УДК 338.242

В. Б. Криштаносов
Белорусский государственный технологический университет

МЕХАНИЗМЫ КОНТРОЛЯ И РЕГУЛИРОВАНИЯ ЦИФРОВОЙ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ: СИСТЕМНЫЙ ПОДХОД

Разработаны институциональные основы проведения системной цифровой трансформации в Республике Беларусь, соответствующие механизмы ее реализации на уровне рабочих групп и предприятий, организационная структура взаимодействия уполномоченных органов государственного управления по осуществлению программы цифровизации, а также модель осуществления цифровой трансформации на уровне страны. Предложена методология оценки экономической эффективности средств управления цифровыми активами, ограничений в управлении киберрисками, стоимости снижения риска, рентабельности инвестиций в обеспечение кибербезопасности. Выделен комплекс мероприятий, направленный на формирование регуляторной экосистемы на уровнях разработки общей стратегии цифровизации (включая обеспечение нормативно-правового регулирования в области цифрового развития), защиты киберпространства (в том числе обеспечение комплексного операционного реагирования на кибератаки, кибербезопасности критической инфраструктуры), финансового рынка и отдельных цифровых инноваций и концепций (главным образом в форме государственно-частного партнерства), включая развитие 5G, комплекс цифровых систем и сервисов, интегрированных с национальной системой цифровой идентификации, внедрение AI, повышение цифровых навыков населения. Выявлена роль таких элементов комплексной цифровизации, как концепты E-Government, CBDC, Crowdfunding, криптовалют, а также сформулированы предложения по реализации ИТ-решений на уровне Союзного государства (ЕАЭС) за счет аккумулирования финансовых, технологических ресурсов и компетенций стран-членов.

Ключевые слова: цифровая трансформация, государственное регулирование, методология оценки рисков и угроз, кибербезопасность, «новая экономика 2.0».

Для цитирования: Криштаносов В. Б. Механизмы контроля и регулирования цифровой экономики Республики Беларусь: системный подход // Труды БГТУ. Сер. 5, Экономика и управление. 2022. № 2 (262). С. 17–32.

V. B. Kryshtanosau
Belarusian State Technological University

MECHANISMS OF CONTROL AND REGULATION OF THE DIGITAL ECONOMICS OF THE REPUBLIC OF BELARUS: A SYSTEM APPROACH

There have been the institutional framework for conducting a systemic digital transformation in the Republic of Belarus, its implementation at the level of working groups and enterprises, the organizational structure for the participation of representative government bodies in submitting a digital transformation program, as well as a model for implementing digital transformation at the country level developed. It was proposed a methodology for assessing the economic efficiency of digital asset management tools, restrictions in cyber risk management, the cost of risk reduction, and the return on investment in cybersecurity. It has been identified a set of measures aimed at forming a regulatory ecosystem at the levels of developing a general digitalization strategy (including ensuring legal regulation in a free area of development), protecting cyberspace (including ensuring integrated operational consumption for cyberattacks, cyber safe critical value of income), the financial market, and individual digital innovations and concepts (mainly public-private), including the development of 5G, a set of digital systems and services integrated with national identification data, the use of AI, increasing the digital skills of the population. There have been the role of such elements of complex digitalization as the concept of E-Government, CBDC, Crowdfunding, cryptocurrencies highlighted, and proposals for the implementation of IT solutions at the level of the Union of States (EAEU) developed through the accumulation of financial, technological resources and competencies of member countries.

Keywords: digital transformation, government regulation, risk and threat assessment methodology, cybersecurity, “new economy 2.0”.

For citation: Kryshtanosau V. B. Mechanisms of control and regulation of the digital economics of the Republic of Belarus: a system approach. *Proceedings of BSTU, issue 5, Economics and Management*, 2022, no. 2 (262), pp. 17–32 (In Russian).

Введение. Анализ выявленных в ходе исследования рисков и угроз цифровизации экономики Республики Беларусь требует разработки эффективной и комплексной модели управления рисками в контексте особенностей развития и направлений цифровой трансформации экономической системы страны. Необходима адаптация лучших международных практик и теорий управления рисками к текущему состоянию и перспективной динамике развития имплементации цифровых инноваций в национальную экономику. При этом важно отметить, что управление цифровыми рисками является более сложным и комплексным по сравнению с управлением финансовыми рисками по причине трудности в измерении и отсутствия единого признанного стандарта управления.

