Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 2. С. 36–45.
Pacific Rim: Economics, Politics, Law. 2022. Vol. 24, no. 2. P. 36–45.

Научная статья
УДК 338:004(470+571):004.056
https://doi.org/10.24866/1813-3274/2022-2/36-45

К ПРОБЛЕМЕ РАЗРАБОТКИ КОНЦЕПЦИИ БЕЗОПАСНОСТИ ЦИФРОВОЙ ЭКОНОМИКИ РОССИИ*

Артур Георгиевич Кравченко
Дальневосточный федеральный университет, 690922, Россия, г. Владивосток, о. Русский, пос. Аякс, корпус D, kravchenko.ag@dvfu.ru
https://orcid.org/0000-0003-4729-1573

Аннотация. Исследуя проблемы обеспечения безопасности в цифровой экономике, автор выделяет основные составляющие двух сегментов – национального и международного, анализирует положения «Доктрины информационной безопасности Российской Федерации», рассматривая четыре уровня обеспечения безопасности цифровой экономики, отражаемой в национальной правовой политике. В статье анализируется содержание динамичного развития цифровой экономики России, приводятся особенности угроз, формулируются основные проблемы правовой политики по защите от обозначенных угроз. В заключение автор акцентирует внимание на необходимости рассмотрения системы безопасности цифровой экономики в геополитическом контексте, указывая на необходимость обеспечения стабильного функционирования инфраструктуры цифровой экономики (элементной базы, программного обеспечения, информационной среды), а также формирования системных условий развития и удержания человеческого капитала в национальной цифровом пространстве как ключевого фактора обеспечения безопасности цифровой экономики России.

Ключевые слова: цифровая экономика, информационная безопасность, правовое регулирование, риск, безопасность каналов связи, цифровые платформы, международные электронные платёжные системы, человеческий капитал, геополитическая конкуренция.

Финансирование. Статья подготовлена при финансовой поддержке гранта РФФИ № 19-011-00820 (а) «Правовая политика российского государства, её приоритеты и принципы в условиях цифровой экономики и цифрового технологи-

ческого уклада: концептуальные, методологические, отраслевые аспекты цифровизации права и правового регулирования».

Для цитирования: Кравченко А. Г. К проблеме разработки концепции безопасности цифровой экономики России // Азиатско-Тихоокеанский регион: экономика, политика, право. 2022. Т. 24, № 1. С. 36–45. https://doi.org/10.24866/1813-3274/2022-2/36-45

Original article

TO THE PROBLEM OF DEVELOPING THE CONCEPT OF SAFETY OF THE DIGITAL ECONOMY OF RUSSIA

Artur G. Kravchenko
Far Eastern Federal University, 690922, Russia, Vladivostok, Fr. Russian, 10 Ajax Bay, building D, kravchenko.ag@dvfu.ru, https://orcid.org/0000-0003-4729-1573

Abstract. Exploring the problems of ensuring security in the digital economy, the author identifies the main components of two segments – national and international, analyzes the provisions of the "Information Security Doctrine of the Russian Federation" considering the four levels of ensuring the security of the digital economy reflected in the national legal policy. The article analyzes the content and features of threats to the dynamic development of the digital economy of Russia, formulates the main problems of legal policy aimed at dealing with these threats. In conclusion, the author focuses on the need to consider the security system of the digital economy in a geopolitical context, pointing to the need of ensuring stable functioning of the infrastructure of the digital economy (element base, software, information environment), as well as the formation of systemic conditions for the development and retention of human capital in the national digital space, as a key factor of ensuring the security of the digital economy of Russia.

Keywords: digital economy, information security, legal regulation, risk, security of communication channels, digital platforms, international electronic payment systems, human capital, geopolitical competition.

Financing. The article was prepared with the financial support of the RFBR grant No. 19-011-00820 (a) “Legal policy of the Russian state, its priorities and principles in the digital economy and digital technological order: conceptual, methodological, sectoral aspects of the digitalization of law and legal regulation”.

