

5/22

ПРЕПРИНТЫ

**ЦИФРОВОЕ ОБЩЕСТВО
И ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ. ИННОВАЦИИ
DIGITAL SOCIETY AND
INFORMATION TECHNOLOGIES
INNOVATIONS**

**ЦИФРОВОЕ ОБЩЕСТВО
И ИНФОРМАЦИОННЫЕ
ТЕХНОЛОГИИ. ИННОВАЦИИ
DIGITAL SOCIETY AND
INFORMATION TECHNOLOGIES
INNOVATIONS**

А. Д. Левашенко, А. А. Коваль

**ПОДХОДЫ К УСТРАНЕНИЮ
ПРАВОВЫХ БАРЬЕРОВ В ОБЛАСТИ
РЕГУЛИРОВАНИЯ ОБОРОТА ДАННЫХ,
ТЕХНОЛОГИЙ И ОНЛАЙН-ПЛАТФОРМ
ДЛЯ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ
В РОССИИ**

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ»

JEL K31

Левашенко А.Д., Коваль А.А.

**Подходы к устранению правовых барьеров в области
регулирования оборота данных, технологий
и онлайн-платформ для развития цифровой
экономики в России**

Москва 2022

FEDERAL STATE BUDGETARY EDUCATIONAL
INSTITUTION OF HIGHER EDUCATION
«RUSSIAN PRESIDENTIAL ACADEMY OF NATIONAL ECONOMY
AND PUBLIC ADMINISTRATION»

JEL K23

A.Levashenko, A.Koval

**Approaches to the elimination of legal barriers in the field
of regulation of data flows, technologies and online
platforms for the development of the digital economy
in Russia**

Moscow 2022

Аннотация. Предметом исследования являются правоотношения в области регулирования оборота данных; использования прорывных цифровых технологий (например, блокчейн, Интернет вещей, Искусственный интеллект и др.), развития платформенной экономики, развития цифрового взаимодействия между субъектами экономики.

Актуальность исследования обусловлена тем, что в России реализуется федеральный проект «Нормативное регулирование цифровой среды», который предусматривает разработку и принятие ряда нормативно-правовых актов, направленных на снятие первоочередных барьеров, препятствующих развитию цифровой экономики в таких сферах как: гражданский оборот, финансовые технологии, интеллектуальная собственность, телекоммуникации, судопроизводство и нотариат, стандартизация и др. Вместе с тем, проект не ставит амбициозных задач по устранению существующих барьеров в области регулирования данных, являющихся основой для цифровизации экономики, которые связаны, например, с применяемым тотальным требованием локализации данных и бинарным подходом к определению персональных данных; задач по созданию правовых условий для широкомасштабного внедрения прорывных цифровых технологий с учетом новых регуляторных требований (например, в отношении функционирования систем искусственного интеллекта) и лидерства России с точки зрения развития платформенной экономики. Без решения этих задач невозможно обеспечить цифровую трансформацию российской экономики.

Новизна исследования в том, что в рамках исследования решаются задачи создания в России системы регулирования цифровой экономики, учитывающей последние рекомендации в данной области и актуальные вызовы.

Цель исследования заключается в формировании предложений, направленных на устранение правовых барьеров в области регулирования оборота данных; использования прорывных цифровых технологий (например, блокчейн, Интернет вещей, Искусственный интеллект и др.), развития платформенной экономики, развития возможности цифрового взаимодействия между субъектами экономики.

Методология исследования основана на применении методов логического, системного и сравнительного анализа с использованием российских и зарубежных нормативно-правовых актов, аналитических материалов компетентных авторов и международных организаций.

Для достижения поставленной цели предполагается решение следующих **задач**:

- проведение анализа влияния правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ на создание условий для цифровой трансформации экономики.
- проведение анализа стандартов ОЭСР в области регулирования оборота данных, использования прорывных цифровых технологий (например, блокчейн, Интернет вещей, Искусственный интеллект и др.), развития платформенной экономики, развития возможности цифрового взаимодействия субъектами экономики.
- проведение анализа подходов государств-членов ОЭСР в области устранения правовых барьеров для цифровой трансформации экономики.
- формирование предложений по устранению правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ, препятствующих цифровой трансформации российской экономики, в т.ч. в условиях применения экономических мер ограничительного характера в отношении России, а также ответных мер, которые могут создавать риски для развития цифровой экономики.

Результатами исследования стала разработка предложений для по устранению правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ, препятствующих цифровой трансформации российской экономики.

Перспектива исследования состоит в необходимости совершенствования российского законодательства в части регулирования цифровой экономики.

Данная работа подготовлена на основе материалов научно-исследовательской работы, выполненной в соответствии с Государственным заданием РАНХиГС при Президенте Российской Федерации на 2022.

Ключевые слова: цифровая экономика, правовые барьеры, регулирование оборота данных, передача данных, прорывные технологии, блокчейн, искусственный интеллект, интернет вещей, цифровизация

Левашенко Антонина Давидовна – старший научный сотрудник, руководитель Российского центра компетенций и анализа стандартов ОЭСР РАНХиГС при Президенте РФ; 119571, Москва, Россия; +7 (916) 932 60 81, antonina.lev@gmail.com; ORCID: 0000-0003-2029-3667

Коваль Александра Александровна – научный сотрудник Центра Россия-ОЭСР Российской академии народного хозяйства и государственной службы при Президенте РФ, koval-aa@ranepa.ru, ORCID : 0000-0002-0431-1725

JEL Classification: K31

Abstract. The subject of the research work is legal relations in the fields of regulation of data circulation; of the use of disruptive digital technologies (for example, blockchain, the internet of things, artificial intelligence, etc.), of the development of the platform economy, of the development of digital interaction between economic entities.

The relevance of the study is prompted by the implementation of the federal project “Legal regulation of the digital environment”, which provides for the development and adoption of several legal acts aimed at removing the primary barriers against development of the digital economy in such areas as civil circulation, financial technologies, intellectual property, telecommunications, legal proceedings and notaries, standardization, etc. At the same time the project does not set the ambitious goals to remove the existing barriers in the field of the data regulation, which drive the digitalization of the economy, and which are related to, for example, the requirement for total data localization and to the binary approach to the definition of personal data, to create legal conditions for the large-scale implementation of breakthrough digital technologies, with regard to new regulatory requirements (for example, the functioning of artificial intelligence systems) and Russia's leadership in the development of the platform economy. Without solving these problems, it is impossible to ensure the digital transformation of the Russian economy.

The novelty of the study is in that it suggests solutions to the tasks of creating a digital economy regulation system in Russia that consider the latest recommendations in this area and current challenges.

The objective of the research work is to form proposals for eliminating legal barriers in the regulation of data circulation; the use of breakthrough digital technologies (for example, blockchain, the Internet of things, artificial intelligence, etc.), the development of platform economy, the development of digital interaction between economic entities.

The research methodology includes methods of logical, systemic, and comparative analysis using Russian and foreign legal acts, and analytical materials of competent authors and international organizations.

To achieve the objective, the following tasks are to be solved:

- analysis of the impact of legal barriers in the regulation of data circulation, the use of digital technologies, and the operation of digital platforms on creating conditions for digital transformation of the economy.
- analysis of the OECD standards for data circulation regulation, use of breakthrough digital technologies (for example, blockchain, internet of things, artificial intelligence, etc.), development of the platform economy, and development of digital interaction between economic entities.
- analysis of the approaches of the OECD member states to the task of removing legal barriers to the digital transformation of the economy.
- proposals for the elimination of legal barriers in the regulation of data circulation, the use of digital technologies, and the operation of digital platforms that impede the digital transformation of the Russian economy, also in the context of the application of restrictive economic measures against Russia, as well as retaliatory measures that may create risks for the development of the digital economy.

The research resulted in the development of proposals for the elimination of legal barriers in the circulation regulation, the use of digital technologies, and the operation of digital platforms that impede the digital transformation of the Russian economy.

The contribution of the study is prompted by the need to improve Russian legislation on the digital economy.

This work has been prepared based on the materials of the research work carried out under the State task of the RANEPa at the President of the Russian Federation for 2022.

