

ISSN 2523-4714

УДК 338.242

В. Б. Криштаносов

Белорусский государственный технологический университет, Минск, Беларусь

РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ЭКОНОМИКИ: ОПЫТ РЕСПУБЛИКИ БЕЛАРУСЬ

Отмечены институциональные основы формирования цифровой экономики в Республике Беларусь, включая законодательные и организационные составляющие. Выделены факторы рисков и угроз цифровизации экономики для национальной экономической безопасности Республики Беларусь, а также актуальные тенденции развития цифровой инфраструктуры. Представлен комплекс мероприятий, направленных на дальнейшее продвижение цифровизации экономики страны.

Ключевые слова: цифровая экономика, государственное регулирование, защита персональных данных, кибербезопасность, государственно-частное партнерство

Для цитирования: Криштаносов, В. Б. Регулирование цифровой экономики: опыт Республики Беларусь / В. Б. Криштаносов // Бизнес. Инновации. Экономика : сб. науч. ст. / Ин-т бизнеса БГУ. — Минск, 2022. — Вып. 6. — С. 60–70.

V. Kryshtanosau

Belarusian State Technological University, Minsk, Belarus

REGULATION OF THE DIGITAL ECONOMY: EXPERIENCE OF THE REPUBLIC OF BELARUS

The institutional foundations for the formation of the digital economy in the Republic of Belarus, including legislative and organizational components, are noted. Based on the analysis, the factors of risks and threats of digitalization of the economy for the national economic security of the Republic of Belarus, as well as current trends in the development of digital infrastructure, are identified. It was presented a set of measures aimed at further promoting the digitalization of the country's economy.

Keywords: digital economy, state regulation, personal data protection, cybersecurity, public-private partnership

For citation: Kryshtanosau V. Regulation of the digital economy: experience of the Republic of Belarus. *Biznes. Innovatsii. Ekonomika = Business. Innovations. Economics*. Minsk, 2022, iss. 6, pp. 60–70 (in Russian).

Введение

В условиях растущих неопределенностей, рисков и угроз экономической безопасности на фоне стремительной цифровизации национальной экономической системы Республика Беларусь стремится к осуществлению амбивалентной политики, направленной, с одной стороны, на стимулирование технологических инноваций, с другой — на обеспечение безопасности их внедрения. При этом уровень проникновения и гетерогенный характер цифровых систем, их сложность и комплексность воздействия на экономику страны мотивируют регуляторов и национальное правительство к выстраиванию международного взаимодействия, привлечению опыта и компетенций на уровне экспертного сообщества, наднациональных институтов и наиболее продвинутых в технологическом развитии государств.

Цель работы — выделить теоретические подходы, связанные с регулированием цифровой экономики, и их адаптацию в Республике Беларусь с учетом национальной специфики и влияния современных вызовов и угроз.

Государственное регулирование цифровизации экономики включает в себя такие элементы, как:

- разработка и установление норм и стандартов управления и планирования исследовательским процессом;
- разработка и установление правил, регулирующих создание цифровых инноваций и функционирование инновационной экосистемы;
- финансирование исследований и цифровых инноваций;
- разработка и внедрение процедур оценки экономического потенциала новых технологий и ее результативности на всех уровнях и этапах;
- предоставление сертификатов качества;
- содействие сотрудничеству между государственным и частным секторами на всех уровнях;
- поддержка образования и обучения.

Распространение мировых тенденций цифровизации затрагивает Республику Беларусь, ее экономическое развитие, конкурентоспособность как продукции, так и экономики в целом, проблематику обеспечения экономической безопасности, связанную с внедрением новых технологий в ключевые сферы жизнедеятельности государства [1].

Важным институциональным элементом регуляторной среды является созданный в 2005 г. Парк высоких технологий (ПВТ), который представляет собой особую экономическую зону, способствующую благоприятному развитию IT-бизнеса, со специальным налогово-правовым режимом. Фактически ПВТ — это инновационный кластер, резиденты которого занимаются разработкой программных продуктов и предоставлением IT-услуг.

17 декабря 2017 г. Президентом Республики Беларусь был подписан Декрет № 8 «О развитии цифровой экономики» [1], цель которого — создание условий для привлечения мировых IT-компаний в Беларусь, открытия ими своих представительств, центров разработок и создания конкурентоспособного высокотехнологического цифрового продукта (услуги) с высокой добавленной стоимостью. Кроме того, задачами документа являлось обеспечение инвестиций в будущее (IT-кадры и образование) и внедрение новейших финансовых инструментов и технологий, включая блокчейн и криптовалюты.

