4. Развитие и деятельность Содружества независимых государств в 2022 году. Сборник информ.-аналит. материалов. – Минск : Изд. Исполком СНГ, 2023. – Вып.11. – 243 с.

5. Стратегия развития сотрудничества государств-участников СНГ в области туризма на 2021 – 2030 годы [Электронный ресурс] Официальный сайт Исполнительного комитета СНГ. – Режим доступа: https://cis.minsk.by/news/15440/o_strategii_razvitija_sotrudnichestva_gosudarstv_%E2%80%93_uchastnikov_sodruzhestva_nezavisimyh_gosudarstv_v_oblasti_turizma_na_2021%E2%80%932030_gody – Дата доступа: 15.01.2024.

6. Международный проект стран СНГ «Драгоценное ожерелье Содружества» [Электронный ресурс] Официальный сайт Исполнительного комитета СНГ. – Режим доступа: https://cis.minsk.by/news/25039/predstaviteli_stran_sng_obsudili_voprosy_realizacii_proekta_%C2%ABdragocennoe_ozherele_sodruzhestva%C2%BB – Дата доступа: 15.01.2024.

УДК 339.5:004

ЦИФРОВАЯ ЭКОНОМИКА И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ В КОНТЕКСТЕ ПРАВИЛ МИРОВОЙ ТОРГОВОЙ СИСТЕМЫ

канд. экон. наук, доцент И.А. Шамардина, *ФММП БНТУ, г. Минск;*
канд. экон. наук, доцент З.М. Горбылева, *ФКТИ БГЭУ, г. Минск; аспирант Сяо Емэн*, *ФММП БНТУ, г. Минск*

Резюме. *Рассмотрены вызовы цифровой экономики в контексте угроз, которые имеют растущие последствия для национальной безопасности. Анализируются правила международной торговли, связанные с цифровой безопасностью. Предложены новые подходы по обеспечению баланса интересов мировой торговли и национальной безопасности.*

Ключевые слова: *цифровая экономика, национальная безопасность, торговля, ИТ-товары и услуги, мировая торговая система, ВТО, цепочки создания стоимости.*

Введение. Цифровые технологии значительно изменили образ жизни человечества. Эффективность работы как государственного, так и частного секторов зависит от устойчивой цифровой инфраструктуры, которая облегчает трансграничные потоки данных. Стремительное развитие «умных городов» в сочетании с прогрессом в области интернета вещей и искусственного интеллекта все больше трансформирует социальную и экономическую деятельность в данные, что, в свою очередь, порождает новые формы уязвимостей: умножение рисков цифровой безопасности.

Основная часть. В нашей повседневной жизни поставщики цифровых технологий – от производителей мобильных телефонов до платформ социальных сетей – имеют возможность настраивать аппаратное или программное обеспечение таким образом, чтобы получать доступ к компьютерным системам в обход стандартных механизмов безопасности. На национальном уровне угрозы цифровой безопасности стали серьезной проблемой для стран. В частности, критически важная инфраструктура все чаще, если не исключительно, контролируется компьютерами [1]. Это значительным образом влияет не только на само техническое обеспечение, но также и на экономические процессы и их регулирование в мировой экономике.

Кибератаки могут нанести ущерб критически важной инфраструктуре различными способами, включая, например, прямой контроль над промышленными процессами для блокирования функционирования электростанций, систем распределения воды, транспортных сетей, систем здравоохранения и т.д. [2]. Более того, благодаря относительно низкой стоимости и широкой доступности цифровых технологий, кибер-риски в цепочках поставок критически важных отраслей промышленности воспринимаются как угрозы целостности критически важной инфраструктуры государства, создавая взаимозависимые отношения между цифровой торговлей, экономической и национальной безопасностью. Так, меры, применяемые для обеспечения цифровой безопасности в части, ограничивающей торговлю, включают как торговлю товарами (например, запрет на оборудование Huawei), так и торговлю услугами (например, запрет на TikTok), осуществляемую с помощью цифровых технологий.