Keywords: digital economy, legal barriers, regulation of data circulation, data transfer, breakthrough technologies, blockchain, artificial intelligence, internet of things, digitalization

Levashenko A. – Senior Researcher, Head of the Russia-OECD Centre, RANEPА; 119571, Moscow, Russia; +7 (916) 932 60 81, antonina.lev@gmail.com; ORCID: 0000-0003-2029-3667

Koval A. –Researcher, Russia-OECD Centre, RANEPА ПФ, koval-aa@ranepa.ru, ORCID : 0000-0002-0431-1725

JEL Classification: K31

Содержание

Введение	8
1. Анализ влияния правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ на создание условий для цифровой трансформации экономики	10
2. Анализ стандартов ОЭСР в области регулирования оборота данных, использования прорывных цифровых технологий, развития платформенной экономики, развития возможности цифрового взаимодействия субъектами экономики.....	11
3. Анализ подходов государств-членов ОЭСР в области устранения правовых барьеров для цифровой трансформации экономики.....	17
4. Предложения по устранению правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ, препятствующих цифровой трансформации российской экономики	22
Заключение.....	33
Благодарности.....	36
Список использованных источников.....	37

Введение

Мировая цифровая экономика переживает стремительный рост с развитием прорывных информационных технологий следующего поколения. В 2020 году добавленная стоимость цифровой экономики составила 32,6 трлн долларов США в 47 крупнейших экономиках мира, включая Россию. Чтобы стимулировать развитие цифровой экономики, страны принимают разные стратегии. Например, страны ЕС разрабатывают правила управления данными и разработали единый цифровой рынок для создания экосистемы цифровой экономики. Опираясь на прочную промышленную основу и жизнеспособность рынка, Китай продвигает строительство инфраструктуры и интеграцию цифровой экономики с реальной экономикой, ускоряя как социальное, так и экономическое развитие.

Однако для реализации экономического потенциала цифровых решений в масштабе страны необходимо обеспечить благоприятные правовые условия для применения регуляторных решений в области цифровой экономики. Поэтому актуальная задача для развития цифровой экономики – это выявление правовых барьеров в области регулирования оборота данных, внедрения цифровых технологий, составляющих три столпа цифровой экономики, и платформ.

Формирование сильной цифровой экономики сегодня стоит в повестке национального развития. В России реализуется федеральный проект «Нормативное регулирование цифровой среды». Проект предусматривает обеспечение разработки, а также принятия ряда правовых актов, которые направлены на снятие первоочередных барьеров, препятствующих развитию цифровой экономики в таких сферах, как: гражданский оборот, финансовые технологии, интеллектуальная собственность, телекоммуникации, судопроизводство и нотариат, стандартизация и др. Однако проект не ставит целей по устранению существующих барьеров в области регулирования данных, препятствующих формированию рынка данных, барьеров в области регулирования оборота данных выделяются барьеры в области цифровых технологий. Такие барьеры прежде всего связаны с отсутствием качественного регулирования электронного документооборота как на уровне публично-частных взаимодействий, так и внутри частного сектора. Например, отсутствует система гармонизации правил и стандартов электронного документооборота, которая бы позволила повысить интероперабельность систем различных субъектов. Организация электронного документооборота среди компаний включает в том числе вопрос возможности заключения сделок в электронном формате или наделения актов юридической силой. Поэтому сегодня многие страны обеспечивают регулирование цифровой подписи и другие системы идентификации и аутентификации субъектов.

Экономический анализ регуляторных ограничений позволяет вычислить экономический эквивалент негативного воздействия инструментов. Уже сегодня ученые демонстрируют негативный эффект действия законов о локализации, например, по критерию снижения ВВП - Бразилия (-0,2% ВВП, -4,2% инвестиции); Китай (-1,1% ВВП; -1,8% инвестиции); РФ (-0,3% ВВП; -1,4% инвестиции); ЕС (-0,4% ВВП, -3,9% инвестиции). Однако характеристика непосредственно негативного воздействия национальных ограничений на оборот данных индивидуальна для каждой страны.

1. Анализ влияния правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ на создание условий для цифровой трансформации экономики

По оценкам международных экспертов, нивелирование правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ входит в число основных условий для цифровой трансформации экономики.

Ключевое значение регулирование приобретает для создания экономики, основанной на данных. Сегодня свободная передача данных является значительным фактором роста и развития стран и различных секторов экономики.

При этом ограничения на трансграничную передачу данных влияют на глобальную экономику и экономику отдельных стран. Исследователи сообщают, что увеличение количества барьеров негативно сказывается на развитии экономики. Фонд международных технологий и инноваций (International Technology & Innovation Foundation, ITIF) составил индекс для оценки связанности между отраслями переработки и сбыта и национальными ограничениями доступа к данным (the data restrictiveness linkage – DRL) по критерию интенсивности передачи данных в этих отраслях. ITIF, базируясь на отчетах ОЭСР, утверждает, что увеличение на 1 пункт уровня ограничения данных в стране сокращает ее валовую торговлю на 7%, снижает производительность труда на 2,9% и повышает минимальные цены на 1,5% в промежутке пяти лет.

Ограничения на трансграничную электронную торговлю влияют на глобальную экономику и экономику отдельных стран. В цифровую эпоху размываются различия между товарами и услугами, а также процесс пересечения ими границ. При этом барьеры, воздействующие на поток товаров, услуг или информации, могут иметь значительные последствия для цифровой торговли. Правовая неопределенность и дополнительные затраты на соблюдение требований, связанные с различными режимами регулирования, могут снизить мотивацию компаний для выхода на новые рынки. Кроме того, поскольку информация и данные являются сырьем для цифровой экономики, необходим сбалансированный нормативный подход к трансграничным потокам данных с целью обеспечения возможности получения выгод от цифровой торговли при одновременном обеспечении достижения законных целей государственной политики. Разрозненные подходы к этим вопросам могут привести к издержкам для фирм, работающим в разных юрисдикциях. Трансграничные потоки данных способствуют повышению динамичности бизнеса и экономическому росту.

2. Анализ стандартов ОЭСР в области регулирования оборота данных, использования прорывных цифровых технологий, развития платформенной экономики, развития возможности цифрового взаимодействия субъектами экономики

Организация экономического сотрудничества и развития выступает флагманом в области разработки международно признанных стандартов по регулированию оборота данных и других сфер цифровой экономики. Работа ОЭСР изначально адресована широкому кругу стран и потому сохраняет свою актуальность независимо от вовлечения конкретной страны в текущую работу организации. Более того, благодаря международной ориентированности стандарты ОЭСР в определенной мере отвечают тематической повестке на других международных площадках. Поэтому стандарты ОЭСР хорошо исследовать в том числе в сопоставлении с аналогичными стандартами, разработанными на иных площадках, как ООН, Международный Союз Электросвязи, Международная организация стандартизации, и др. В рамках настоящего исследования рассматриваемые рекомендации ОЭСР анализируются с точки зрения возможностей их имплементации в России с учетом актуальной правовой среды и программных задач.

Стандарты ОЭСР по развитию регулирования оборота данных. Международные эксперты разработали Рекомендацию ОЭСР по улучшению доступа к данным и обмену ими (OECD Recommendation on Enhancing Access to and Sharing of Data, EASD – далее: Рекомендация EASD). Рекомендация была принята в октябре 2021 г. Юристы во многих странах высоко оценивают принятие такой рекомендации, как первого согласованного на международном уровне инструмента по повышению доступности данных. Примечателен широкий предметный охват Рекомендации: принципы повышения доступности данных применимы для многих категорий данных, в том числе персональных, неперсональных, открытых, служебных, публичных и частных – в различных отраслях. Структурно документ включает семь основных рекомендаций.

Во-первых, для развития оборота и доступности данных необходимо прежде всего укреплять доверие к надежности систем данных. Вопрос надежности становится тем более актуальным, чем более открытыми становятся данные, а соответственно, и более подверженными рискам информационной безопасности.

Во-вторых, необходимо придерживаться системного подхода к вопросам обеспечения доступа к данным на всех уровнях и областях управления. В зарубежных исследованиях соответствующий подход определяется как стратегический и системный («strategic whole-

of-government approach»). Такой подход означает выработку единых принципов в управлении данными, применимых на всех уровнях управления во всех аспектах.

В-третьих, необходимо обеспечить баланс между мерами облегчения доступа к данным и мерами защиты публичных и частных прав, связанных с этими данными.

В-четвертых, повышение доступности данных должно происходить в справедливых и конкурентных условиях цифровой экономики. Это значит, что перед регуляторами стоит задача предупреждения практик манипулирования данными со стороны цифровых компаний для получения большей доли на рынке тех или иных цифровых услуг.

В-пятых, не должно проводиться различий по правовому режиму данных в зависимости от юрисдикции расположения пользователя, владельца информационной системы, серверов облачного провайдера и т.д. Доступ к данным должен быть трансграничным. Это значит, что если даже государства используют меры ограничения трансграничного оборота данных (например, в случае требований локализации данных, как в России, Китае), то такие меры должны быть соразмерны целям их введения.

В-шестых, доступность данных должна обеспечиваться не только с юридической точки зрения, но также в технологическом аспекте. Это значит, что данные должны быть доступными благодаря унифицированным форматам передачи данных, благодаря доступным технологиям и ИКТ-инфраструктуре.

В-седьмых, для эффективного использования открытых данных соответствующими цифровыми навыками должны обладать сами участники оборота данных. Таким образом, международные эксперты указывают на необходимость цифрового образования населения и содействия повышению квалификации ИКТ-специалистов, работающих в сферах данных.