В целях институционального развития цифровизации национальной экономики, осуществления общей координации данной деятельности в 2018 г. был создан Совет по развитию цифровой экономики¹, организационное и информационное обеспечение деятельности которого осуществляется Министерством связи и информатизации.

В апреле 2020 г. Советом Министров принято распоряжение о переводе некоторых административных процедур для юридических лиц и индивидуальных предпринимателей в разряд «цифровых» через единый портал электронных услуг². Создана Белорусская интегрированная сервисно-расчетная система (БИСРС) — комплекс информационных систем и ресурсов, предназначенный для оказания пользователям (физическим и юридическим лицам) государственных услуг и административных процедур в электронной форме с применением идентификационных карт (ID-карт).

В феврале 2021 г. Советом Министров Республики Беларусь была принята государственная программа «Цифровое развитие Беларуси» на 2021–2025 гг., направленная на внедрение передовых информационных технологий в отрасли национальной экономики и сферы жизнедеятельности общества. Программой предусматривается выполнение мероприятий по созданию (развитию) современной информационно-коммуникационной инфраструктуры, внедрению цифровых инноваций в отрасли экономики и технологий Smart City (умных городов) [2]. Программа предполагает охват к 2025 г. 17 городов и регионов [3].

¹ О создании Совета по развитию цифровой экономики : постановление Совета Министров Республики Беларусь, 28 февр. 2018 г., № 167. — URL: <https://etalonline.by/document/?regnum=C21800167> (дата обращения: 26.06.2021).

² Единый перечень административных процедур, осуществляемых государственными органами и иными организациями в отношении юридических лиц и индивидуальных предпринимателей, утвержден постановлением Совмина № 156 от 17 февраля 2012 г. Речь идет о 147 процедурах. Предполагается, что они станут электронными в 2020–2024 гг.

Ожидается, что в результате реализации Государственной программы будет создано не менее семи государственных цифровых платформ, которые могут выступить в качестве типовых¹. В процессе реализации Государственной программы предполагается проведение следующих мероприятий:

- оцифровка данных — создание отсутствующих (недостающих) государственных информационных ресурсов;
- разработка унифицированных протоколов обмена данными в едином формате, протоколов межведомственного (межплатформенного) взаимодействия;
- развитие функционирующих и создания новых государственных информационных систем как сервисов государственной цифровой платформы — полноценный переход к микро-сервисной архитектуре;
- формирование государственной цифровой информационной экосистемы, построенной на базе государственных цифровых платформ, взаимодействующих между собой в автоматизированном режиме [2].

На базе ОАО «ЦНИИТУ» в рамках реализации промышленной политики организуется центр компетенций цифровой трансформации промышленности Республики Беларусь, который будет формировать подходы и основные направления развития предприятий республики на этапах внедрения концепции «Индустрия 4.0» [4]. В рамках мероприятий, 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», включая:

- создание «цифровых двойников» технологических и бизнес-процессов, выпускаемой (планируемой к производству) продукции;
- внедрение платформенных решений для управления производством, активами предприятий, обеспечения накопления и обработки данных в режиме реального времени, использования систем поддержки принятия решений, инструментов предсказательной и отчетной аналитики;
- развитие современных инструментов работы с заказчиками и поставщиками, каналов продвижения продукции и взаимодействия с клиентами.

Указом Президента Республики Беларусь № 107 от 16 марта 2021 г. «О биометрических документах» в целях дальнейшего совершенствования порядка документирования населения Республики Беларусь, осуществления административных процедур и оказания услуг населению в условиях формирования электронного правительства и цифровой экономики введены в действие биометрические документы, удостоверяющие личность, и биометрические документы для выезда из Республики Беларусь и (или) въезда в Республику Беларусь, содержащие биометрические и иные персональные данные².

С учетом интегрированности белорусской экономики и цифровой экосистемы в международную среду проблема кибербезопасности будет иметь нарастающее влияние на экономику Беларуси. Базовым законодательным актом регулирования вопросов информационной безопасности в Республике Беларусь стало принятие 10 ноября 2008 г. Закона «Об информации, информатизации и защите информации» № 453. Данный законодательный акт устанавливает основы политики государственного регулирования в области информации, информатизации и защиты информации.

¹ Государственная цифровая платформа — комплекс программно-технических средств, обеспечивающий использование информационных ресурсов и функционирующих на них сервисов значительным количеством субъектов информационных отношений и возможность их взаимодействия на основе единых принципов и по общим правилам, создаваемый и (или) приобретаемый за счет средств республиканского или местных бюджетов, государственных внебюджетных фондов, а также средств государственных юридических лиц.