For citation: Kravchenko A. G. To the problem of developing the concept of safety of the digital economy of Russia // PACIFIC RIM: Economics, Politics, Law. 2022. Vol. 24, no. 2. P. 36–45. https://doi.org/10.24866/1813-3274/2022-2/36-45.

Условно проблему обеспечения безопасности цифровой экономики можно разделить на несколько групп. Во-первых, это – национальный сегмент цифровой экономики России, включающий как частные, так и публичные интересы, охраняемые законом, среди которых следует выделить: сферу функционирования интернет-платформ, экосистем, обеспечивающих информационные коммуникации с участниками цифровой экономики; вопросы безопасности каналов связи, идентификации участников экономических отношений, правовой политики государства, влияющей прямо и косвенно на цифровую инфраструктуру общественных отношений цифровой экономики. Во-вторых, это – международный сегмент, включающий международные отношения в сфере электронной коммерции, в том числе инфраструктуру международных электронных платежных систем, таможенных отношений, вопросов предпринимательских и потребительских договорных отношений.

Обращаясь к рассмотрению проблемы концепции безопасности цифровой экономики, мы должны, прежде всего, уяснить понятие безопасности в экономическом смысле, основанное на управлении рисками**:** «…это категория риска, связанная с использованием, развитием и управлением цифровых технологий в процессе экономической деятельности». Этот риск может возникнуть в результате сочетания угроз и уязвимости в цифровой среде, подрывая достижение экономических целей, нарушая конфиденциальность, целостность и доступ» [4]. Как отмечает в этой связи Д. А. Горулев, «безопасность – есть управляемый риск. И ключевой вопрос состоит не только в принятии и контроле должного (допустимого) уровня риска, но также в выборе ключевых инструментов управления рисками и их соотношения, исходя из специфичности и не повторяемости (с точки зрения субъекта, принимающего решение) тех объектов, которые затронуты риском и могут быть подвержены уничтожению, изменению или утрате в результате реализации риска» [2]. Однако экономическая безопасность – это материя, включающая не только вопросы управления предпринимательскими рисками, это понятие гораздо шире и включает в себя социальные, политические и даже культурно-духовные риски. Но, если в отношении предпринимательского риска в формуле расчёта действует соотношение издержки (риск) и прибыль, то в социальной, культурно-духовной и политической сфере риску противостоят базовые человеческие ценности (жизнь, здоровье, мирная жизнь, социальная стабильность и т.п.), без обеспечения которых экономическая безопасность становится просто бессмысленна [8]. В этом смысле концептуальные документы, определяющие основы информационной безопасности России, скорее обращены к социальной и политической, нежели экономической природе отношений. Очевидно, отсюда проистекает конструкция в понятийном аппарате, применяемом законодателем, который под информационной безопасностью понимает «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация консти-

туционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [7]. Тем не менее, публичная безопасность всегда представляла собой комплексную, очень сложную многоаспектную задачу взаимоувязанных факторов и явлений, не ограниченную только социальным и политическим аспектом. Какие-то элементы национальной безопасности могут быть подвергнуты большему риску в поисках реализации возможностей экономического роста, какие-то меньшему, но это – в конечном итоге – единая система, в которой утрата контроля за одним из элементов приводит к утрате общей защищённости. Между тем, эта комплексная, взаимоувязанная природа сегментов национальной безопасности говорит о необходимости концептуальных связок между ними, включая безопасность цифровой экономики. Поэтому так важна выработка регуляторных решений с учётом общих издержек участников рынка, применение пропорционального и риск-ориентированного подходов одновременно.

