утраты суверенитета национальных государств;
- риски роста безработицы.

Следует подчеркнуть, что многие из перечисленных выше рисков, такие как риски террористических атак, межгосударственных конфликтов, утраты национального суверенитета и другие, на первый взгляд, не являются специфичными именно для цифровой экономики, поскольку подобные риски имели место в мировой истории задолго до появления цифровых технологий.

Однако появление и распространение цифровых технологий качественно меняет природу данных рисков, например, делая возможным совершение террористических атак и актов межгосударственной агрессии (в том числе вывод из строя систем управления объектами критической инфраструктуры, коммуникаций, промышленных и военных объектов) дистанционно, например через кибератаки, которые, в свою очередь, могут быть как причиной (или поводом) для межгосударственных конфликтов, так и действенным оружием в конкурентной борьбе. Риски утраты национального суверенитета также значительно возрастают в результате возможной «цифровой колонизации» экономик и государств, не имеющих собственных технологий и сильно зависимых от их импорта. Таким образом, перечисленные риски на самом деле теснейшим образом связаны с разработкой и внедрением цифровых технологий, формированием и функционированием цифровой экономики.

Повышение взаимосвязанности и взаимозависимости предметов и систем, распространение «Интернета вещей» и развитие кибер-физических систем, с одной стороны, повышает устойчивость критической инфраструктуры, с другой стороны, делает ее более уязвимой. В теории распределенные системы более устойчивы к внешним шокам, однако на практике взаимозависимость больших и сложных систем (энергетических, транспортных и др.) таит в себе риски одновременных сбоев многих систем жизнеобеспечения в результате действия самых разных факторов — природных катаклизмов, сбоев в программном обеспечении, кибератак и др. Многими экспертами данное обстоятельство рассматривается как один из ключевых стратегических рисков государственного управления в цифровой экономике.

Значимость данной группы рисков может быть проиллюстрирована на примере вируса WannaCry, поразившего в 2017 г. компьютеры в более чем 150 странах мира. Действие вируса на некоторое время практически парализовало работу крупных структур, функционирующих в разных секторах мировой экономики — Национальной службы здравоохранения Великобритании, испанской телекоммуникационной компании Telefonica, американской логистической компании FedEx, немецкой железнодорожной компании Deutsche Bahn, ряд крупных промышленных компаний (Nissan Motor, Renault и др.) на время остановили производственные линии.

Риски утраты суверенитета национальных государств связаны, кроме того, с угрозами непропорционального роста влияния крупных корпоративных игроков на социально-экономические процессы по сравнению с государством. Предпосылкой такого риска является более высокая оперативность корпоративного сектора по сравнению с государством во внедрении передовых технологий и моделей управления, которая в условиях цифровой экономики с ее возможностями по сбору и анализу Больших данных еще больше усиливает конкурентные преимущества и лоббистские возможности крупного капитала. Констатируется, что подобная тенденция уже начинает проявляться во многих странах, независимо от уровня их развития. Данный риск, в свою очередь, усиливает риски монополизации экономики и социально-экономической нестабильности [4]. В государствах, уделяющих должное внимание внедрению цифровых технологий в систему государственного управ-

ления и своевременной адаптации управленческих моделей, подобного рода риски в определенной мере нивелируются. Вместе с тем существующее антимонопольное регулирование даже в наиболее передовых государствах пока что слабо учитывает реалии цифровой экономики [15].

Мнение о том, что развитие цифровой экономики может привести к значительному росту безработицы, разделяется широким кругом экспертов, в том числе российских. При этом риски роста безработицы порождают риски роста социальной дезадаптации и социального неравенства [1]. Эксперты ВЭФ подчеркивают, что наиболее сильное влияние на рынок труда потенциально могут оказать технологии искусственного интеллекта, способные заместить значительное количество и белых, и синих воротничков, вызвав тем самым социальные шоки. Помимо этого, развитие технологий искусственного интеллекта порождает дополнительный пласт специфичных проблем и угроз, в том числе:

- проблемы социальной ответственности искусственного интеллекта (например, уже сейчас эта проблема широко обсуждается применительно к разработке алгоритмов поведения беспилотного автомобиля в потенциально аварийных ситуациях);
- угрозы милитаризации искусственного интеллекта на фоне ограниченных возможностей международного регулирования данного процесса.