² О биометрических документах : Указ Президента Респ. Беларусь, 16.03.2021, № 107. — URL: <http://etalonline.by/document/?regnum=p32100107> (дата обращения: 26.06.2021).

В рамках утвержденной в 2019 г. Концепции информационной безопасности Республики Беларусь¹ предложены такие определения в сфере цифровых угроз, как кибератака, кибербезопасность, киберинцидент, кибертерроризм, киберустойчивость. В документе отмечено, что цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели.

Вместе с тем политическая и социально-экономическая сферы, общественная и военная безопасность становятся более уязвимыми перед преднамеренными или случайными технологическими воздействиями. Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Отдельно отмечены угрозы и риски незаконного и необоснованного вмешательства в частную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и избыточное профилирование.

В качестве наиболее вероятных источников угроз кибербезопасности рассматриваются отказы технических средств и сбои программного обеспечения в информационных и телекоммуникационных системах, противоправная деятельность отдельных лиц и преступных групп, преднамеренные действия и ошибки персонала информационных систем, выражающиеся в нарушении установленных регламентов их эксплуатации и правил обработки информации, зависимость Беларуси от других стран — производителей программных и аппаратных средств при создании и развитии информационной инфраструктуры².

В 2019 г. Национальным банком Республики Беларусь утверждена Концепция обеспечения кибербезопасности в банковской сфере³, направленная на обеспечение кибербезопасности банков, небанковских кредитно-финансовых организаций, ОАО «Банк развития Республики Беларусь». Данный документ вводит понятие «киберриск» в отношении банковской деятельности и обозначает «потенциальную возможность (вероятность) для банка, Национального банка понести потери (убытки), иные дополнительные затраты, не получить запланированные доходы вследствие противоправных действий лица либо группы лиц, совершенных посредством использования информационных технологий, в целях несанкционированного доступа к объектам информационной инфраструктуры банка, Национального банка и направленных на нарушение конфиденциальности, целостности, доступности, подлинности и сохранности защищаемой информации». Среди основных отраслевых киберугроз выделяются: воздействие через аппаратные уязвимости, компьютерный шпионаж, целенаправленные кибератаки, клиентоориентированные кибератаки.

В соответствии с мировыми тенденциями государственной защиты цифровых персональных данных 7 мая 2021 г. в Республике Беларусь принят новый Закон «О защите персональных данных» № 99-З [5]. Аналогично европейскому регулированию сферы защиты персональных данных (GDPR) белорусское законодательство вводит новые требования для обработки цифровых персональных данных, включая:

- назначение лица или отдела, ответственного за защиту данных;
- разработку политики компании в отношении обработки данных и предоставление доступа к ней для неограниченного круга лиц;
- обучение сотрудников работе с персональными данными и др. [6].

¹ О Концепции информационной безопасности Республики Беларусь : постановление Совета Безопасности Респ. Беларусь, 18 марта 2019 г., № 1. — URL: <https://pravo.by/document/?guid=3961&p0=P219s0001> (дата обращения: 26.06.2021).

² Там же.

³ Концепция обеспечения кибербезопасности в банковской сфере : постановление Правления Национального банка Респ. Беларусь, 20 нояб. 2019 г., № 466. — URL: <https://www.nbrb.by/legislation/documents/konceptsiya-kiberbezopasnosti.pdf> (дата обращения: 04.04.2021).

Государственное институциональное регулирование и управление в области информации, информатизации и защиты информации осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, НАН Беларуси, Оперативно-аналитическим центром при Президенте Республики Беларусь, Министерством связи и информатизации Республики Беларусь, иными государственными органами в пределах их компетенции [7].

Уполномоченным органом по управлению сетью электросвязи общего пользования в Республике Беларусь является оперативно-аналитический центр (ОАЦ) при Президенте Республики Беларусь [7], который осуществляет регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий¹.

При оценке рисков в сфере информационной безопасности ОАЦ руководствуется методологией, основанной на отдельных критических показателях уровня вероятного ущерба по пяти основным сферам: политической, экономической, социальной, информационной и экологической². В экономической плоскости в качестве критериев оценки информационного объекта выделен потенциальный ущерб более 100 тыс. базовых величин, для расчетных банковских систем и энергосистем – прекращение или нарушение функционирования на период более двух часов.