Все семь рекомендаций являются взаимосвязанными. Это значит, что государствам необходимо принимать шаги по всем семи направлениям, чтобы обеспечить системное развитие доступности данных.

Стандарты ОЭСР по развитию регулирования технологии блокчейн. Стандарты Организации предусматривают необходимость внедрения следующих принципов:

1. Приверженность и соответствие. Положение данной рекомендации указывает, что все лица, создающие решения с применением технологии блокчейн, должны учитывать действующее законодательство, в том числе и в ситуациях, когда создаются «более» децентрализованные приложения.

2. Управление, прозрачность и подотчетность.

3. Интероперабельность

4. Цифровая безопасность и конфиденциальность данных. Положение данной рекомендации закладывает ключевой принцип ОЭСР в отношении хранения персональных данных на блокчейн – следует хранить только те персональные данные в блокчейне, которые остро необходимы для его корректной работы. Такой подход объясняется свойствами технологии, в том числе невозможностью удаления информации или ее изменение.

5. Образование и развитие навыков. Данная рекомендация предусматривает необходимость проведения консультаций с заинтересованными сторонами по вопросам работы блокчейн платформы.

Таким образом, 5 рекомендаций в отношении применения технологии блокчейн определяют базовые правила для компаний. Несмотря на то, что рекомендация является верхнеуровневой, в ней заложено ряд существенных требований для разработчиков, в том числе в части соответствия децентрализованных решений национальному законодательству стран, необходимости проведения внешнего аудита, порядка и объема хранения персональных данных.

Стандарты ОЭСР по развитию регулирования технологии Интернета вещей: цифровая безопасность IoT и др. Интернет вещей (Internet of Things, IoT) представляет собой экосистему, сеть передачи данных между физическими объектами, оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой. В Интернете вещей устройства и объекты имеют либо прямое подключение к Интернету, либо опосредованное через локальные или глобальные сети. Согласно определению, данному ОЭСР, Интернет вещей включает в себя все устройства и объекты, состояние которых может быть изменено через Интернет как с активным участием человека, так и без него.

Повсеместное внедрение Интернета вещей в жизнь людей потребует оценки последствий для их безопасности и конфиденциальности данных, включая безопасность их личной информации, выработку и принятие соответствующих мер. Правовые рамки конфиденциальности и защиты прав пользователей станут основными факторами признания Интернета вещей и доверия к нему. Помимо этого, Интернет вещей будет оказывать влияние на коммуникационные инфраструктуры и услуги. Поэтому для управления Интернетом вещей необходимо выработать политику, способствующую доступности, качеству и использованию таких инфраструктур и услуг. В связи с этим, возможно, потребуется пересмотреть международное управление и нормы, чтобы обеспечить производительность и безопасность коммуникационных сетей и услуг и, таким образом, способствовать укреплению доверия к Интернету вещей.

Разработанная ОЭСР Рекомендация по безопасности цифровых продуктов направлена на выявление и уменьшение рисков цифровой безопасности, связанных с рынком Интернета вещей. Риск цифровой безопасности — это категория риска, связанная с использованием, развитием и управлением цифровой средой в ходе любой социально-экономической деятельности. Уровень риска цифровой безопасности зависит от нескольких факторов, к которым относятся уровень цифровой безопасности продукта и контекст его использования. Риск цифровой безопасности возникает в результате сочетания угроз и уязвимостей, что приводит к инцидентам, влияющим на конфиденциальность, целостность и доступность данных, продуктов или сетей. Инциденты цифровой безопасности имеют технические последствия, которые могут привести к экономическим и социальным последствиям.

Стандарты ОЭСР по развитию регулирования Искусственного интеллекта. Как отмечает ОЭСР, использование искусственного интеллекта значительно влияет на экономическое развитие стран, создает возможности для роста производительности и повышения качества жизни людей. Вместе с тем существуют проблемы, связанные с этикой использования систем ИИ, защитой прав и законных интересов населения, в том числе в сфере защиты персональных данных, конкуренции, прав потребителей, распределения ответственности за действия систем ИИ и т.д., в следствие чего существует необходимость в правовом регулировании такого использования. Также, для успешного внедрения и развития систем искусственного интеллекта необходимо регулирование защиты и обеспечения качества данных, режима открытых данных, в том числе данных государственного и банковского сектора. ОЭСР в 2019 г. приняла Рекомендацию по искусственному интеллекту, на её основе в том же году G20 разработаны Принципы искусственного интеллекта. Рекомендация ОЭСР представляет собой правовой инструмент, которым устанавливаются основные принципы ответственного управления системами искусственного интеллекта:

1) Инклюзивный рост, устойчивое развитие и благополучие. Данный принцип означает, прежде всего, недопустимость дискриминации в принимаемых системами ИИ решениях;

2) Справедливость и человекоцентричность. Данный принцип предполагает уважение верховенства права, прав человека и демократических ценностей, а также внедрение в системы ИИ соответствующих механизмов и мер предосторожности.;

3) Прозрачность и объяснимость. Данный принцип включает в себя принятие общих норм, определяющих понятие систем ИИ, доведение до заинтересованных лиц сведений об их взаимодействии с ИИ, сведений о последствиях (результатах) такого взаимодействия и создание возможности для лиц, на которых негативно повлияла работа ИИ, обжаловать результаты такой работы.

4) Устойчивость и безопасность. Системы ИИ должны быть устойчивыми и безопасными на протяжении всего жизненного цикла, для обеспечения их нормального функционирования как при нормальной эксплуатации, так и в случае неправильной эксплуатации;

5) Надежность. Каждое лицо, вовлеченное в создание и обеспечение функционирования систем ИИ, должно обеспечивать их должное функционирование в соответствии с перечисленными выше принципами. Данный принцип предполагает принятие компаниями организационных и иных мер, направленных на системное внедрение перечисленных выше принципов, например, за счет внедрения международных стандартов, таких как стандарт ISO/IEC TR 24028:2020.

Стандарты ОЭСР по развитию цифровых платформ. Чистая прибыль ведущих цифровых платформ в США в 2020 году достигла 192,4 млрд долларов США, увеличившись на 21,1% по сравнению с 2019 годом. Рост крупных технологических компаний, таких как Google, Amazon, Apple, Microsoft и Facebook вызывает ряд вопросов, связанных с потенциальным экономическим ущербом, вызванным размером таких платформ, в частности, важно рассмотреть проблемы конкуренции платформ с учетом размера сетевых эффектов, которые создают такие платформы, а также риски применения платформами антиконкурентных практик и практик, которые могут вводить в заблуждение или обманывать потребителей.

Онлайн-платформы стимулируют развитие трансграничной торговли, в рамках которой нередко происходят нарушения прав потребителей. По оценкам Европейской комиссии, ущерб, причиняемый потребителям несоблюдением основных потребительских правил ЕС на некоторых трансграничных онлайн-рынках, а также неэффективным трансграничным правоприменением, составляет 770 миллионов евро в год. Примерно от 1 до 3% онлайн-транзакций приводят к возникновению потребительских споров (данные ОЭСР).

В части защиты прав потребителей на цифровых платформах, важным является вопрос регулирования продажи цифровых продуктов, а также связанных вопросов доставки, послепродажного обслуживания и пр. Основным инструментарием ОЭСР является Руководство ОЭСР по защите прав потребителей в электронной коммерции 2016 г. Для цифровых продуктов в 2014 г. ОЭСР было выпущено «Руководство по потребительской политике в отношении нематериальных продуктов цифрового контента». К нематериальным продуктам цифрового контента относятся продукты, которые приобретаются на интернет-платформах и в мобильных сетях, либо в электронном формате (например, загруженное платное приложение), либо приобретается потребителями у предприятий через электронную коммерцию (т. е. когда подтверждение заказов на продукцию осуществляется в электронном виде). К таким товарам относятся СМИ и развлечения (фильмы, музыка, игры, предметы

виртуального мира, электронные книги, журналы, журналы, изображения, новости и пр.), приложения и услуги персонализации / дополнения, включая рингтоны и заставки.

Важным аспектом защиты прав потребителей является возможность отзыва товаров, то есть выведения из продаж товаров, которые были признаны небезопасными, в том числе изъятие таких товаров у потребителей. Роль онлайн - платформ заключается в обеспечении того, чтобы отозванные продукты не были доступны для продажи через их канал. По данным портала ОЭСР Global Recalls, наибольшее количество отзывов происходит в отношении игрушек, автомобилей, и электротоваров, одежды и спортивного инвентаря – 70% отзывов каждый год.