Проведенный анализ выявил наиболее уязвимые в контексте рисков цифровизации отрасли Республики Беларусь как в среднесрочной перспективе роста их технологичности, так и на стадии формирования полноценной цифровой архитектуры в рамках концепции «новой экономики 2.0»[1]. Принимая во внимание ограниченность ресурсов страны, представляется целесообразным формирование национальной политики в области регулирования цифровых рисков с учетом данных факторов и потенциала выявленных угроз.

Как видно из теории, для эффективного управления рисками недостаточно только внутренних ресурсов управляющей системы, необходимо использование ресурса внешней управляющей системы. Кроме того, национальная система управления цифровыми рисками с точки зрения обеспечения устойчивости развития цифровой экономики и эффективности принимаемых решений, как показывает международная практика формирования институциональной экосистемы регулирования цифровой экономики, предполагает формирование ряда взаимосвязанных организационных, институциональных, правовых и технологических элементов.

Комбинация государственных и рыночных механизмов (совместных финансовых, организационных, технологических и образовательных ресурсов, а также компетенций), направленных на централизацию, систематизацию и автоматизацию функций управления цифровизацией, является важным условием формирования эффективной системы управления цифровыми рисками, генерирующими дополнительный эффект синергии многоуровневой системной цифровой трансформации национальной экономики посредством синхронного запуска цифровых проектов (с последующим их масштабированием) в рамках реализации в Республике Беларусь концепций Smart City, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, Intellectual Transport Systems, Telemedicine, FinTech, CBDC, RTGS, InsurTech и Cryptocurrency.

Основная часть. Институциональная основа организационного механизма государственного регулирования данной сферы может быть представлена Министерством цифровизации (далее – МЦ), имеющим соответствующие компетенции по трансформации и интеграции цифровых систем, включающие:

– разработку и внедрение системы формализации оценки цифровых рисков (совместно с Оперативно-аналитическим центром при Президенте Республики Беларусь (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 даст возможность внедрить новый инструментарий с меньшими затратами, а также обеспечить раннее выявление и устранение угроз и рисков;

– использование «упреждающего регулирования», предполагающего выявление изменений в окружающей экосреде на ранних этапах с целью 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.

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, включая (рис. 1):

1) руководителей цифровой трансформации на уровне отрасли (сфера компетенций – осуществление управленческой деятельности по интеграции цифровых технологий);

2) владельцев риска цифровой трансформации на уровне предприятий (сфера компетенций – все риски трансформации);

3) рабочих группы по трансформации с участием компетентных сотрудников МЦ, отраслевых министерств и предприятий, участвующих в программе трансформации (группы работают в гибких командах с назначенными ресурсами по управлению рисками), включая менеджеров по рискам трансформации (межфункциональные группы). Межфункциональные группы имеют возможность проработать направления улучшения механизмов взаимодействия с использованием механизмов «цифровых лабораторий»;

4) организации-партнеры по управлению рисками в рамках государственно-частного партнерства.

Рис. 1. Организационная схема взаимодействия уполномоченных органов государственного управления по осуществлению программы цифровизации (разработана автором)

Важным этапом выстраивания национальной политики в области цифровой безопасности является проведение комплексного последовательного анализа уровня цифровизации на уровне предприятий, отраслей и секторов экономики для формирования национальной карты цифровизации экономики на основе цифровых портретов (профилирования) субъектов хозяйствования по предложенной методике, начиная с бизнес-аудита предприятия (организации) и формализации бизнес-модели и заканчивая получением статистических отчетных данных и расчетом комплексного показателя уровня цифровизации.

Профилирование позволит выявить и определить приоритетность реагирования на цифровые риски и угрозы, что в сочетании с анализом результатов регуляторных экспериментов и инноваций, а также мониторинга и оценки на основе данных, может быть использовано для создания структуры управления, которая способна к постоянному совершенствованию как ответной реакции на анализ входящей информации, полученной в том числе в результате прогнозирования. В свою очередь, эта более гибкая регулирующая система может генерировать важную информацию о будущих цифровых инновациях и угрозах, которые следует учитывать при прогнозировании (рис. 2).

Как показано на рис. 2, на стратегическом уровне в рамках компетенции МЦ 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 выполняется разработка прототипов для последующего масштабирования наиболее эффективных практик, а также вырабатываются принципы и пределы стратегической гибкости для первичной реализации цифровых возможностей. На третьем этапе осуществляется непосредственная трансформация, которая 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 фонда[2] (первый и второй этапы) путем его переподчинения МЦ, а также собственных средств отраслей и предприятий, участвующих в программе трансформации (третий этап).