Последний пункт включает в себя риски, связанные не только с ведущимися разработками систем вооружения, использующих технологии искусственного интеллекта, но и разработками в области управления поведением больших групп людей на основе технологий искусственного интеллекта, нейротехнологий и технологий анализа Больших данных (когнитивного оружия), преследующими зачастую отнюдь не мирные цели [4].

Применительно к России рассмотренную картину следует дополнить некоторыми специфичными именно для нашей страны рисками и их модификациями, на которые обращает внимает Наталья Касперская [10].

Согласно Касперской, дальнейшее развитие и массовое внедрение технологий искусственного интеллекта, автоматизации и роботизации повышает риски сокращения рабочих мест и роста безработицы, расширения социального иждивенчества и сопутствующего этим процессам роста социальной напряженности. Распространение платформенных технологий и соответствующая «уберизация» медицины, образования, транспорта и других услуг повышает риски юридической неопределенности и мошенничества, риски разрушения сложившихся социальных связей. Развитие и широкое внедрение технологий сбора и анализа Больших данных, электронной идентификации и аутентификации, создание «цифровых двойников» граждан повышают риски неприкосновенности частной жизни, риски манипулирования общественным мнением, утечки персональных данных российских граждан за рубеж.

Риски неконтролируемого распространения криптовалют, эмиссия и оборот которых практически неподконтрольны государству, угрожают стабильности не только финансовой системы и фондового рынка, но и всей экономики, а также грозят расширением финансирования различных видов незакон-

ной деятельности. На значимость данного риска и для других экономик обращают внимание и некоторые зарубежные эксперты [14].

Ставка на импорт зарубежных технологий и продуктов для формирования цифровой экономики без должной «цифровой гигиены» порождает риски усиления контроля внешних игроков над российским рынком и риски внешнего управления, так называемой «цифровой колонизации». Одной из характеристик современных бизнес-моделей различных продуктовых и сервисных компаний, особенно в сфере информационных технологий, можно считать так называемую «модель подписки», в рамках которой при непосредственном приобретении продукта потребитель платит, по сути, только начальную сумму, а основные платежи по этапу жизненного цикла продукта приходятся на подписку на программное обеспечение, обновление программного обеспечения, расходные материалы и пр. Таким образом иностранные компании за счет относительно невысокой цены продукта (начальной суммы) «подсаживают» потребителей на свои продукты, вынуждая их платить вновь и вновь для поддержания работоспособности приобретенного продукта. В результате массовое использование в целях формирования отечественной цифровой экономики импортных технологий и продуктов частными и тем более государственными структурами чревато дальнейшим усилением контроля иностранных игроков над российским рынком и российской экономикой в целом. Но еще более важно то, что практически все современные продукты, имеющие цифровую составляющую (включая смартфоны и другую потребительскую электронику, транспортные средства, средства производства и пр.), постоянно связаны с интернетом, скачивают обновления и управляются извне: если это американские или европейские продукты, то и управляются они, соответственно, с территории США или Европейского Союза. Таким образом, импорт многих технологий и продуктов без необходимой «цифровой гигиены» значительно усиливает риски удаленного контроля и внешнего управления.

3. Вызовы для системы государственного управления

По мнению экспертов ВЭФ [21], рассмотренные цифровые технологии и другие связанные с ними технологии четвертой промышленной революции неизбежно окажут серьезное влияние на глобальное развитие — как положительное, так и отрицательное. При этом степень, до которой положительное влияние можно максимизировать, а негативное влияние — смягчить, во многом зависит от качества государственного управления, в том числе правил, норм, стандартов, стимулов, институтов и других механизмов, которые определяют развитие и распространение каждой конкретной технологии.