Уполномоченным правоохранительным органом по борьбе с киберпреступностью является Главное управление МВД по противодействию киберпреступности («Управление К»). По его данным в 2020 г. в Беларуси зарегистрировано свыше 25,5 тыс. киберпреступлений с нарастающей динамикой, к уголовной ответственности привлечены 1 592 чел. Пострадавшими от данного вида преступлений в Беларуси в 2020 стали около 100 тыс. чел.³ Основными видами киберпреступлений, по данным правоохранительных органов⁴, являлись шифрование коммерческой информации, подмена реквизитов при переводе средств, фишинговые письма.

Вместе с тем проведенный анализ показал необходимость учета следующих факторов для оценки рисков и угроз цифровизации экономики для национальной экономической безопасности Республики Беларусь.

1. Финансово-экономические:

- наличие жестких ограничений в сфере располагаемых финансовых ресурсов для внедрения новых технологий в сфере цифровизации. Сложность и высокая стоимость внедрения технологий выступают в качестве барьера для их принятия;
- нарастающее давление на внешних и внутренних конкурентных рынках как для традиционных национальных отраслей, так и в инновационных сферах предоставления услуг и высокотехнологического производства, которые меняют структуру международной торговли.

2. Технологические:

- низкий уровень используемой ИТ-инфраструктуры и соответствующих компетенций на уровне предприятий;
- неразвитая инновационная инфраструктура;
- недостаточная защищенность внутренней ИКТ инфраструктуры перед угрозой киберпреступности. Дополнительные проблемы обеспечения конфиденциальности, безопасности, договорные риски и риски технологического соответствия, связанные с аутсорсингом услуг в сфере ИКТ.

¹ Оперативно-аналитический центр при Президенте Республики Беларусь. – URL: <https://oac.gov.by/info> (дата обращения: 26.06.2021).

² О показателях уровня вероятного ущерба национальным интересам Республики Беларусь : приказ Оперативно-аналитического центра при Президенте Респ. Беларусь, 20 февр. 2020 г., № 65. – URL: <https://pravo.by/document/?guid=3961&p0=T62004469> (дата обращения: 26.06.2021).

³ Необходима надежная защита от киберпреступности. – URL: <https://www.sb.by/articles/informatsiya-bez-opasnosti3445.html> (дата обращения: 26.06.2021).

⁴ Главное управление по противодействию киберпреступности КМ МВД РБ предупреждает. – URL: <https://www.mrik.gov.by/glavnoe-upravlenie-po-protivodejstviyu-kiberprestupnosti-km-mvd-rb-preduprezhdaet> (дата обращения: 26.06.2021).

3. Управленческие:

- недостаточная поддержка и понимание необходимости внедрения цифровых технологий на уровне руководства предприятий и организаций;
- возрастающее значение государственно-частного партнерства в разрезе необходимости эффективного внедрения цифровых технологий в сферы госуправления.

4. Социально-образовательные: отсутствие системного подхода к подготовке, обучению населения использованию ИТ-технологий как на уровне государства, так и предприятий традиционных отраслей. Базовые навыки программирования, аналитика больших данных способствуют внедрению цифровых технологий.

5. Системно-организационные:

- наличие общей концепции цифровизации (стратегический подход) и плана мероприятий (операционный подход). Оценка эффективности принимаемых управленческих решений по внедрению цифровых технологий. Стоимость внедрения;
- низкая вовлеченность МСП в инновационную деятельность;
- низкая коммерциализация проектов.

6. Политические: в контексте текущей политико-экономической ситуации в стране возрастает вероятность осуществления хакерских атак или DDoS-атак во имя «социальной справедливости» и/или «возмездия» в отношении отдельных организаций, государственных институтов, а также инсайдерские угрозы, создаваемые недовольными сотрудниками, включают в себя использование доступа к внутренней системе и учетным данным или «социальную инженерию» для получения конфиденциальной информации либо нарушения стабильного функционирования ИТ-систем организаций.

Среди факторов, определяющих актуальные тенденции развития цифровой инфраструктуры в Республике Беларусь, следует выделить:

- политический кризис в стране;
- COVID-19;
- сложную макроэкономическую ситуацию;
- ужесточение государственного регулирования сектора ИТ;
- санкционную политику со стороны ЕС, США, Великобритании не только в отношении Беларуси, но и Российской Федерации.

С учетом обозначенных факторов, определяющих текущий этап формирования цифровой регуляторной среды, представляется целесообразным совершенствование в Республике Беларусь институционального механизма, направленного на реализацию национальных интересов в сфере цифровизации, обеспечение управления цифровыми рисками с точки зрения устойчивости развития экономики.