В этом контексте, прежде всего, следует обратить внимание на то, что цифровая экономика – это не чистый цифровой субстрат информационных благ, в настоящее время это – неразрывный сплав информационной надстройки (цифровых технологий) и мира вещей (материальных благ). Поэтому, говоря об обеспечении безопасности цифровой экономики, следует понимать её прямую зависимость от традиционной экономики [6], и далеко не во всех аспектах цифровая экономика может оптимистично рассматриваться как средство решения кризисных проблем, например, вызванных пандемией Covid-19 [1].

В частности, вся инфраструктура цифровой экономики основана на материальных технологиях коммуникационных каналов связи, ретрансляторов и серверных решений.

Отсюда формируется первый уровень: угроза-вызов – зависимость национального государства от рынка микроэлектроники, технологических решений передачи данных и т.п. Решение этой задачи определяется либо наличием всего спектра национальных технологий, позволяющих обеспечить технически всю цепочку информационных коммуникаций, либо созданием условий диверсификации импортирования соответствующих товаров. Данный уровень безопасности в настоящее время определён законодателем и обеспечивается программой импортозамещения: «План мероприятий по направлению "Информационная безопасность" программы "Цифровая экономика Российской Федерации"» (утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 № 2)), предусматривающей сокращение зависимости от импорта технологий до 2024 года [12]. Тем не менее, и в этом процессе не всё однозначно, поскольку про-

цесс импортозамещения не реализуем в краткосрочной перспективе установленной программой, и экономический опыт это наглядно демонстрирует. Сложность реализации такой монополитики заключается в том, что российский сектор высоких технологий микроэлектроники крайне фрагментарен (отечественные производители не могут предоставить готовые экосистемы, на их разработку нужно время) [3], не конкурентоспособен в силу технологического отставания [15]. В этом ключе очевидна необходимость отражения в правовой политике России диверсификации импорта микроэлектроники, приоритетного развития национального производства компонентов элементной базы, представленных международными рынками с наивысшими геополитическими рисками ограничения поставок.

Второй уровень безопасности формируется в отношении программного обеспечения, поддерживающего цифровую инфраструктуру экономических коммуникаций. Угрозами этого порядка выступают: программные закладки стран-экспортёров, хакерские атаки, отключения от программных решений (цифровые блокировки). Указанный уровень также охвачен текущей правовой политикой российского государства и включает в себя комплекс технических стандартов информационной безопасности программных продуктов и специальных программных решений цифровой защиты [10]. Определены меры защиты цифровой экономики и в отношении потенциальной блокировки цифровой платёжной системы SWIFT [14]. Тем не менее, данные меры фактически ограничены внутренним цифровым рынком, что не представляется достаточным и требует своего развития на международном уровне, в частности в рамках БРИКС [13], и комплексных программных продуктов для противодействия несанкционированному доступу на международном уровне.

Третий уровень безопасности противостоит угрозам информационных искажений, влияющих на ценообразование, потоки инвестиций, котировки акций и т.п., влияющих на принятие управленческих решений человека как непосредственно применяемыми технологиями (цифровыми ассистентами), так и третьими лицами, формирующими избирательность информационных потоков программными способами без искажений их истинности. В отношении этого уровня безопасности можно наблюдать институциональную рефлексию по отдельным узким сегментам цифровой экономики [11] и упор преимущественно на административно-уголовные средства правового воздействия, применение которых сопряжено со значительными рисками угнетения динамики развития цифровой экономики. С другой стороны, одну из ключевых угроз информационного общества и цифровой экономики законодатель попрежнему игнорирует, несмотря на многочисленные доктринальные наработки, связанные с рисками информационной манипуляции и влияния на принятие решений как в сфере публичного, так и бизнес управления, частных инвестиций.

Четвёртый уровень безопасности определяет противодействие институциональным угрозам, среди которых: процессы деградации образования, культуры, духовно-

сти общества; исход человеческого капитала из страны; высокий уровень административных барьеров; бюрократизация; системное развитие коррупции; монополизм и низкий уровень конкуренции; тоталитарное мировоззрение, сочетающееся с критически низкой инициативностью в системах публичного и частного управления; сокращение рабочих мест вследствие автоматизации процессов производства.