Стандарты ОЭСР по развитию возможности цифрового взаимодействия субъектами экономики. ОЭСР рекомендует странам развивать регуляторные инструменты и продвигать следующие меры для достижения компаниями цифровой зрелости в части электронного взаимодействия с налоговыми органами:

- 1) Создание цифровых идентификаторов и возможностей для получения услуг в цифровом виде;
- 2) Использование цифровых идентификаторов в рамках налогового администрирования;
- 3) Развитие цифровых сервисов в «точках соприкосновения» компаний с органами власти;
- 4) Обеспечение доступности данных частного и государственного сектора для обмена между компаниями и органами власти и стандартов таких данных;
- 5) Обеспечение безопасности и приватности таких данных;
- 6) Развитие регулирования в сфере налогообложения с учетом цифровизации отношений бизнеса и власти;
- 7) Развитие навыков, связанных с цифровизацией налогового администрирования в компаниях и в органах власти;
- 8) Формирование стратегий цифрового налогового управления в странах.

3. Анализ подходов государств-членов ОЭСР в области устранения правовых барьеров для цифровой трансформации экономики

Стандарты государств-членов ОЭСР по развитию регулирования оборота данных. Рекомендации ОЭСР по регулированию оборота данных уже в той или иной мере реализуются во многих странах с помощью различных инструментов регулирования оборота данных. Эксперты ОЭСР в отчёте о возможностях повышения доступа к данным и передаче данных выделяют несколько видов инструментов:

1) руководства и руководящие принципы по формированию договоров в области управления и передачи данных (contract guidelines and principles). Так, в 2018 г. Министерство экономики, торговли и промышленности Японии разработало Руководство по контрактам об использовании ИИ и данных. Руководство выделяет вопросы и факторы, которые сторонам следует учитывать при составлении контракта, связанного с повторным использованием данных или разработкой и использованием программного обеспечения на основе ИИ; разъясняются основные понятия; даются комментарии по правам и обязанностям сторон.

2) разработка подходов к управлению неперсональными данными (non-personal data). Например, в 2016 г. Еврокомиссией были разработаны стандарты обращения с данными в области сельского хозяйства.

3) создание партнерств по обмену данными. Инструмент партнерств в области данных в частном секторе и/или между частным и государственным секторами по большей части опирается на концепцию открытого доступа к данным государственного сектора. Например, в Чили правительство заключило академические соглашения об открытых данных с академическими и исследовательскими учреждениями для повторного использования данных в открытом формате.

4) создание систем сертификации платформ обмена данными (certification systems for data-sharing platforms). Например, в Японии для поддержки компаний, готовых делиться своими данными, разработана система сертификации платформ обмена данными.

5) определение категории данных для публичного интереса. Например, Австралия в настоящий момент рассматривает возможность создания основ для определения наборов данных, представляющих национальный интерес.

б) законодательное закрепление правового статуса новых участников обмена данными, выступающих в качестве третьих сторон в договорных отношениях по обмену данными. Например, в США законодательно закреплена деятельность информационных брокеров в нескольких штатах.

7) создание публичных институтов укрепления режима персональных данных. В Китае, где установлено строгое публичное регулирование сферы персональных данных, был создан Национальный центр управления данными. Цель проекта в гармонизации управления данными на различных уровнях и создании эффективного управления в отдельных отраслях, таких как кредитование, транспорт, медицина и др.

Стандарты государств-членов ОЭСР по развитию регулирования технологии блокчейн. Среди зарубежных государств активные меры, направленные на развитие технологии блокчейн, приняты в таких странах, как Италия, США, Австралия и др. Так, например, в Италии принято законодательство, направленное на введение законодательного определения блокчейна и смарт-контрактов.

Стратегия блокчейн федерального правительства Германии была опубликована в сентябре 2019 г. Это целостная стратегия, направленная на использование возможностей технологии блокчейн и мобилизацию смежных областей. Помимо конкретных мер, в стратегии изложены десять принципов, которыми руководствуется федеральное правительство в своих действиях. К этим принципам относятся: продвижение инноваций, стимулирование инвестиций, обеспечение стабильности, укрепление устойчивости, создание условий для честной конкуренции, углубление единого цифрового рынка, расширение международного сотрудничества (тесное сотрудничество с европейскими партнерами, Европейской комиссией и другими международными органами, такими как ОЭСР в области технологии блокчейн), интеграция заинтересованных сторон, обеспечение безопасности ИТ и защиты данных, а также создание условий для адаптации.

Китай также демонстрирует колоссальное вовлечение в «гонку разработки блокчейн», подтверждая статус одной из ключевых стран в развитии этой области. КНР принимает новые законы, определяет стандарты работы с блокчейном в промышленных и иных областях. Примечательно, что Китай развивает централизованные структуры блокчейна, когда существует контролирующее лицо или несколько регуляторов, которые называются Alliance Chain или Private Chain. Власти верят в огромную роль блокчейна и прикладывают значительные усилия для его развития в стране.

Стандарты государств-членов ОЭСР по развитию регулирования технологии Интернета вещей. Среди зарубежных государств активные меры, направленные на разви-

тие регулирования технологии Интернета вещей, приняты в США, государствах-членах Европейского союза и др. В США в 2020 г. был принят Закон об улучшении кибербезопасности Интернета вещей (IoT). Основной целью данного закона является создание нормативной базы для разработки специальных мер и руководств для обеспечения безопасности использования устройств Интернета вещей в органах власти США. Национальному институту стандартов и технологий было поручено разработать руководство для федеральных агентств по надлежащему использованию и управлению устройствами Интернета вещей, подключенных к информационным системам.

Министерство промышленности и информационных технологий Китая 25 октября 2021 года выпустило руководство по созданию базовой системы стандартов безопасности Интернета вещей. В частности, в руководстве подчеркивается необходимость создания фундаментальной основы для систем и моделей безопасности для предотвращения рисков безопасности общественных сетей, содействия разработке и внедрению стандартов для IoT. Более конкретно, в руководстве подробно описано, что стандартные требования к безопасности терминалов в системах безопасности IoT должны включать меры по обеспечению безопасности программного обеспечения, аутентификации доступа и безопасности данных. Далее, в руководстве отмечаются методы тестирования и оценки соответствующих мер безопасности, относящихся к IoT, которые включают тестирование сертификации доступа и тестирование безопасности данных. Руководство направлено на создание и развитие системы базовых стандартов IoT, которая будет реализована в два этапа. К 2022 году будет создана указанная система и разработано не менее 10 отраслевых стандартов, а также уточнены требования к безопасности. После этого, к 2025 году будет разработано более 30 отраслевых стандартов, направленных на повышение уровня безопасности межотраслевого применения IoT.

Стандарты государств-членов ОЭСР по развитию регулирования Искусственного интеллекта. Страны принимают стратегические документы и специальные акты в сфере регулирования искусственного интеллекта. Стратегическими документами устанавливаются общие принципы регулирования ИИ, в том числе в сфере этики ИИ в соответствии с Рекомендацией ОЭСР по искусственному интеллекту 2019 г. Помимо этических принципов устанавливаются стандарты разработки и эксплуатации систем ИИ, меры ответственности за нарушения норм в сфере использования систем ИИ, недопустимые виды использования таких систем, а также специальные нормы использования отдельных видов систем ИИ, таких как рекомендательные сервисы. Таким образом, формирование правового регулирования систем искусственного интеллекта (как общего, так и отраслевого) и имплементация принципов этики использования систем искусственного интеллекта в качестве

правовых норм, а не только положений в стратегических документах, является общим для развитых стран трендом. Отсутствие целенаправленной и, что крайне важно, системной работы по развитию такого регулирования, как и в случае с регулированием любой сферы общественных отношений, которые выходят за рамки действующего в стране правового регулирования, не только создает риски правонарушений (в случае с системами ИИ таких, как нарушения в сфере защиты конкуренции, персональных данных, прав потребителей, трудовых прав), но и влечет за собой проблемы, связанные с определением правовой ответственности в случае причинения ущерба в рамках новой сферы отношений (например, ущерба, причиняемого автономными транспортными средствами), а также может повлечь за собой избыточные бюджетные издержки (например, при неправильном внедрении органами власти в свою деятельность систем ИИ), а также создание барьеров для экспортеров систем ИИ (в силу несоответствия продуктов, использующих ИИ, международным стандартам доверенного искусственного интеллекта).

Стандарты государств-членов ОЭСР по развитию цифровых платформ. Анализ стандартов США, Европейского союза, Китая и других стран показывает, что:

1) в зарубежных странах вводится понятие дистанционного контракта на поставку услуг, а также цифрового контента, что предоставляет потребителям дополнительные гарантии при покупке мобильных приложений онлайн-игр и любого другого цифрового контента;

2) создается возможность вернуть товар/ услугу/ контент при дистанционном способе заключения контракта в течение 14 дней, при этом у потребителя не возникает обязательств объяснять причину отказа, а также не должно возникать дополнительных затрат для возврата продукта.;

3) внедряются требования к ограничению сроков доставки, а также по возложению рисков доставки на продавца.