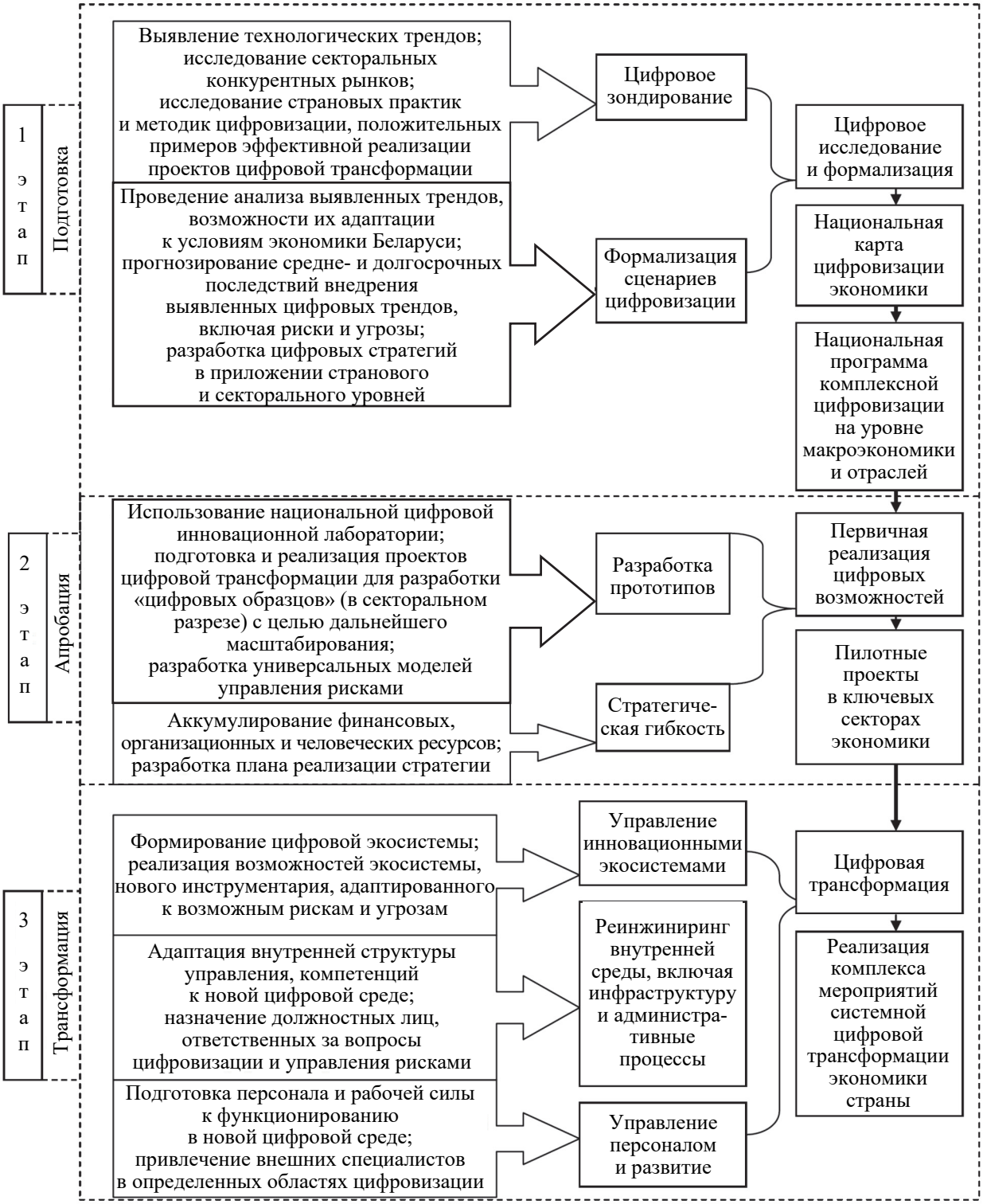

Рис. 2. Модель осуществления цифровой трансформации на уровне страны (разработана автором)

Для реализации представленной модели необходимо формировать универсальную систему управления рисками как на уровне МЦ (во взаимодействии с ОАЦ), так и на уровне рабочих групп трансформации с учетом их адаптации к условиям и характеристикам отраслей и конкретных предприятий (таблица).