Перспективной технологией противодействия вышеназванному уровню угроз, требующей правовой институционализации, являются цифровые платформы, экосистемы, которые основаны на условии объединения человеческого, экономического капитала. Объединяющий потенциал цифровых технологий позволяет участникам цифровой экономики преодолевать пространственные, временные, институциональные барьеры, создавая структурно сложные эффективные тандемы для реализации социальных и экономических проектов и задач. Такое свойство тем ценнее, чем в более ограниченных ресурсных условиях действуют его участники. Так, уже сегодня естественным образом начинают развиваться практики сетевого взаимодействия университетов, находящихся в условиях ограниченного человеческого капитала. В области цифровой экономики также активно развиваются краудфандинговые платформы бизнес-аналитики, медицинские платформы и т.п. Таким образом, перспективными являются разработки по основам правового регулирования режима взаимодействия участников подобных экосистем, их взаимной ответственности по взятым на себя обязательствам, защищённости проектных рисков. Сегодня это направление активно развивает Министерство экономического развития РФ, подтверждая актуальность и востребованность развития данной технологии. К сожалению, из сферы его внимания выпадает развитие государственных экосистем, которые позволили бы успешно решать социально-экономические задачи [9]. Так, например, крайне необходимой видится создание государственной научной платформы, позволяющей создавать научные коллективы под конкретную исследовательскую задачу. Нет (несмотря на явный тренд) и единой образовательной платформы для университетов, позволяющей оформить трудовые отношения их работников для совместной деятельности. Между тем очевидно, что для успешного функционирования таких платформ требуется внести законодательные изменения в отдельные отраслевые акты.

При формировании концептуальных решений институциональных угроз нельзя забывать и о понятии безопасности как комплексного явления. Отсюда, решение задач экономической безопасности исключительно через экономическую логику сокращения издержек создаёт критические провалы для экономической безопасности государства. Так, не является оптимальным решение проблемы демографического спада посредством замещения рабочей силы процессами автоматизации [5], поскольку помимо предпринимательской составляющей существует масса других факторов, формирующих экономическую безопасность. В частности, чем выше

уровень автоматизации, тем более уязвимы системы от потенциальных угроз, а контроль автоматизации операторами выступает механизмом, обеспечивающим защищенность таких систем. К тому же, в производственных операциях, где необходимы ценностные ориентиры, автономность воли, творчество, сложные интеллектуальные операции, человек становится драйвером цифровых процессов. Отсюда необходимость наращивания качества человеческого капитала и развития его цифровых компетенций является ключевой повесткой цифровой экономики. В этой связи, оценивая цифровую конкурентоспособность стран, Европейский центр цифровой конкурентоспособности выделил в качестве критериев оценки две группы показателей – цифровая экосистема (доступность развития бизнеса) и цифровое мышление (доминирование в обществах предпринимательского мышления, инициативности, цифровых компетенций) [16]. Красной нитью через совокупность этих критериев проходят «человеческий капитал» и институциональные возможности реализации его потенциала.

Институциональный уровень угроз является самым неочевидным, но самым сложно-решаемым фактором сдерживания потенциала развития цифровой экономики. Обеспечение экономической безопасности на этом уровне требует не просто решения технологических и организационных задач, а формирует в повестке современной России тренды на фундаментальные мировоззренческие, ценностные изменения через сложную матрицу государственно-правового воздействия на общество, обеспечивая геополитическую конкурентоспособность страны в области развития национальных технологий и производств.

Исходя из вышесказанного, следует заключить, что в настоящее время экономическая и правовая доктрина представлена широким спектром концептуальных наработок, позволяющих учитывать множество особенностей в механизмах обеспечения безопасности цифровой экономики. С другой стороны, правовая институционализация безопасности цифровой экономики фрагментарна и надлежащим образом не представлена в едином нормативно-концептуальном документе, что значительно снижает организационно-правовой инструментарий государственной власти по обеспечению безопасности цифровой экономики России.