Институциональная основа организационного механизма государственного регулирования данной сферы может быть представлена «Министерством цифровизации», имеющим соответствующие компетенции по трансформации и интеграции цифровых систем, которые включают в себя:

- разработку и внедрение системы формализации оценки цифровых рисков (совместно с ОАЦ);

- обеспечение последующего мониторинга рисков цифровых технологий (совместно с ОАЦ). Это позволит на следующих этапах осуществлять реинжиниринг процессов и переподготовку сотрудников, используя гибкие подходы в управлении. Автоматизация данных процессов позволит внедрить новый инструментарий с меньшими затратами, а также обеспечить раннее выявление и устранение угроз и рисков;

- использование «упреждающего регулирования», предполагающего выявления изменений в окружающей экосреде на ранних этапах для их учета при формировании текущих и будущих стратегий регулирования;

- выявление любых противоречивых целей, нормативных проблем и препятствий эффективного внедрения и использования новых технологий, а также формирование предложений по их решению.

Для управления рисками представляется целесообразным использование поэтапной модели цифровой трансформации, где на первом этапе осуществляется цифровое зондирование и формирование цифровых сценариев для подготовки цифрового исследования и соответствующей формализации. На втором этапе требуется осуществление разработки прототипов для последующего масштабирования наиболее эффективных практик, а также вырабатываются принципы и пределы стратегической гибкости для первичной реализации цифровых возможностей. Третий этап — непосредственная трансформация — предполагает управление инновационными экосистемами, реинжиниринг внутренней среды, включая инфраструктуру и административные процессы, а также управление персоналом и развитие цифровых компетенций.

Финансирование комплекса мероприятий возможно осуществлять за счет Белорусского инновационного фонда¹ (первый и второй этапы), а также собственных средств отраслей и предприятий, участвующих в программе трансформации (третий этап).

Кроме того, важнейшим аспектом успешной реализации государственных программ является создание системных горизонтальных и вертикальных связей как на уровне компетентных органов государственного управления, так и привлеченных организаций в рамках государственно-частного партнерства. На низовом уровне представляется целесообразным формирование специализированной управленческой структуры, состоящей из ответственных за минимизацию рисков цифровой трансформации сотрудников на уровне отраслей и конкретных предприятий, для подготовки (переподготовки) которых целесообразно создание Национального центра цифровых компетенций (возможно на базе ОАО «ЦНИИТУ»).

В рамках институционализации регулирования цифровой трансформации, формирования регуляторной экосистемы на уровнях разработки общей стратегии цифровизации, защиты киберпространства, финансового рынка и отдельных цифровых инноваций и концепций целесообразны следующие мероприятия:

1. Уровень стратегии цифровизации: обеспечение нормативно-правового регулирования в области цифрового развития, включая:

1.1. разработку долгосрочной (горизонт планирования 20–30 лет) стратегии национальной цифровой трансформации, соответствующих политик и нормативных актов, направленных на обеспечение комплексного и безопасного развития цифровых технологий во всех сферах экономики страны с учетом их взаимосвязей и взаимозависимостей²;

1.2. принятие недискриминационного, технологически нейтрального, принципиального и основанного на оценке риска подхода к регулированию и надзору, который соответствует стандартам соразмерности и прозрачности;

1.3. реализацию политики развития целостных экосистем, которые позволяют оцифровывать все транзакции и взаимодействия между государством, юридическими и физическими лицами.

2. Уровень защиты киберпространства.

2.1. Развитие нормативно-правового и технологического обеспечения национальной кибербезопасности:

2.1.1. обеспечение суверенитета в киберпространстве, предполагающее защиту национальных информационных систем и информационных ресурсов от внешних угроз, вмешательства, атак или ущерба. В настоящее время отдельным законодательным актом вопросы кибербезопасности в Республике Беларусь не регулируются, правовое обеспечение базируется главным образом на концепции информационной безопасности Республики Беларусь и правовых актах ОАЦ;

2.1.2. разработка и принятие закона о национальной цифровой безопасности, который охватывает широкий спектр отраслей и секторов экономики и социальной сферы страны,

¹ В настоящее время в соответствии с постановлением Совета Министров Республики Беларусь от 12.11.1998 № 1739 Белорусский инновационный фонд находится в подчинении Государственного комитета по науке и технологиям Республики Беларусь.

² Примеры таких правил в этой области охватывают законодательство о защите данных (например, GDPR), схемы облачной сертификации.