Таким образом, можно выделить ряд тенденций развития правового регулирования защиты прав потребителей в ЕС, которые могут быть реализованы в России. Во-первых, это регулирование договора на поставку цифрового контента или цифровых услуг.

Во-вторых, важной тенденцией является регулирование обманной практики, таких как обман при бесплатных онлайн-подписках на контент или услуги, недостоверное рейтингование и обман путем фальсификации потребительских отзывов.

В-третьих, важной тенденцией права ЕС является предотвращение рисков гео-блокировки, а также гарантии доступа к онлайн-контенту, на который абонент был подписан на территории одного государства-члена, но временно находится на территории другого

государства. Подобные инструменты могут использоваться в России и в ЕАЭС для предотвращения дискриминации потребителей онлайн услуги и контента из разных государств-членов.

Стандарты государств-членов ОЭСР по развитию возможности цифрового взаимодействия субъектами экономики. Среди зарубежных государств активные меры, направленные на развитие регулирования возможностей цифрового взаимодействия, приняты в государствах-членах Европейского союза, Великобритании и др. Все государства-члены ЕС обязаны имплементировать в свое законодательство нормы электронного инвойсинга, определенные в Директиве 2014/55/ЕС об электронном инвойсинге. Это означает, что во всех странах ЕС транзакции между государственными органами и другими субъектами влекут за собой обязательство использовать электронный инвойс, который соответствует критериям европейского стандарта, определено ЕС. Это касается ситуаций, когда какой-либо орган, организация или орган, деятельность которого регулируется публичным правом, является стороной сделки.

Требование ЕС в отношении электронного счета-фактуры B2G сосредоточено на способности государственных органов получать и обрабатывать электронные счета-фактуры. Это не налагает никаких подобных обязательств на поставщика. Это означает, что счета-фактуры могут быть представлены в любом формате, включая бумажный. На практике большинство государств-членов также предусматривают для продавца (так называемого экономического оператора) полномочия по представлению (отправке) электронного счета-фактуры. Однако в девяти государствах-членах поставщик может выбрать выставление соответствующего электронного счета-фактуры в транзакциях B2G.

Гармонизация правового регулирования e-invoicing ограничивается семантическим стандартом электронных счетов. Другими словами, законодательство ЕС определяет набор данных и полей, которые должны быть в таком документе. Однако инфраструктура, которая позволяет создавать, передавать и архивировать электронные счета, представляет собой отдельные решения и может независимо управляться провайдерами в разных странах. Стандарт ЕС по электронному выставлению счетов (EN 16931), помимо семантической части, должен обеспечивать единый формат документа за счет использования синтаксиса. В настоящее время только два синтаксиса соответствуют критериям стандарта электронного счета-фактуры: UBL и CII, что не исключает существования и использования синтаксиса (формата) электронного счета-фактуры для конкретной страны.

4. Предложения по устранению правовых барьеров в области регулирования оборота данных, использования цифровых технологий и работы цифровых платформ, препятствующих цифровой трансформации российской экономики

Предложения по устранению правовых барьеров в области регулирования оборота данных. Россия может улучшить свои результаты в управлении данными, опираясь на международные стандарты и практики, как Рекомендация ОЭСР 2021 г. (Рекомендация EASD). Но для этого необходимо обеспечить необходимые условия для имплементации стандартов, в том числе проработать существующие пробелы законодательства в области регулирования данных. Для качественной имплементации международных стандартов по повышению доступа к данным и обмену данными, необходимо принять следующие меры:

- для целей обеспечения контроля субъектом персональных данных в отношении собственных данных, переданных для обработки Роскомнадзору следует разработать пакет поправок в ФЗ «О персональных данных» в части: 1) уточнения требований к согласию на обработку персональных данных, а именно введения требования об обработке данных исключительно для целей, указанных в форме предоставления согласия на обработку данных и введения условия о письменной и электронной форме согласия, чтобы исключить возможность презюмирования согласия из конклюдентных действий субъекта персональных данных (например, в качестве пользователя цифровой платформы); 2) в части введения обязательства оператора данных уведомлять субъекта персональных данных об инцидентах, связанных с безопасностью полученных данных с целью повышения осознанности субъектов в распоряжении своими данными, что в долгосрочной перспективе способствует формированию культуры ответственного потребления цифровых услуг и ответственной передачи данных.

- Роскомнадзору следует разработать проект поправок в ФЗ «Об информации, информационных технологиях и защите информации» в части введения института посредника по передаче данных и регламентации условий его работы. Положения об информационном посреднике должны включать как минимум: принципы работы посредника по передаче информации, порядок регистрации для оказания посреднических услуг, порядок работы с клиентами, условия обеспечения профессиональной ответственности за качество услуг.

- Роскомнадзор может разрабатывать для участника обмена данными руководства и руководящие принципы по формированию договоров в области управления и передачи данных (отраслевые или общие) в целях гармонизации договорных положений по информационной безопасности, а также для обеспечения справедливых условий для МСП.

- ФСТЭК как орган, в чью компетенцию входят вопросы информационной безопасности, может разработать систему стандартов информационной безопасности для новейших технологий (как облачные технологии) и на их основе ввести систему сертификации. Для популяризации системы сертификации ФСТЭК может рекомендовать другим публичным институтам учитывать наличие сертификата по стандартам ФСТЭК, как преимущество для потенциальных поставщиков информационных услуг публичным институтам.

- Минцифры может сформировать рекомендации или основы по созданию публично-частных партнерств по управлению данными, которые бы включали модельные положения по передаче данных, по распределению ответственности при передаче данных, при обработке данных; рекомендации по перспективным сегментам экономики, где обмен данными является наиболее востребован (например, в области образования, здравоохранения, промышленности, транспортной инфраструктуры).

Предложения по развитию регулирования технологии блокчейн. Для дальнейшего развития технологий распределенного реестра необходимо:

– Минцифры совместно с Минэкономразвития разработать Методические рекомендации по лучшим практикам реализации проектов с использованием технологии распределенного реестра, в том числе блокчейн, для участников рынка. Такие рекомендации должны включать задачи для разработчиков программного обеспечения: по обеспечению прозрачности работы алгоритма для пользователей, информированию пользователей о принципах и субъектах, которые могут управлять работой реестра. Разработчики ПО должны обеспечить возможность независимого аудита кода, а также принять все необходимые меры для устранения найденных уязвимостей. Для целей обеспечения соблюдения законодательства о персональных данных разработчики кода должны обеспечить минимальную потребность в хранении персональных данных в распределенном реестре для пользователей. В методических рекомендациях также необходимо установить необходимость обеспечения интероперабельности, в том числе на основе стандартов ISO, а также Рекомендации ОЭСР о распределенном реестре и блокчейн 2022 года.

– Правительству РФ совместно с заинтересованными ФОИВами провести регуляторный эксперимент по использованию технологии блокчейн для повышения качества государственных услуг в соответствии с ФЗ «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации».

– Минпромторг России совместно с Центром развития перспективных технологий и участниками рынка разработать методические рекомендации по использованию технологии распределенного реестра для обеспечения прослеживаемости отдельных категорий товаров и сырья. В качестве пилотных категорий товаров следует взять те, в отношении которых уже сегодня внедрены требования к маркировке готовой продукции, в том числе табачная продукция, лекарства, товары легкой промышленности. Использование IoT-устройств для записи данных в блокчейн позволит повысить качество производимой продукции, фиксируя место происхождения сырья, условия транспортировки готовой продукции и другие параметры.

– Минфин России совместно с Банком России и Минэкономразвития России подготовить законопроект о регулировании выпуска и оборота в России платежных токенов (цифровых валют), стейблкоинов, продуктовых токенов (утилитарные цифровые права). В настоящее время в большинстве блокчейн-платформ предусмотрено использование токенов в качестве средства для получения доступа к информации на платформе, внесение записей в такой блокчейн и др. В соответствии с российским законодательством такие токены (даже те, что не обращаются свободно на криптобиржах) могут расцениваться в качестве цифровых валют, а операции по их использованию в качестве оплаты доступа к услуге, что запрещено законодательством РФ.

Предложения по развитию регулирования технологии Интернета вещей. Для достижения результатов в направлениях экономики, наиболее чувствительных к эффектам применения технологии IoT, как промышленность, а также для обеспечения конкурентоспособности российского рынка IoT, российским ведомствам рекомендуется использовать лучшие практики и международные стандарты:

- использовать стандарты NIST SP 800-53 (из практики США) или аналогичные стандарты гармонизации практик обеспечения информационной безопасности в публичном секторе для разработки руководства технологий IoT для бизнеса. Разработку следует осуществлять при участии экспертов и представителей профильных компаний;

- использовать международные практики при разработке руководства или регуляторных положений в части условий обеспечения безопасности данных, собираемых IoT датчиками. Такие положения в особенности востребованы в сферах, где данные могут составлять коммерческую тайну (например, в промышленности), или где от их сохранности зависит безопасность функционирования объекта (например, в сегменте телекоммуникационных услуг).