Список источников

1. Бархатов В. И., Дьяченко О. В. Развитие цифровой экономики России в условиях пандемии // Вестник Челябинского государственного университета. 2020. № 10 (444). С. 177–82.

2. Горулев Д. А. Экономическая безопасность в условиях цифровой экономики // Технико-технологические проблемы сервиса. 2018. № 1 (43). С. 77–84.

3. Импортозамещение сетевого оборудования: как не наступить на грабли. URL: https://www.cnews.ru/articles/2021-09-21_importozameshchenie_setevogo_oborudovaniya.

4. Лев М. Ю., Лещенко Ю. Г. Цифровая экономика: на пути к стратегии будущего в контексте обеспечения экономической безопасности // Вопросы инновационной экономики. 2020. Т. 10, № 1. С. 25–44.

5. Лытнева Н. А., Воронов С. С., Киданова Н. Л. Глобальные вызовы и формирование цифровой экономики: состояние, проблемы безопасности, тенденции развития // На страже экономики. 2020. № 4 (15). С. 52–60.

6. Наталья Касперская: «Какая уж тут цифровая экономика?» // Федеральное информационное агентство REGNUM. URL: https://regnum.ru/news/economy/2962102.html.

7. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента РФ от 5 декабря 2016 г. № 646. URL: https://login. consultant.ru/link/?req=doc&demo=2&base=LAW&n=208191&dst=1000000001&date=10.10.2021.

8. Об утверждении Концепции развития системы управления рисками Федеральной службы по регулированию алкогольного рынка на период до 2020 года: приказ Росалкогольрегулирования от 8 декабря 2016 г. № 429. URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=256088&dst=100106&date=10.10.2021.

9. Об утверждении Концепции цифровой и функциональной трансформации социальной сферы, относящейся к сфере деятельности Министерства труда и социальной защиты Российской Федерации, на период до 2025 года: распоряжение Правительства РФ от 20 февраля 2021 г. № 431-р (ред. от 07.06.2021). URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=386588&dst=1000000001&date=08.12.2021.

10. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: приказ ФСТЭК России от 11 февраля 2013 г. № 17 (ред. от 28.05.2019) (Зарегистрировано в Минюсте России 31.05.2013 № 28608) (с изм. и доп., вступ. в силу с 01.01.2021). URL: http://www.consultant.ru/document/cons_doc_LAW_147084/.

11. Основные направления развития финансового рынка Российской Федерации на 2022 год и период 2023 и 2024 годов (разработаны Банком России). URL: http://www.consultant.ru/document/cons_doc_LAW_404693/.

12. План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации» (утв. Правительственной комиссией по использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности (протокол от 18.12.2017 № 2)). URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=287996&dst=100040&date=08.11.2021.

13. Пятивалютная корзина: страны БРИКС создают единый платёжный сервис. URL: https://iz.ru/851277/dmitrii-grinkevich/piativaliutnaia-korzina-strany-briks-sozdaiut-edinyi-platezhnyi-servis.

14. Стратегия развития национальной платежной системы на 2021–2023 годы (утв. Банком России). URL: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=382148&dst=1000000001&date=08.09.2021.

15. Суровый российский сервер. URL: https://www.kommersant.ru/doc/5131374/.

16. Digital Riser 2021. URL: https://www.tadviser.ru/images/2/29/Digital_Riser_Report-2021.pdf.

References

1. Barkhatov V. I., Dyachenko O. V. Development of the digital economy of Russia in a pandemic. *Vestnik Chelyabinskogo gosudarstvennogo universiteta*, 2020, no. 10 (444), pp. 177–82. (In Russ.).

2. Gorulev D. A. Economic security in the digital economy. *Tekhniko-tekhnologicheskie problemy servisa*, 2018, no. 1 (43), pp. 77–84. (In Russ.).