В идеальной ситуации государственные режимы должны быть достаточно стабильными, предсказуемыми и прозрачными для создания атмосферы доверия и осведомленности в среде инвесторов, компаний и ученых, а также потенциальных конечных потребителей новых продуктов. Однако при этом государственные режимы должны быть достаточно гибкими, для того чтобы оперативно реагировать на изменения технологий как в части их эффективного регулирования, так и в части адаптации в своих интересах. Например,

в настоящее время в некоторых странах звучат призывы к запрету беспилотного транспорта поскольку, во-первых, нет доказательств его полной безопасности, во-вторых, его широкое распространение может привести к росту безработицы среди водителей, таксистов и пр. В такой ситуации возрастает важность как обратных связей с обществом, так и опережающего развития регулирования, что возможно лишь в среде стабильности и взаимного доверия, с одной стороны, и разумной гибкости системы государственного управления, — с другой.

Таким образом, хотя, на первый взгляд, многие из рассмотренных технологических и других связанных с ними рисков не имеют прямого отношения к системе государственного управления, именно регулирование разработки и распространения тех или иных технологий, в том числе через систему стандартов и регламентов, с целью максимизации извлекаемых выгод и минимизации возможных угроз, являющееся неотъемлемой и одной из приоритетных задач современной системы государственного управления, можно считать одним из механизмов управления такими рисками.

Так, на сегодняшний день в мире практически отсутствует регуляторная база технологий искусственного интеллекта. Исключением можно считать разработанную Департаментом транспорта США нормативную базу в области беспилотного транспорта, использующего технологии искусственного интеллекта, которая не регулирует непосредственно сами технологии искусственного интеллекта, однако устанавливает достаточно детализированные требования к безопасности, контролируемости и испытаниям беспилотных транспортных средств. В целом же, согласно результатам исследования ВЭФ, технологии искусственного интеллекта и робототехники (наряду с биотехнологиями) воспринимаются в мировом сообществе в числе наиболее остро нуждающихся в эффективном государственном регулировании.

Внедрение новых технологий и радикальных инноваций способно оказать разрушающее воздействие на существующие бизнес-модели и целые сектора промышленности. Однако грамотное государственное регулирование и разумная инвестиционная политика могут помочь национальной промышленности если не стать первопроходцами и теми, кто создает правила игры, то хотя бы смягчить возможные негативные последствия, в том числе за счет обеспечения поэтапного внедрения новых технологий, развития эволюционного сценария вместо революционного. В качестве примера экспертами ВЭФ снова приводится беспилотный транспорт. Действительно, появление полностью беспилотного автомобиля можно считать делом не столь отдаленного, но все же будущего. Однако количество и качество отдельных элементов, технологий и продуктов будущих систем автономного транспорта, внедренных в «обычные» современные автомобили, постоянно возрастает, и их производители все лучше осваивают соответствующие компетенции. Таким образом, появление на рынке полностью беспилотных автомобилей едва ли станет шоком для сегодняшних ведущих автогигантов и будет способствовать их вытеснению с рынка. При этом такое развитие событий во многом обусловлено именно разумной государственной политикой.

Похожие примеры можно привести и относительно постепенного развития и распространения и многих других технологий четвертой промышленной революции. В частности, развитию и распространению платформенных технологий в области совместного потребления также способствуют меры государственной политики (например, льготные условия оплаты парковки для каршеринговых автомобилей).