- использовать опыт стран ОЭСР (например, практику стран ЕС по реализации программы Horizon Europe в направлении «Digital») при разработке программы финансирования решений на основе технологий IoT с целью поддержки инновационных проектов, которые вносят вклад в достижение национальных целей развития. Базовыми проектами для финансирования являются проекты мета-операционных систем (цифровых экосистем для экономических сегментов). Также важны социально значимые проекты устойчивого развития, такие как проект распределения продуктов по магазинам в городах для минимизации пищевых отходов и для поддержки нуждающихся семей (что соответствует целям по сокращению голода и развитию ответственного потребления (механизм уже реализуется в Милане в рамках проекта RELOW49).

- использовать опыт стран ОЭСР (например, практику стран ЕС в создании систем бизнеса и научных структур в области прорывных технологий, как проект «Электронные компоненты и системы для европейского лидерства», созданный Промышленной ассоциацией Advanced Research & Technology for Embedded Intelligent Systems Industry Association (ARTEMIS-IA)) для развития эффективного взаимодействия бизнеса и научных центров.

Предложения по развитию регулирования Искусственного интеллекта. Указом Президента РФ от 10.10.2019 № 490 утверждена Национальная стратегия развития искусственного интеллекта на период до 2030 года (далее - Стратегия). В Стратегии перечислены основные принципы, соблюдение которых обязательно при её реализации (и, следовательно, при реализации Стратегии развития информационного общества программы «Цифровая экономика», иных национальных и федеральных проектов и программ, Национальной технологической инициативы и т.д.). Перечисленные принципы в целом соответствуют международной практике, в том числе Рекомендации ОЭСР по развитию искусственного интеллекта 2019 г. Вместе с тем, принципы Стратегии не охватывают в полной мере общепринятые международные принципы использования и развития технологии искусственного интеллекта. Так, например, Стратегией не охвачен принцип надежности, то есть необходимости определения сторон (разработчиков, операторов и т.д.) и отдельных лиц, ответственных за правомерность действий и обеспечение ответственного использования ИИ на всех этапах его жизненного цикла.

В 2020 г. также был утверждён Федеральный проект «Искусственный интеллект» (далее – «Федеральный проект»), целью которого обозначено повышение использования предприятиями и гражданами преимущественно отечественных решений в сфере ИИ, которые «обеспечивают качественно новый уровень эффективности деятельности». Следует отметить, что, согласно данному Федеральному проекту, государственное управление не

относится к сферам, в которых планируется целенаправленно внедрять и повышать доступность и качество данных, необходимых для развития технологии искусственного интеллекта. Ещё одна содержательная проблема Федерального проекта заключается в том, что в рамках его реализации практически не предусмотрено осуществление международного взаимодействия в сфере регулирования ИИ, участия в разработке международных стандартов в сфере использования ИИ.

В России разработан проект федерального закона «О высокоавтоматизированных транспортных средствах»; под такими транспортными средствами понимаются средства, оснащенные автоматизированной системой вождения и допущенные к участию в дорожном движении на территории РФ. В части разработки регулирования высокоавтоматизированных транспортных средств рекомендуется при разработке новой версии соответствующего законопроекта установить точные критерии разграничения ответственности между субъектами регулирования, предусмотреть ответственность дилеров в пределах их обязанностей по осуществлению технического осмотра и ремонта ВАТС и критериев установления факта добросовестного выполнения дилером таких требований в части проверки корректности работы систем ИИ в ВАТС. К критериям разграничения ответственности в случае попадания ВАТС в ДТП могут быть отнесены ошибка водителя, дефект разработки, неправильное обслуживание или эксплуатация ВАТС.

Предложения по развитию цифровых платформ. Для развития регулирования, направленного на противодействие злоупотребления отдельными платформами доминирующего положения, следует внести следующие положения в Пятый антимонопольный пакет поправок:

1) установить в рамках запрета на монополистическую деятельность (в части запрета на злоупотребление доминирующим положением) для «хозяйствующих субъектов, предоставляющих ПО и Интернет для совершения сделок между продавцами и покупателями по покупке товаров» оценивается количество пользователей, например, от 45 – 50 млн потребителей и 10 тыс. бизнес-пользователей. В некоторых случаях оцениваются не размеры компании или количество пользователей, а доступ к данным, сложность перехода на другие платформы и пр.;

2) установить, что помимо сетевых эффектов необходимо также оценивать возможность для пользователей использовать услуги разных платформ (поставщиков услуг), например, оценивать, обеспечивает ли платформа интероперабельность с другими системами, а также величину затрат, которые несет пользователь при смене платформы (поставщика услуг); использование платформой новых технологических решений, которые могут давать конкурентные преимущества цифровой платформе (экосистеме) и ее пользователям

и пр.

3) распространить действие Пятого антимонопольного пакета не только на хозяйствующих субъектов, предоставляющих ПО и Интернет для совершения сделок между продавцами и покупателями по покупке товаров, но и для сферы услуг, охватив услуги поисковых систем, сервисы социальных сетей, сервисы обмена видео, услуги операционных систем, рекламные услуги и пр.

4) ФАС принять разъяснения в отношении того, какие действия могут быть признаны злоупотреблением доминирующим положением, в частности, запрет:

– смешивать персональные данные пользователей, полученные в рамках услуг платформы и полученные от использования сторонних сервисов;

– ставить в качестве условия доступа к услугам платформы согласие пользователя на обработку данных другими сервисами платформы или сторонним провайдером без предоставления пользователю достаточного выбора относительно того, будут ли данные обработаны, каким образом и для каких целей;

– вмешиваться в ценовую политику бизнес-пользователей, в частности, устанавливать требования паритета цен для бизнес-пользователей, то есть, требование поддерживать одну и ту же цену на разных платформах;

– требовать, чтобы бизнес-пользователь использовал механизмы идентификации только предоставляемой этой платформой (чтобы могли использовать любые другие инструменты и др.

В России развивается законодательство по защите прав потребителей в электронной коммерции. С 2019 г. вступили поправки в Закон РФ от 7 декабря 1992 г. № 2300-1 «О защите прав потребителей», установившие правовой режим деятельности владельцев агрегаторов (электронных площадок). Тем не менее действующее законодательство не устанавливает режим регулирования и ответственности агрегатора, а также продавца при торговле цифровыми услугами, контентом, в частности, кто несет ответственность за поставку контента или услуг, какие договоры должны использоваться в данном случае, какие гарантии потребителю должен предоставлять продавец, а какие платформа и пр. Предложения по развитию регулирования в России:

1) включить в потребительское законодательство аспекты регулирования цифровых услуг, цифрового контента, а также товаров, которые содержат в себе цифровой контент или цифровую услугу. Внести изменения в Закон РФ от 07.02.1992 N 2300-1 «О защите прав потребителей»:

– в преамбуле установить понятие поставки цифрового контента и цифровой услуги.

– в преамбуле установить понятие совместимость – способность товаров, цифровых услуг или цифрового контента функционировать с использованием оборудования и/ или программного обеспечения, которое обычно используется с товарами, цифровыми услугами или цифровым контентом подобного типа.

– в преамбуле установить понятие интероперабельность – способность товаров, цифровых услуг или цифрового контента функционировать с использованием оборудования и/ или программного обеспечения, отличного от того, которое обычно используется с товарами, цифровыми услугами или цифровым контентом подобного типа.

– в преамбуле установить понятие функциональность – способность товаров, цифровых услуг или цифрового контента выполнять свои функции в соответствии с предназначением.

2) расширить регулирование товаров, которые содержат цифровой контент или услуги. Внести изменения в Закон РФ от 07.02.1992 N 2300-1 «О защите прав потребителей», включив специальную статью 26.3, содержащую требования:

– по предоставлению продавцом аксессуаров и инструкции по установке необходимого программного обеспечения или других технических средств для использования потребителем товара, содержащего цифровые услуги или контент;

– по пригодности товара для целей, для которых используют данный тип товаров, с учетом технических стандартов и других законодательных актов;

– по применению обновлений цифрового контента или услуг. Если товар с цифровыми элементами требует технических обновлений, продавец должен обеспечить, чтобы потребитель был осведомлен о таких обновлениях;

– если предусмотрена плата за использование товаров в течение определенного периода (например, товары с абонентской платой за цифровой контент), то в случае замены товара по причине несоответствия заявленным свойствам потребитель не обязан оплачивать период использования, предшествующий замене и др.