Основные геополитические игроки в цифровой экономике принимают все более комплексные меры цифровой безопасности. Так, в США были приняты к реализации комплексы торговых мер по диверсификации цепочек поставок и обеспечению инфраструктурной устойчивости сетей 5G. Следуя инициативам «Чистая сеть» и «Чистый путь», Федеральная комиссия по связи (FCC) опиралась на основания национальной безопасности, чтобы ограничить американские телекоммуникационные компании в использовании вплоть до исключения из оборота оборудование Huawei (например, вышки сотовой связи) и сервисы (например, облачные сервисы) из своих сетей [3], затребовать удаление TikTok в магазинах приложений у цифровых платформ США [4]. С другой стороны, признавая, что цифровые технологии представляют собой уязвимую мишень, Европейский союз (ЕС) принял комплекс мер, которые направлены на достижение разнообразия среди поставщиков и сокращение участия китайских компаний (особенно Huawei) во внедрении 5G [4], а также предложен Закон ЕС о «киберустойчивости» для обеспечения более защищенных аппаратных и программных продуктов. Эти меры могут существенно изменить конъюнктуру мировых рынков ИТ-товаров.

В то же время режим цифровой безопасности Китая стал еще более сложным и строгим с тех пор, как был введен в действие соответствующий закон от 1 июля 2017 г. Zhonghua Renmin Gongheguo Wanglao Anquan Fa

(China's Cybersecurity Law). Широкая сфера применения и расплывчатые формулировки этого дают правительству еще большую свободу действий для реализации своих политических и экономических программ. Например, приняты ограничения на иностранные товары и услуги в области информационных технологий (ИТ) на основе потенциальных рисков национальной безопасности, связанных с надежностью цепочек поставок. Более того, Закон Китая о криптографии от 1 января 2020 г. Zhonghua Renmin Gongheguo Mima Fa (China's Cryptography Law) также содержит правила, ограничивающие торговлю коммерческими продуктами шифрования, которые связаны с национальной безопасностью. Неоднозначно определенные «продукты шифрования», охватывающие широкий спектр товаров и услуг в области ИТ, должны в обязательном порядке проходить оценку рисков кибербезопасности.

Учитывая международную практику, торговые ограничения, основанные на цифровой безопасности, потенциально могут вступать в противоречие с правилами международной торговли во многих отношениях, как на уровне Всемирной торговой организации (ВТО), так и на уровне соглашений о свободной торговле (ССТ). Запреты на ИТ-товары и услуги в конкретных странах могут нарушать принцип наибольшего благоприятствования, который, как правило, запрещает дискриминацию между «похожими» товарами из разных стран (ГАТТ, ст. I, ГАТС, ст. II). Вероятно, основные конкуренты Huawei из Европы (Nokia и Ericsson) и Южной Кореи (Samsung) получат выгоду от запрета Huawei в США. Меры кибербезопасности также могут быть несовместимы с обязательствами по национальному режиму, если отечественный ИТ-товар или услуга и запрещенный иностранный товар или услуга являются «подобными» продуктами или услугами (ГАТТ, ст. III, ГАТС, ст. XVII). В случаях, когда стандарты цифровой безопасности представляют собой технические регламенты, уникальные стандарты кибербезопасности, которые предоставляют импортируемым продуктам менее благоприятный режим, чем тот, который предоставляется «аналогичным» продуктам национального происхождения, также могут нарушать обязательства по недискриминации (Соглашение о технических барьерах в торговле, ст. 2.1). Более того, положения о недискриминации в главах ССТ, касающихся электронной торговли/цифровой торговли в цифровом формате, также требуют от стран обеспечивать недискриминационный режим в отношении «аналогичных» цифровых продуктов, например в ст. 19.4 Соглашения между Соединенными Штатами, Мексикой и Канадой от 30 ноября 2018 г., ст. 14.4. Всеобъемлющего и прогрессивного соглашения о Транстихоокеанском партнерстве от 30 декабря 2018 г.