Проблемам управления рисками государственного управления в цифровой экономике значительное внимание уделяется и в Организации экономического сотрудничества и развития (ОЭСР). Так, в рамках состоявшейся в 2016 г. в Канкуне (Мексика) министерской встречи «Цифровая экономика: инновации, рост и общественное благосостояние» в качестве ключевых рисков цифровой экономики на современном этапе были выделены риски цифровой безопасности и защиты персональных данных. Было констатировано, что цифровая экономика, связанные инновации и развивающиеся технологии дают значительные возможности для экономического роста и социального процветания. Однако для того чтобы этого достичь, цифровая экономика требует эффективной системы управления рисками цифровой безопасности и защиты персональных данных. Тем не менее в настоящее время наблюдается рост числа и сложности угроз и инцидентов в данной области с растущими негативными последствиями для экономики и общества. Государственные и частные организации, включая инфраструктурные, все чаще сталкиваются с нарушениями в работе систем, прямыми финансовыми убытками, ухудшением репутации, снижением доверия и конкурентоспособности. Физические лица также все чаще страдают от несанкционированного доступа, удаления, использования, модификации и раскрытия их персональных данных [17]. Проблемы обеспечения экономической безопасности в контексте цифровизации бизнес-среды поднимаются и российскими авторами [3]. Таким образом, в условиях цифровой экономики, постоянно растущих объемов данных и каналов их обработки и использования стратегическим вызовом для государства становится проблема обеспечения цифровой безопасности, в том числе предотвращения неожиданного или нежелательного использования персональных данных.

В Обзоре цифровой экономики, подготовленном ОЭСР в 2017 г. [18], помимо рассмотренных, отмечаются и другие риски цифровой экономики и порождаемые ими вызовы для системы государственного управления.

Так, по мнению авторов Обзора, развитие цифровой экономики породит не столько массовую безработицу, сколько серьезную трансформацию рынка труда — на смену утраченным рабочим местам и специальностям придут другие, возникнут новые формы занятости. Однако для трансформации рынка труда в рамках безболезненного сценария требуется заблаговременная трансформация системы образования и трудового законодательства. Таким образом, риском можно считать консервативность системы образования и трудового законодательства и их неспособность смягчить негативные последствия цифровизации для рынка труда. Одновременно в Обзоре констатируется, что даже в странах ОЭСР наблюдается дефицит цифровой грамотности, с одной стороны, тормозящий дальнейшее внедрение и повсеместное использование

не только перспективных цифровых технологий, но и цифровых технологий «вчерашнего дня», с другой стороны, снижающий конкурентоспособность значительной части населения на рынке труда.

Риски цифровой безопасности и защиты персональных данных в Обзоре рассматриваются еще более широко — например, с учетом рисков недобросовестного поведения интернет-магазинов по отношению к потребителям и недостаточной защищенности потребителей в таких ситуациях в рамках существующей нормативной базы. Кроме того, экспертами ОЭСР констатируется, что даже в наиболее продвинутых в этом отношении странах существующих мер в области защиты персональных данных недостаточно, что снижает доверие населения к цифровой экономике. Например, около 60% граждан Европейского Союза беспокоит то, что их активность в интернете фиксируется и анализируется в целях создания контекстной рекламы.

В целом же ключевым интегральным риском развития цифровой экономики эксперты ОЭСР считают возрастающую сложность и взаимозависимость технологий, активов, сетей, процессов, цепочек поставок, организационных структур, государств и пр. В результате риски непреднамеренных или преднамеренных сбоев в работе цифровой инфраструктуры или предоставлении цифровых услуг приводят к последствиям, перешагивающим как границы отдельных организаций и целых секторов экономики, так и государственные границы, и в дальнейшем данная тенденция будет только усиливаться. Создание эффективных механизмов регулирования и управления такими рисками на принципах государственно-частного партнерства является ключевой задачей любого национального государства, однако ситуация обостряется постепенным размыванием национальных границ для цифровых технологий и необходимостью международного регулирования на основе консенсуса, который в настоящее время отсутствует.

Отдельные российские эксперты отмечают, что распространение цифровых технологий в образовании требует переосмысления подходов к развитию системы образования в самом широком смысле. С одной стороны, цифровые технологии в образовании позволяют расширить доступ к образовательным услугам, повысить адаптивность образовательных программ и модулей, содействовать эффективной реализации концепции «непрерывного образования». С другой стороны, уже сейчас наблюдаются и определенные негативные последствия цифровизации образования, в том числе формирование у подрастающего поколения так называемого «кликового» и «клипового» сознания. Суть последнего заключается в том, что человек с детства привыкает простым нажатием кнопки (click) получать информацию в концентрированном виде (clip), однако при этом у него не вырабатываются навыки по ее анализу, следствием чего является утрата творческих начал [2].