включая промышленность, сельское хозяйство, строительство, энергетику, коммунальную инфраструктуру, транспорт и коммуникации, а также технико-экономические концепции Smart City, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, Intellectual Transport Systems, E-Commerce, Telemedicine с особым вниманием к проблематике AI, IoT, Cloud Computing, Blockchain, Big Data и пр.;

2.1.3. создание и внедрение национальных программных продуктов, которые направлены на снижение зависимости Беларуси от иностранных поставщиков технологий и цифровых услуг;

2.1.4. разработка и внедрение национальных и стандартов¹ в отношении аккумулирования, хранения, обмена и использования данных, соответствующих принципам безопасности и конфиденциальности, прозрачности, подотчетности, целостности;

2.1.5. законодательное закрепление определения «государство — спонсор киберпреступлений», предполагающее широкое трактование с включением даже тех стран, которые предоставили убежище группам киберпреступников, реализация программы (аналогичной развернутой в США), направленной на финансовое поощрение за предоставление информации о хакерах, в особенности спонсируемых иностранными государствами².

2.2. Обеспечение комплексного операционного реагирования на кибератаки:

2.2.1. разработка планов кризисного реагирования на внешние цифровые угрозы, а также создание единой государственной системы цифрового мониторинга, в том числе в целях аккумулирования данных о зафиксированных кибератаках не только в отношении государственных учреждений, предприятий и объектов критически важной инфраструктуры, но и частных компаний (обязанных сообщать о таких случаях в течение 24 ч);

2.2.2. проведение формализованного описания профилей цифровых угроз (карты цифровых угроз) для последующей разработки соответствующих моделей реагирования, организационно-экономических механизмов, адаптированных к влиянию конкретных факторов и условий;

2.2.3. формирование с учетом опыта Европейского союза специальных ИТ-групп быстрого реагирования на киберинциденты для устранения наиболее опасных взломов цифровых систем;

2.2.4. развитие страхового инструментария обеспечения гарантий исполнения обязательства в отношении рисков, связанных с киберпреступлениями;

2.2.5. введение ответственности в отношении выбора частными предприятиями оптимальных в контексте безопасности технологий³;

2.2.6. разработка и внедрение профессиональных стандартов по кибербезопасности для сотрудников, обеспечивающих защиту цифровых систем объектов критической инфраструктуры⁴.

2.3. Обеспечение кибербезопасности критической инфраструктуры:

2.3.1. разработка стандартов и критериев, выделяющих объекты критически важной инфраструктуры с учетом актуальных международных тенденций. К таковым объектам в Республике

¹ В этом контексте термин «технологический суверенитет» или «цифровой суверенитет» недавно появился в качестве зонтичной концепции для разработки цифровой политики в Европе.

² В США осуществляется программа поощрения анонимных информаторов и «белых хакеров», которые за сообщение о террористах, могут получить награду в криптовалютах. В стране запущена платформа «Rewards for Justice», которая позволяет оставлять анонимные сообщения и получать вознаграждение. При этом одним из способов выплаты таких наград стали криптовалютные переводы. Максимальный размер вознаграждения установлен в 10 млн долл. США. Власти США заинтересованы в получении информации о хакерах, спонсируемых иностранными государствами.

³ Усиление ответственности в рамках гражданско-правового регулирования позволит потребителям как государственным, так и частным потребовать возмещения убытков, понесенных в результате критических сбоев инфраструктуры, нарушения стабильности функционирования чувствительных для потребителей продуктов и услуг. Обеспечение надежной структуры защиты потребителей, которая поддерживает прозрачность и сводит к минимуму риски для конфиденциальности, доступности и целостности данных.

⁴ Например, Банк России инициировал разработку стандарта для специалистов информбезопасности банков, который уже согласован с отраслевым сообществом и находится на стадии обсуждения в Минтруда Российской Федерации.

Беларусь следует относить все системы и активы (как государственные, так и частные) в физической или виртуальной форме, нарушение операционного функционирования или разрушение которых потенциально может оказать существенное воздействие на национальную безопасность страны, включая экономическую;

2.3.2. разработка и имплементация секторальных и индивидуальных повторяющихся системных подходов к выявлению, оценке и управлению рисками кибербезопасности вне зависимости от размера организации, подверженности угрозам или актуального уровня сложности кибербезопасности;

2.3.3. мониторинг на технологическом уровне таких систем, как ИТ, управления производством, киберфизических и подключенных устройств в целом, включая IoT;

2.3.4. подготовка ежегодного специализированного отчета о национальном профиле рисков, отражающем актуальную оценку существующих и прогнозируемых рисков и угроз для национальной безопасности Республики Беларусь в разрезе цифровой трансформации, критической инфраструктуры, а также важнейших механизмов государственного управления и социального обеспечения.