Предложения по развитию возможности цифрового взаимодействия субъектами экономики. В России создан ряд средств для цифрового взаимодействия между компаниями и органами власти. В частности, ФНС разработан сервис государственной онлайн-регистрации бизнеса. Сервис позволяет заполнить через Личный кабинет налогоплательщика заявление о государственной регистрации ИП или юридического лица, использовать типовой устав ООО, выбрать режим налогообложения, способа предоставления документов (в том числе в электронном виде с электронной подписью заявителя). В 2022 г. ФНС России введен экспериментальный налоговый режим – автоматизированная упрощенная

система налогообложения (АУСН). В рамках данного режима организация или ИП может договориться с банком, по сути, об автоматическом перечислении налога в бюджет. Кроме того, режим АУСН предполагает снижение объемов отчетности участвующих в нем организаций: вместо 4-х видов отчетности (декларация, расчет по взносам, СЗВ-М и СЗВ-СТАЖ, 4-ФСС) налогоплательщики учитывают сведения о выплатах и иных вознаграждениях физлицам, которые облагаются взносами и освобождаются от обложения.

В 2020–2021 г. Центром Россия-ОЭСР РАНХиГС была разработана законодательная инициатива по введению в российское законодательство режима цифрового лица (ЦЛ). Такой режим должен позволить юридическим лицам, зарегистрированным в России, преимущественно выстраивать рабочие процессы между собой и органами государственной власти с помощью сети Интернет, т.е. за счет использования всех благ платформенной экономики. Режим предоставляет следующие возможности для компаний:

- отказ от физического адреса компании;
- упрощение налогового администрирования за счет доступности первичных документов на платформе, как следствие снижение количества налоговых проверок;
- снижение затрат на должную осмотрительность за счет автоматизации получения данных о компании, процессах, количестве и сумм сделок контрагента и др.

В частности, концепцией предлагается создание правовых условий для формирования режима, позволяющего регистрировать юридические лица без физического адреса (цифровые лица) посредством специально создаваемых цифровых платформ.

С учетом изложенного, в части развития регулирования цифрового взаимодействия между субъектами экономики в Российской Федерации Минэкономразвития России рекомендуется:

- Совместно с Минфином России, ФНС России и Минцифры России разработать правовое регулирование, направленное на создание условий для подтверждения официальных организационных ролей в организациях с помощью цифровых идентификаторов в соответствии с ISO 5009, ISO 17442.

- Совместно с Минцифры России разработать правовое регулирование, направленное на формирование в России стандартов электронной идентификации юридических лиц, включая электронные печати организаций и электронные метки времени.

- Совместно с Минцифры России, ФНС России создать экспериментальный правовой режим для функционирования в России цифровых юридических лиц с одновременной разработкой правового регулирования института цифровых юридических лиц, предусматривающего осуществление юридическими лицами деятельности, включая ведение доку-

ментооборота и взаимодействие с органами государственной власти целиком в электронном виде.

Оценка влияния санкций на изменение подходов в регулировании цифровой экономики в России и предложения по минимизации негативных последствий санкций. По оценкам Всемирного Банка, экономические санкции недружественных государств в отношении России могут привести к сокращению ВВП страны на 11,2% в 2022 г., тогда как по оценкам российских экономистов потери варьируются от 6,4 до 11,5% в зависимости от уровня цен на нефть, курса валют, торгового оборота. Экономическое давление на российский рынок послужило триггером к усугублению кадровой ситуации в IT-отрасли России и оттоку технологических компаний.

Помимо сокращения персонала среди IT-компаний популярным решением для оптимизации потерь становится перенос бизнеса в зарубежные юрисдикции с целью выведения бизнеса из-под экономических санкций. Как подчеркивают специалисты, это не всегда значит физический переезд кадров, речь идет именно о перенаправлении усилий квалифицированных ресурсов на другие рынки. Для отечественной отрасли это может означать приостановку российских проектов, общее торможение развития и как следствие потерю конкурентоспособности российской отрасли в высокотехнологичных сферах, как информационная безопасность, технологии искусственного интеллекта, облачные технологии и др.

Меры поддержки IT-отрасли должны учитывать факторы, препятствующие развитию и укреплению конкурентоспособности IT-отрасли в условиях экономических санкций.

1. Фактор недостатка кадров. Рекомендуется:

- Расширить государственную программу «Цифровые профессии» по поддержке получения дополнительного профессионального образования, путем вовлечения в программу большего числа региональных образовательных учреждений и компаний в IT-сегменте;

- Обеспечить кадровое насыщение рынка путем предоставления специальных налоговых вычетов на НДФЛ на образовательные расходы налогоплательщиков по курсам переквалификации, повышения квалификации, обучения начальным профессиональным навыкам в сферах ИКТ.

- Обеспечить государственное субсидирование не менее 80% учебных мест по IT-специальностям в российских вузах.

- Обеспечить финансирование курсов довузовской подготовки IT-специалистов.

- Обеспечить финансирование школ для привлечения квалифицированных преподавателей информатики, для организации программ дополнительного образования, связанного с ИКТ.

– Обеспечить поддержку технологическим компаниям, организующим программы стажировок для студентов профильных программ.

– Обеспечить поддержку компаний, с лучшими показателями по доле женщин ИТ-специалистов в компаниях (с показателями выше среднего в соответствующем регионе).

2. Фактор неконкурентоспособных зарплат ИТ-специалистам в сравнении с предложениями зарубежных юрисдикций. Рекомендуется:

- Обеспечить субсидирование ставки по ипотеке, которая бы максимально сократила период погашения ипотечных обязательств из расчёта средней заработной платы ИТ-специалистов в регионе приобретения жилья. Мера доступна как ИТ-специалистам, работающим в ИТ-компаниях, так и специалистам, работающим в качестве самозанятого или индивидуального предпринимателя.

3. Фактор необходимости высвобождения средств для технического оснащения. Рекомендуется:

- Обеспечить субсидирование ставок договоров лизинга на ИТ-оборудование, заключаемых между банками, зарегистрированными на территории РФ, и технологическими компаниями.

- Обеспечить субсидирование программ рефинансирования кредитов, полученных ИТ-компаниями по ставкам выше ставок, обеспечиваемых в рамках мер поддержки ИТ-отрасли.

4. Фактор необходимости сохранения экспорта ИТ в зарубежных юрисдикциях. Рекомендуется:

- Освободить компании-экспортеры в ИТ-сфере от валютных требований, установленных Указом Президента РФ от 28.02.2022 № 79 и от любых последующих валютных требований, вводимых в ответ на экономические санкции, если эти требования ограничивают возможности российских экспортеров ИТ-продуктов и ИТ-услуг свободно распоряжаться валютной выручкой и использовать зарубежные счета.

- Обеспечить меры поддержки по продвижению на новых зарубежных рынках дружественных стран.

Финансовые меры поддержки:

- в части компенсации затрат по обеспечению инфраструктуры точек сбыта в новых юрисдикциях.

- в части компенсации затрат по участию в национальных и региональных выставках информационных технологий, телекоммуникационных технологий или смежных отраслей (LegalTech, Fintech).

Нефинансовые меры поддержки:

- в части предоставления юридических консультаций по ведению бизнеса в новых юрисдикциях, в том числе в регионе ведения бизнеса.

- в части содействия поиска рынков сбыта. РЭЦ необходимо установить партнерства с зарубежными ведомствами или агентствами по вопросам внешней торговли в соответствующих юрисдикциях при содействии двусторонних торговых палат, таких как китайско-русская торговая палата, российско-индийская торговая палата и др.

- в части содействия маркетинговому продвижению на новом рынке на базе РЭЦ могут проводиться аналитические исследования потребительского рынка, наиболее популярных цифровых платформ, бизнес-площадок, бизнес-объединений, популярных отраслевых стандартов качества, действующих на интересующем рынке, с целью обеспечения российских экспортеров практическими рекомендациями в соответствии с их бизнес-профилем.

Заключение

В рамках исследования выявлены основные направления правового регулирования цифровой экономики, правовые барьеры в которых могут блокировать потенциал цифровой экономики – барьеры регулирования оборота данных, барьеры в области цифровых технологий, барьеры в регулировании цифровых платформ и электронной коммерции. Но страны вырабатывают национальные подходы к устранению таких барьеров или к нивелированию негативных эффектов от введения ограничивающих регуляторных инструментов, например выборочное ограничение трансграничной передачи стратегически ценных данных.

Развитие правового режима данных могут обеспечить положения Рекомендации ОЭСР по улучшению доступа к данным и обмену ими (OECD Recommendation on EASD). С учетом предложенных стандартов российские регулирующие органы могут разрабатывать инструменты, которые направлены на укрепление доверия к надежности систем данных, на формирование единого подхода к вопросу обеспечения доступа к данным на всех уровнях и областях управления, на обеспечение баланса между мерами повышения доступа к данными и мерами защиты публичных и частных прав, связанных с данными; на обеспечение условий конкурентной цифровой экономики; на обеспечение свободной трансграничной передачи данных; на обеспечение интероперабельности информационных систем и единообразия стандартов регулирования технологий; на обеспечение условий эффективного использования открытых данных.