Более того, с точки зрения доступа на рынки меры цифровой безопасности могут одновременно представлять собой количественные ограничения на международную торговлю товарами и нарушать обязательства по устранению количественных ограничений (ГАТТ, ст. XI) и доступу на рынки для торговли услугами (ГАТС, ст. XVI). Так, китайская сторона воспользовалась возможностью мировой торговой системы и открыла спор в арбитраже ВТО о нарушении обязательств США в отношении рекламы, развлечений и аудиовизуальных услуг по итогам запретов китайских программ Tik Tok, WeChat, Moves.

Заключение. В век цифровой экономики коммерческие интересы и интересы кибербезопасности тесно переплетены. Из этого вытекают фундаментально сложные вопросы с юридической, технологической и экономической точек зрения: в какой степени опасения по поводу кибербезопасности законны, каким образом они меняют глобальное производство и цепочки создания стоимости, как найти баланс между национальной безопасностью и незаконными протекционистскими мерами, вытекающих из неконкурентных методов торговой политики. Это особенно важно, поскольку правительства переходят к подходам, основанным на оценке рисков для защиты цифровой безопасности. Такой подход предоставляет национальным регулирующим органам гибкость в поощрении инноваций, с другой стороны – сопряжен с опасностью злоупотребления полномочиями по принятию решений. Одним из возможных будущих направлений управления торговлей и кибербезопасностью видится тщательное изучение различия между критической и некритической инфраструктурой. Это могло бы послужить маркером для определения границ интересов безопасности и полезным инструментом для отсеивания чрезмерного обобщения заявлений о национальной безопасности. В конечном счете, может быть поддержан более справедливый баланс между свободной торговлей и национальной, и, в частности, цифровой, безопасностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Good Governance for Critical Infrastructure Resilience [Электронный ресурс]. OECD: 2019. – Режим доступа: https://www.oecd-ilibrary.org/sites/02f0e5a0-en/1/1/4/index.html?itemId=/content/publication/02f0e5a0-en&_csp_=eb11192b2c569d5c3d1424677826106a&itemIGO=oecd&itemContentType=book. – Дата доступа: 31.01.2024.

2. Панин, Д.Н. Анализ кибератак на критическую информационную инфраструктуру с IoT технологиями / Д.Н. Панин, Е.О. Бобков, Е.А. Балашова // [Электронный ресурс]: Автономия личности. – 2020. – №2 (22). – Режим доступа: https://cyberleninka.ru/article/n/analiz-kiberatak-na-kriticheskuyu-informatsionnuyu-infrastrukturu-s-iot-tehnologiyami – Дата доступа: 31.01.2024.

3. FCC Bans Sale of New Devices from Chinese Companies Huawei, ZTE and Others / E. Graham // [Электронный ресурс]: The Center for Security and Emerging Technology. – 2022. – Нояб. 28. – Режим доступа: https://cset.georgetown.edu/article/fcc-bans-sale-of-new-devices-from-chinese-companies-huawei-zte-and-others/. – Дата доступа: 31.01.2024.

4. FCC Commissioner Calls on Apple and Google to Remove TikTok from Their App Stores / B.Fung // [Электронный ресурс]: CNN – 2022. – Июнь 29. – Режим доступа: https://www.cnn.com/2022/06/29/tech/fcc-google-apple-tiktok-block/index.html. – Дата доступа: 31.01.2024.
5. Cybersecurity of 5G networks – EU Toolbox of risk mitigating measures [Электронный ресурс]. European Commission: 2020. – Режим доступа: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=64468. – Дата доступа: 31.01.2024.