3. Уровень развития цифрового финансового рынка:

3.1. формирование привлекательной среды для внедрения цифровых бизнес-моделей в финансовом секторе (FinTech);

3.2. развитие существующих и создание новых интегрированных финансовых экосистем, предоставляющих высококачественные, дифференцированные и функционально совместимые продукты и услуги;

3.3. содействие развитию безопасных и эффективных цифровых платежных систем, повышающих доступность национальной финансовой системы за счет разработки и создания благоприятной инфраструктуры, правил, продуктов и услуг;

3.4. обеспечение на законодательном уровне проблематики цифровой безопасности в финансовом секторе, включая такие технико-экономические концепции, как: FinTech, CBDC, RTGS, Crowdfunding, Mobile Money, InsurTech, Blockchain, Cryptocurrency, RegTech, цифровая идентификация.

4. Уровень регулирования отдельных цифровых инноваций и концепций (главным образом, в форме государственно-частного партнерства):

4.1. содействие развитию 5G как основы развития цифровой инфраструктуры. Обеспечение и стимулирование разработки и поставки цифровых решений для регионов с низкой технологичной инфраструктурой;

4.2 разработка комплекса цифровых систем и сервисов, интегрированных с национальной системой цифровой идентификации (цифровыми паспортами и ID-картами), обладающих такими характеристиками, как простота, безопасность, надежность и конфиденциальность;

4.3. стимулирование внедрения AI в целях национального развития в таких областях, как промышленность, сельское хозяйство, здравоохранение, энергетика, образование, коммунальное хозяйство, логистика и транспорт, государственное управление с поступательным переходом к полноценной реализации концепций, включая: «Smart City», «Industry 4.0», «Agriculture 4.0», «Smart Supply Chain», «Smart Grid», «Intellectual Transport Systems», «E-Commerce», «Telemedicine», «E-Government»;

4.4. разработка национального законодательства, направленного на обеспечение безопасности технологий AI, сведение к минимуму алгоритмической предвзятости при создании и продаже продуктов и услуг на базе AI, обеспечение этических стандартов и структур управления, направленных на повышение их надежности, прозрачности, объяснимости, справедливости (при этом следует учитывать опыт ЕС по внедрению рискоориентированного подхода к использованию AI в различных отраслях и сегментах экономики). Представляется целесообразным на законодательном уровне ввести дифференцированное регулирование норм и стандартов внедрения AI в зависимости от возможного размера угроз и рисков, а также запрет на использование его в прямом управлении критическими важными для национальной безопасности системами;

4.5. создание национальной лаборатории AI/ML;

4.6. повышение цифровых навыков населения, развитие учебных программ и платформ образовательных технологий, направленных на противодействие тенденциям высвобождения малопродуктивной рабочей силы в условиях цифровой трансформации экономики¹.

Выводы

Система государственного регулирования цифровой экономики Республики Беларусь хоть и с опозданием, но адаптирует действующие механизмы управления к современным требованиям и угрозам в сфере цифровизации. От централизованной формы государственного управления цифровой экономикой Республика Беларусь поступательно движется к смешанной, используя механизмы государственно-частного партнерства.

В качестве эффективных мер продвижения цифровизации экономики, представляется целесообразным использовать следующий комплекс мероприятий:

1) для государственного сектора и национальной политики цифровизации:

- создание Совета ЕАЭС по цифровым технологиям с учетом опыта интеграции цифровых систем ЕС и стран Центральной и Восточной Европы;
- создание гармонизированной цифровой деловой среды в ЕАЭС;
- стимулирование обмена передовым опытом внедрения цифровых технологий;
- ускорение оцифровки государственных услуг, поступательное формирование интегрированной цифровой платформы в рамках концепции E-Government, формирование технологических и правовых условий для развития рынка деперсонализированных цифровых данных (с учетом практики ЕРИП²);

2) коммерческого сектора:

- развитие цифровой экосистемы как для сектора ИКТ, так и традиционных отраслей;
- стимулирование цифровизации МСП;
- повышение доступности финансирования на ранних стадиях для стартапов;
- поддержка развития технологических кластеров в целях ускорения внедрения цифровых технологий;
- повышение операционной эффективности традиционных отраслей (внедрение цифровых приложений и каналов распространения, использование аналитики больших данных и искусственного интеллекта, реализация улучшенной ИТ-архитектуры);
- стимулирование трудовой ИТ-миграции в страну;

3) сектора среднего, высшего и послевузовского образования:

- на уровне среднего образования — реализация государственных проектов внедрения обучающих программ знакомства с цифровыми технологиями;
- расширение обучающих программ для сектора ИКТ в системе высшего образования;
- реализация программ переобучения и повышения квалификации.