3. Import substitution of network equipment: how not to step on a rake. Available at: https://www.cnews.ru/articles/2021-09-21_importozameshchenie_setevogo_oborudovaniya. (In Russ.).

4. Lev M. Yu., Leshchenko Yu. G. Digital economy: on the way to the strategy of the future in the context of ensuring economic security. *Voprosy innovatsionnoi ekonomiki*, 2020, vol. 10, no. 1, pp. 25–44. (In Russ.).

5. Lytneva N. A., Voronov S. S., Kidanova N. L. Global challenges and the formation of the digital economy: state, security problems, development trends. *Na strazhe ekonomiki*, 2020, no. 4 (15), pp. 52–60. (In Russ.).

6. Natalya Kasperskaya: "What kind of digital economy is there?". *Federal Information Agency REGNUM*. URL: https://regnum.ru/news/economy/2962102.html. (In Russ.).

7. Approval of the Doctrine of Information Security of the Russian Federation: Decree of the President of the Russian Federation of December 5, 2016 No. 646. Available at: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=208191&dst=1000000001&date=10.10.2021. (In Russ.).

8. On approval of the Concept for the development of the risk management system of the Federal Service for Regulation of the Alcohol Market for the period up to 2020: Order of the Federal Service for Alcohol Regulation No. 429 dated December 8, 2016. Available at: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=256088&dst=100106&date=10/10/2021. (In Russ.).

9. On approval of the Concept for the digital and functional transformation of the social sphere, related to the field of activity of the Ministry of Labor and Social Protection of the Russian Federation, for the period up to 2025: Decree of the Government of the Russian Federation of February 20, 2021 No. 431-r (as amended on June 7, 2021). Avail-

able at: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=386588&dst=1000000001&date=12/08/2021. (In Russ.).

10. On approval of the Requirements for the protection of information not constituting a state secret contained in state information systems: order of the FSTEC of Russia dated February 11, 2013. No. 17 (as amended on May 28, 2019) (Registered in the Ministry of Justice of Russia on May 31, 2013 No. 28608) (with amended and supplemented, effective from 01.01.2021). Available at: http://www.consultant.ru/document/cons_doc_LAW_147084/. (In Russ.).

11. Main directions for the development of the financial market of the Russian Federation for 2022 and the period of 2023 and 2024 (developed by the Bank of Russia). Available at: http://www.consultant.ru/document/cons_doc_LAW_404693/.(In Russ.).

12. Action plan in the direction of "Information Security" of the program "Digital Economy of the Russian Federation" (approved by the Government Commission on the use of information technologies to improve the quality of life and conditions for doing business (Minutes No. 2 of December 18, 2017)). Available at: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=287996&dst=100040&date=11/08/2021. (In Russ.).

13. Five-currency basket: BRICS countries create a single payment service. Available at: https://iz.ru/851277/dmitrii-grinkevich/piativaliutnaia-korzina-strany-briks-sozdaiut-edinyi-platezhnyi-servis. (In Russ.).

14. Strategy for the Development of the National Payment System for 2021–2023 (approved by the Bank of Russia). Available at: https://login.consultant.ru/link/?req=doc&demo=2&base=LAW&n=382148&dst=1000000001&date=09/08/2021. (In Russ.).

15. Severe Russian server. Available at: https://www.kommersant.ru/doc/5131374/. (In Russ.).

16. Digital Riser 2021. Available at: https://www.tadviser.ru/images/2/29/Digital_Riser_Report-2021.pdf.

Информация об авторе

А. Г. Кравченко – к. ю. н., доцент, зав. кафедрой гражданского права и процесса Юридической школы Дальневосточного федерального университета, г. Владивосток, Россия.

Information about the author

A. G. Kravchenko – Candidate of Law, Associate Professor, Head of Department of Civil Law and Process, Law School, Far Eastern Federal University, Vladivostok, Russia.