Кроме того, неконтролируемый доступ к виртуальному пространству может привести к утрате человеком грани между действительностью и фантазиями, формированию не соответствующих действительности представлений об окружающем мире. Более того, расширение функционала и повышение доступности устройств на основе цифровых технологий, помимо безусловных преимуществ, таит в себе серьезные угрозы примитивизации насе-

ления и массового распространения аддикций, в том числе болезненную зависимость от различных аудиовизуальных и иных раздражителей, включая социальные сети и другие интернет-ресурсы, бесконечное прослушивание музыки в наушниках и пр., и сопутствующих им девиаций. Ограничение такого рода негативных влияний на человеческий капитал является значимым вызовом для системы государственного управления.

Выводы и следствия

Цифровизация экономики кардинально меняет модель экономического роста, что, в свою очередь, требует от государства принципиально новых подходов к регулированию экономики [22]. В свою очередь, несмотря на то что цифровизация рассматривается как одно из ключевых средств повышения качества государственных услуг, на практике имеют место примеры, когда недостаточно продуманная цифровизация приводит, по мнению потребителей государственных услуг, к снижению их качества [13]. В числе ключевых причин снижения качества предоставления отдельных государственных услуг в результате цифровизации отмечаются, в частности, недостаток цифровых компетенций как у сотрудников государственного аппарата, так и у потребителей государственных услуг, неразвитость цифровой инфраструктуры и неполное покрытие ею территории страны, отсутствие у потребителей необходимых технических средств для получения услуг в цифровой форме, культурно-психологические аспекты [19].

Некоторыми экспертами справедливо отмечается, что одной из базовых проблем государственного регулирования развития цифровой экономики в нашей стране можно считать отсутствие достоверной и точной статистической информации о реальном положении дел [8]. В этой связи уместно говорить о том, что одним из немаловажных направлений государственного регулирования в контексте развития цифровой экономики становятся ее мониторинг и оценка ее вклада в экономический рост, что требует включения в статистический инструментарий новых, цифровых, товаров и услуг, актуализации статистических классификаторов и методологических подходов и источников статистических данных, разработки адекватных подходов к оценке «цифрового вклада» в производство и потребление [12].

Среди ключевых (первоочередных) направлений государственного регулирования в части управления рисками развития цифровой экономики, разделяя позицию Натальи Касперской [10], представляется целесообразным выделить следующие.

Первое — внедрение в систему государственного управления идеологии и практики опережающего регулирования, то есть регулирования, упреждающего возникновение проблем. В качестве яркого негативного примера в данном случае можно привести регулирование интернета и связанных с ним видов деятельности, когда национальная и международная регуляторная база начали развиваться значительно позже (на 10–15 лет) начала массового влияния интернета на жизни миллионов людей по всему миру.

Второе — апробация и тиражирование инструмента «регуляторных песочниц», то есть пилотных территорий или видов деятельности, где разрешается

условно нерегулируемое (без правовой ответственности) развитие и внедрение новых технологий, происходящее под пристальным наблюдением регуляторов с целью более объективной оценки возникающих возможностей, проблем и рисков. Применительно к цифровой экономике «регуляторные песочницы» особенно актуальны в области беспилотного транспорта, технологий анализа Больших данных, финансовых технологий.

Третье — разработка и внедрение в систему государственного управления эффективных механизмов обратной связи, когда проблемы и риски, возникающие в связи с развитием новых технологий, приводят к быстрому изменению регулирования, его постоянной «точной настройке».

Крайне актуальной представляется и всесторонняя поддержка импортозамещения, направленная на обеспечение цифрового суверенитета — как за счет бюджетных инвестиций и стимулирования частных инвестиций в развитие собственных цифровых технологий, так и за счет ограничения доступа иностранных поставщиков в критически важные сектора, в том числе в рамках публичных закупок. Необходимым условием эффективной реализации данного направления государственной политики применительно к России следует считать более четкое и аргументированное определение, где и до какой степени процесс цифровизации может быть основан на импорте цифровых технологий, а где (в том числе из соображений национальной безопасности) критически важно развивать именно собственные российские технологии, на разработке которых и должны быть сконцентрированы ограниченные ресурсы.