УДК 338.984

ЦИФРОВИЗАЦИЯ КАК СРЕДСТВО ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ

соискатель В.Е.Шолоник, УП «Мингаз», г. Минск

Резюме. *Информационные технологии и инновации активно внедряются в производственные процессы. Разрабатываются многочисленные управленческие информационные инструменты для их реализации. Анализируя процессы цифровизации на предприятиях, необходимо определить понятие «цифровая трансформация». Цифровая трансформация – это технологии, которая постепенно проникает в производственные процессы и, как следствие, оказывает влияние на экономическое развитие предприятий.*

Ключевые слова: *экономика, цифровизация, производство, технологии, цифровая трансформация, организационная структура, показатели эффективности.*

Введение. Цифровизация, или цифровая трансформация, является одним из ключевых факторов развития современного общества. Этот процесс влияет на все сферы жизни – от экономики и образования до здравоохранения и государственного управления.

Цифровая трансформация в настоящее время рассматривается в качестве приоритетного направления развития экономики. Создать условия для развития инструментов цифровой экономики планируется в ходе реализации мероприятий Государственной программы «Цифровое развитие Беларуси» на 2021-2025 годы (далее – Государственная программа). [1]

В рамках мероприятий Государственной программы, направленных на цифровую трансформацию производственных процессов и управления ими, предусматривается выполнение реинжиниринга и оптимизации бизнес-процессов отечественных предприятий с использованием передовых производственных технологий, соответствующих концепции «Индустрия 4.0».

Основная часть. Термин «Цифровая трансформация» (далее – ЦТ) определяет трансформацию системы управления (менеджмента) путем пересмотра целей и стратегий бизнеса, организационной структуры, функций, продуктов, маркетинга под давлением цифровых технологий.

Несмотря на многочисленные публикации и разговоры о ЦТ, у нее нет четкого определения и тем более научной основы, а большинство рассуждений остаются умозрительными.

Интенсивность изменений, которые мы не успеваем понять, не сможем и контролировать. Это значит, что процесс развития современного общества под давлением передовых технологий практически неуправляемый и может привести к масштабным кризисам, как в экономике, так и в социальной среде, в политике.

Тема четвертой промышленной революции и ЦТ назревала во многих научных публикациях на протяжении последнего десятилетия, но началом широкого публичного обсуждения она стала после речи известного швейцарского экономиста Клауса Мартина Шваба, основателя и президента ВЭФ, на форуме в Давосе 20 января 2016 года. Выступление Шваба было основано на материалах его статьи в журнале «Foreign Affairs», в которой он сформулировал фактически провокационные утверждения и сделал ряд жестких и спорных прогнозов, пообещав значительные социальные потрясения. Впоследствии более подробное толкование своих идей Клаус Шваб в соавторстве с Николасом Дэвисом раскрыл в книге «Технологии четвертой промышленной революции» (Shaping The Fourth Industrial Revolution. Эксмо, 2018, ISBN 978-5-04-095565-7). [2].

В своей книге «Четвертая промышленная революция» Клаус Шваб, рассуждая о технологиях «Индустрии 4.0», отмечает, что «некоторые представители научных кругов и профессиональных сообществ считают рассматриваемые процессы изменений всего лишь составляющей частью третьей промышленной революции». Тем не менее, по его мнению, самостоятельность четвертой промышленной революции можно обосновать тремя факторами: темпы развития, широта и глубина, системное воздействие.

В контексте рассматриваемого вопроса слово «революция» следует трактовать как резкое изменение или бурное развитие. Причем, предпосылки для подобных изменений могут формироваться в течение достаточно длительного периода. Для каждой из произошедших промышленных революций формировались свои причины. Но, несмотря на различные предпосылки и используемые технологии, все прошедшие промышленные революции объединены одним – осуществлением новых комбинаций экономических ресурсов. По мнению Йозефа Шумпетера процесс развития осуществляется посредством нахождения таких новых комбинаций [3].

В широком смысле под новыми комбинациями экономических ресурсов следует понимать не что иное, как инновации. При этом субъект, внедряющий эти инновации в свою производственную деятельность, обеспечивает себе значительно более устойчивое финансовое положение, которое может выражаться в двух аспектах: получении дополнительной выручки или снижении затрат. И в первом, и во втором случаях происходит повышение эффективности экономики.