Также важно обеспечить условия регулирования инструментов работы с данными – различного рода технологий. Российские регуляторы могут использовать ряд интересных положений Рекомендации по безопасности цифровых продуктов, например, формирование общегосударственного подхода к цифровой безопасности информационных продуктов, имплементация в национальные регуляторные акты обязанности поставщиков цифровых продуктов проявлять осторожность и разработка руководств по интеграции цифровой безопасности на каждом этапе разработки продукта; разработка политики поощрения поставщиков цифровых продуктов, имплементирующих международные стандарты информационной безопасности и раскрывающих информацию о своей деятельности наиболее полным образом. Реализация таких рекомендаций обретает всё большее значение на фоне распространения на потребительских рынках таких сложных прорывных технологий, как Интернет Вещей и Искусственный интеллект.

В отсутствии регулирования цифровых технологий нет возможности обеспечить прозрачную цепочку создания стоимости продуктов IoT, проконтролировать безопасность разрабатываемых продуктов на каждом этапе жизненного цикла, начиная с проектирования

и заканчивая конечным использованием. Более того, цифровые технологии часто работают с данными, пользуясь правовым режимом персональных данных. Поэтому регулирование технологий в том числе включает вопрос правомерного оперирования используемыми данными. В этом отношении показательна Рекомендация ОЭСР по искусственному интеллекту 2019 г., которая включает принципы справедливости и человекоцентричности. Для имплементации данных принципов национальным регуляторам рекомендуется разрабатывать стандарты безопасности и кодексы этики искусственного интеллекта, также поддерживать другие инструменты «мягкого» регулирования на уровне бизнес-сообщества. Такие инструменты должны основываться на принципах инклюзивного роста и устойчивого развития, уважения прав человека, прозрачности и объяснимости результатов работы системы ИИ, устойчивости и безопасности технологий, надежности функционирования ИИ, развития цифровой экосистемы ИИ. Важно учитывать, что реализация данных принципов возможна только в условиях соответствующей правовой среды. Так, в странах уже есть большой опыт создания цифровых песочниц для прорывных технологий, как ИИ, поэтому практика позволяет переходить к общему регулированию. Кроме того, развитие технологий возможно только при наличии квалифицированных кадров, поэтому политики в сфере ИИ должны включать вопросы доступа к технологическому образованию и поддержки специалистов.

Регулирование требуется как для информационных ресурсов и инструментов управления ими, так и для их пользователей-участников цифровой экономики. Поскольку цифровизация трансформирует отношения среди субъектов цифрового рынка, на международных площадках создаются инструменты измерения цифровой экономики, как Инструментарий G20 по измерению цифровой экономики 2018 г. Один из ключевых аспектов цифровых взаимодействий – это электронный обмен документами. Поэтому в 2017 г. Центр Организации Объединенных Наций по упрощению процедур торговли и электронным деловым операциям (СЕФАКТ ООН) разработал стандартную межотраслевую модель e-invoicing, которая может быть использована как в B2B, так и в B2C и в B2G-отношениях. Цифровизируются операции не только в отношениях среди субъектов цифровой экономики, но также и внутренние операции компаний. Поэтому цифровизация корпоративного управления становится важной областью формирования международных практик, как например, стандарт ISO 5009 для подтверждения официальных организационных ролей в бизнес-структуре с цифровыми идентификаторами.

Важно отметить, что цифровые решения актуальны и востребованы не только в частном секторе, но также для государства. Особенно показательна область цифрового налого-

вого администрирования. Данное направление работы цифровой экономики включает такие аспекты, как цифровая идентификация налогоплательщиков; упрощение взаимодействия налогоплательщика с налоговыми органами, например, с помощью единой информационной системы с индивидуальными личными кабинетами пользователей; управление налоговыми данными. Цифровизация налогового администрирования в российской практике является ярким успешным примером того, какие преимущества даёт цифровизация публичных услуг.

В настоящий момент возможности реализации выявленных лучших практик и международных стандартов зависит от воздействия геополитических изменений в мировой экономике (распространение санкционных режимов среди государств, включая торговые ограничения; прерывание и перестройка цепочек поставок и др.). При планировании мер по имплементации рекомендаций необходимо учитывать фактор ограниченных кадровых ресурсов, ограниченного доступа к технологическим элементам (микросхемам) или доступа к знаниевым компонентам (сведения о содержании технологий для их имплементации на российских производствах). Каждое из ограничений может быть в разной мере чувствительным для отдельных сегментов цифровой экономики.

Благодарности

Препринт подготовлен на основе материалов научно-исследовательской работы, выполненной в соответствии с государственным заданием РАНХиГС при Президенте Российской Федерации на 2022 год.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Data Protection or Data Protectionism? URL: <https://irisbh.com.br/en/data-protection-or-data-protectionism/> (дата обращения 1.06.2022).
2. Data Flows, Online Privacy, and Trade Policy // Congressional Research Service. URL: <https://sgp.fas.org/crs/misc/R45584.pdf> (дата обращения 1.06.2022).
3. European Commission. Communication from the Commission to the European Parliament, the Council. The European Economic and Social Committee and the Committee of the regions. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2015%3A0185%3AFIN> (дата обращения 1.06.2022).
4. Services Trade Restrictiveness Index (STRI): Scoring and Weighting Methodology. URL: <https://www.oecd-ilibrary.org/docserver/5js7n8wbtk9r-en.pdf?expires=1646685406&id=id&accname=guest&checksum=4F93B8C63CDEAF5FBA3751125B5D24BA> (дата обращения 1.06.2022).
5. OECD STRI Scoring Methodology. URL: <https://www.oecd.org/trade/topics/services-trade/documents/oecd-stri-scoring-methodology.pdf> (дата обращения 1.06.2022).
6. OECD Policy Simulator. URL: <https://www.oecd.org/trade/topics/services-trade/> (дата обращения 1.06.2022).
7. Конвенция о защите физических лиц при автоматизированной обработке персональных данных. Заключена в г. Страсбурге 28.01.1981. URL: https://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения 1.06.2022).
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679> (дата обращения 1.06.2022).
9. Robinson M., Chow P., Cotan C., Sakurayuki C. Cross-border data transfers- an Indonesian law update // Lexology. URL: <https://www.lexology.com/library/detail.aspx?g=c93c325c-65ab-4b9d-8ad4-7cadabcb6287> (дата обращения 1.06.2022).
10. Anant V., Donchak L., Kaplan J., Soller H. The consumer-data opportunity and the privacy imperative. McKinsey&Company. URL: <https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/the-consumer-data-opportunity-and-the-privacy-imperative> (дата обращения 15.06.2022).
11. Banerjee S., Sriram V. The impact of electronic data interchange on purchasing: an empirical investigation // International Journal of Operations & Production Management. Vol. 15

No. 3. P. 29-38. URL: <https://www.emerald.com/insight/content/doi/10.1108/01443579510080535/full/html> (дата обращения 15.06.2022).

12. Babati B. What is Electronic Data Interchange? Published on 25.07.2018. URL: <https://www.youredi.com/blog/what-is-electronic-data-interchange> (дата обращения 15.06.2022).

13. Babati B. The Most Common EDI challenges. Published on 07.03.2018. URL: <https://www.youredi.com/blog/the-most-common-edi-challenges> (дата обращения 15.06.2022).

14. Electronic communications compliance survey report // Smarsh. URL: <https://pages.smarsh.com/rs/893-GBT-581/images/GD-Smarsh-2019-Electronic-Communications-Compliance-Survey-Report.pdf> (дата обращения 15.06.2022).

15. Regulation (EU) No 910/2014 Of The European Parliament And Of The Council. URL: <https://www.eid.as/> (дата обращения 15.06.2022).

16. G20. Toolkit for measuring the digital economy. November 2018. URL: <https://www.oecd.org/g20/summits/buenos-aires/G20-Toolkit-for-measuring-digital-economy.pdf> (дата обращения 15.05.2022).

**В СЕРИИ ПРЕПРИНТОВ
РАНХиГС РАССМАТРИВАЮТСЯ
ТЕОРЕТИЧЕСКИЕ
И ПРАКТИЧЕСКИЕ ПОДХОДЫ
К СОЗДАНИЮ, АКТИВНОМУ
ИСПОЛЬЗОВАНИЮ
ВОЗМОЖНОСТЕЙ
ИННОВАЦИЙ В РАЗЛИЧНЫХ
СФЕРАХ ЭКОНОМИКИ
КАК КЛЮЧЕВОГО УСЛОВИЯ
ЭФФЕКТИВНОГО УПРАВЛЕНИЯ**



РАНХиГС
РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА
И ГОСУДАРСТВЕННОЙ СЛУЖБЫ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