Библиографический список

1. Быков А.А. О рисках цифровой экономики // Проблемы анализа риска. — 2017. — № 6. — Т. 14. — С. 4–5.
2. Иванов В.В., Малинецкий Г.Г. Цифровая экономика: мифы, реальность, перспектива. — М.: РАН, 2017.
3. Карев А.В., Нижегородцев Р.М. Формирование цифровой бизнес-среды и вопросы экономической безопасности // Менеджмент и бизнес-администрирование. — 2018. — № 1. — С. 113–119.
4. Корчагин С.А., Польщиков Б.П. Цифровая экономика и трансформация механизмов государственного управления // Свободная мысль. — 2018. — № 1. — С. 23–36.
5. Ленчук Е.Б., Власкин Г.А. Формирование цифровой экономики в России: проблемы, риски, перспективы // Вестник ИЭ РАН. — 2018. — № 5. — С. 9–21.
6. Махалин В.Н., Махалина О.М. Управление вызовами и угрозами в цифровой экономике России // Управление. — 2018. — № 2 (20). — С. 57–60.
7. Петров М. и др. Государство как платформа. Государство для цифровой экономики. Цифровая трансформация. — М.: ЦСР, 2018.
8. Смотрицкая И.И. Государственное управление в условиях развития цифровой экономики: стратегические вызовы и риски // ЭТАП: экономическая теория, анализ, практика. — 2018. — № 4. — С. 60–72.
9. Смотрицкая И.И., Черных С.И. Современные тенденции цифровой трансформации государственного управления // Вестник ИЭ РАН. — 2018. — № 5. — С. 22–36.

10. Шадрина Т. Обогнать, не догоняя. Наталья Касперская: Как России сохранить цифровой суверенитет // Российская газета — Столичный выпуск № 47 (7510) от 04.03.2018.
11. Якутин Ю.В. Стартовые социально-экономические условия реализации правительственной программы «Цифровая экономика Российской Федерации» // Менеджмент и бизнес-администрирование. — 2018. — № 1 — С. 35–68.
12. Barefoot K. et al. Defining and Measuring the Digital Economy. BEA Working Paper 3/15/2018.
13. Berger J.B., Hertzum M., Schreiber T. Does local government staff perceive digital communication with citizens as improved service? // Government Information Quarterly. — 2016. — Vol. 33. — P. 258–269.
14. Bordo M.D., Levin A.T. Central Bank Digital Currency and the Future of Monetary Policy. NBER Working Paper 23711.
15. Colin N. et al. The Digital Economy // Notes du conseil d'analyse économique. — 2015. — Vol. 7. — № 26. — P. 1–12.
16. Janowski T. Digital government evolution: From transformation to contextualization // Government Information Quarterly. — 2015. — Vol. 32. — Issue 3. — P. 221–236.
17. OECD 2016 Ministerial Meeting. The Digital Economy: Innovation, Growth, and Social Prosperity. Panel 3.2. Managing Digital Security and Privacy Risk for Economic and Social Prosperity.
18. OECD Digital Economy Outlook 2017. Paris: OECD Publishing, 2017.
19. O'Sullivan S., Walker Ch. From the interpersonal to the internet: social service digitization and the implications for vulnerable individuals and communities // Australian Journal of Political Science. — 2018. — Vol. 53. — № 4. — P. 1–18.
20. Savage N. Making digital government a better government // Nature. — 2018. — Vol. 563. — P. S136–S137.
21. The Global Risks Report 2017. 12th Edition. Geneva: World Economic Forum, 2017.
22. Watanabe Ch. et al. Consequences of the Digital Economy: Transformation of the Growth Concept // International Journal of Managing Information Technology. — 2018. — Vol. 10. — № 2. — P. 21–39.