Список использованных источников

1. О развитии цифровой экономики [Электронный ресурс]. — Режим доступа: <https://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0>. — Дата доступа: 23.04.2021.
2. Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы [Электронный ресурс]. — Режим доступа: <https://www.mpt.gov.by/ru/news/04-02-2021-6992>. — Дата доступа: 16.04.2021.
3. Шорр, Е. Проект «умные города Беларуси». Нормативные и организационные составляющие. Презентация Минсвязи РБ [Электронный ресурс] / Е. Шорр // ITU Forum, 2021. — Режим доступа: <https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2021/Minsk-SSC/ITU%20Forum%2016%20Mar%202021%20-%20Elena%20Shorr.pdf>. — Дата доступа: 26.06.2021.

¹ В отношении среднего образования следует учесть опыт России, в которой Минцифры подготовило программу бесплатного изучения языков программирования на 2-летних курсах учениками 8–11 классов школ с 2022 г.

² С 1 октября 2021 г. ЕРИП на платной основе предоставляет данные о клиентах, их представителях с целью обновления (актуализации) данных.

4. Проект Концепции Государственной программы «Цифровое развитие Беларуси на 2021–2025 гг. [Электронный ресурс]. – Режим доступа: https://www.mpt.gov.by/sites/default/files/proekt_koncepcii_gosudarstvennoy_programmy.pdf. – Дата доступа: 04.04.2021.

5. Шакель, Н. Новые подходы к защите персональных данных с 15 ноября 2021 года. Комментарий к Закону от 07.05.2021 № 99-З «О защите персональных данных» [Электронный ресурс] / Н. Шакель. – Режим доступа: <https://bii.by/tx.dll?d=456664>. – Дата доступа: 14.04.2021.

6. E-commerce в условиях нового Закона о персональных данных. Чек-лист для ритейлеров [Электронный ресурс]. – Режим доступа: <https://belretail.by/news/e-commerce-v-usloviyah-novogo-zakona-o-personalnyih-dannyih>. – Дата доступа: 25.05.2021.

7. Лукашенко утвердил изменения в закон об электросвязи – новации касаются и угроз нацбезопасности [Электронный ресурс]. – Режим доступа: <https://www.belta.by/president/view/lukashenko-utverdil-izmeneniya-v-zakon-ob-elektrosvyazi-novatsii-kasajutsja-i-ugroz-natsbezopasnosti-442675-2021>. – Дата доступа: 24.05.2021.

References

1. About the development of the digital economy. Available at: <https://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0> (accessed 23 April 2021) (in Russian).

2. State program «Digital Development of Belarus for 2021–2025». Available at: <https://www.mpt.gov.by/ru/news/04-02-2021-6992> (accessed 16 April 2021) (in Russian).

3. Shorr E. Smart cities project in Belarus. Regulatory and organizational components. Presentation of the Ministry of Communications of the Republic of Belarus. ITU Forum, 2021. Available at: <https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2021/Minsk-SSC/ITU%20Forum%2016%20Mar%202021%20-%20Elena%20Shorr.pdf> (accessed 26 June 2021) (in Russian).

4. Draft Concept of the State Program «Digital Development of Belarus for 2021–2025». Available at: https://www.mpt.gov.by/sites/default/files/proekt_koncepcii_gosudarstvennoy_programmy.pdf (accessed 4 April 2021) (in Russian).

5. Shakel N. New approaches to personal data protection from November 15, 2021. Commentary on the Law of 07.05.2021 No. 99-Z «About the protection of personal data». Available at: <https://bii.by/tx.dll?d=456664> (accessed 14 April 2021) (in Russian).

6. E-commerce under the new Law on Personal Data. Checklist for retailers. Available at: <https://belretail.by/news/e-commerce-v-usloviyah-novogo-zakona-o-personalnyih-dannyih> (accessed 25 May 2021) (in Russian).

7. Lukashenko approved amendments to the law on telecommunications – innovations also concern threats to national security. Available at: <https://www.belta.by/president/view/lukashenko-utverdil-izmeneniya-v-zakon-ob-elektrosvyazi-novatsii-kasajutsja-i-ugroz-natsbezopasnosti-442675-2021> (accessed 24 May 2021) (in Russian).

Информация об авторе

Криштаносов Виталий Брониславович – кандидат экономических наук, докторант, Белорусский государственный технологический университет, e-mail: krishtanosov@mail.ru

Information about the author

Kryshtanosau V. – PhD in Economic sciences, doctoral student, Belarusian State Technological University, e-mail: krishtanosov@mail.ru

Статья поступила в редакцию 09.12.2021

Received by editorial board 09.12.2021