Данная таблица позволяет осуществить ряд оценок, включая:

– экономическую эффективность средств управления цифровыми активами (затраты (7 + + 8 + 9 + 10 + 11) относительно зафиксированных случаев нивелирования угроз (1, 2, 3, 4, 5, 6));

– ограничения в управлении киберрисками (затраты (7 + 8 + 9 + 10 + 11) относительно бюджета организации);

– стоимость снижения риска (затраты (7 + 8 + + 9 + 10 + 11));

– рентабельность инвестиций в обеспечение кибербезопасности (затраты (7 + 8 + 9 + 10 + 11) относительно потенциальных потерь (3 + 4 + + 5 + 6)).

В сфере кибербезопасности для измерения киберрисков целесообразным является создание банка данных киберрисков с целью идентификации ключевых факторов их возникновения с привязкой к профилю организации.

В контексте представленной модели на операционном уровне в рамках рабочих групп по цифровой трансформации представляется возможным использование системного подхода в отношении управления рисками с последовательным осуществлением комплекса мероприятий по выявлению угроз, адаптации экосистемы, реализации мер противодействия, внедрению эффективного управления и совершенствованию подходов (рис. 3).

Для обеспечения комплексности и системности реализации цифровой трансформации видится необходимым в рамках государственно-частного партнерства привлечение организаций-партнеров, например компетентных аудиторских компаний, специализирующихся на оценке рисков и киберугроз. При этом задачей МЦ является отбор уполномоченных компаний для участия в программе цифровизации с учетом критериев имеющегося опыта предоставления соответствующих услуг оценки рисков, реализации проектов нивелирования внешних и внутренних цифровых угроз, величины штата и компетенций специалистов. Важнейшим условием участия в программе организаций-партнеров является подписание соглашений о конфиденциальности.

Эффективность реализации данного механизма определяется комплексностью[3], системностью и цикличностью его имплементации, позволяя сформировать скоординированный ответ на возникающие угрозы и риски, выстроить систему взаимодействия на различных уровнях управления. Кроме того, данный механизм позволит осуществить поступательный переход от управления рисками к управлению устойчивостью, поскольку он охватывает не только кризисные, но и посткризисные фазы, формируя способность системы противостоять киберугрозам с постепенной адаптацией и трансформацией на отраслевом уровне и уровне предприятия. Тем самым обеспечивается многомерная устойчивость (мультиравновесие), формирование сложной адаптивной системы.

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 следует включить следующий комплекс мероприятий:

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

а) 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 взаимозависимостей[4];

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

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

Схема управления рисками и угрозами цифровизации на уровне отраслей/предприятий (разработана автором)

Перечень возможных рисков и угроз цифровизации	Вероятность наступления	Потенциальные потери			Каскадный эффект*	Затраты на управление рисками и угрозами				Перечень мероприятий по предотвращению	Сроки реализации	Владельцы риска**
		финансовые	репутационные	косвенные		оборудование	ПО	персонал	страхование			
1	2	3	4	5	6	7	8	9	10	11	12	13

*Рассчитывается на уровне страны, отрасли и предприятия.

**Определяются как по вертикали (МЦ – группы трансформации – уровень отрасли – уровень предприятия), так и по горизонтали на уровне конкретного хозяйствующего субъекта.

Рис. 3. Механизм управления рисками на уровне рабочих групп и предприятий (разработан автором)

2. Уровень защиты киберпространства:

а) развитие нормативно-правового и технологического обеспечения национальной кибербезопасности, включая:

– обеспечение суверенитета в киберпространстве, предполагающего 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;

– разработку и принятие закона о национальной цифровой безопасности, который охватывает широкий спектр отраслей и секторов экономики и социальной сферы страны, 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.;

– разработку и внедрение национальных программных продуктов, которые направлены на снижение зависимости Беларуси от иностранных поставщиков технологий и цифровых услуг;

– разработку и внедрение национальных стандартов[5] в отношении аккумулирования, хранения, обмена и использования данных, соответствующих принципам безопасности и конфиденциальности, прозрачности, подотчетности, целостности;

– законодательное закрепление определения «государство – спонсор киберпреступлений», предполагающего широкое трактование с включением даже тех стран, которые предоставили убежище группам киберпреступников, а также реализацию программы (аналогичной развернутой в США), направленной на финансовое поощрение за предоставление информации о хакерах, в особенности спонсируемых иностранными государствами[6];

– формирование на уровне государства резервных фондов: финансовых, материальных, информационных на отраслевом и национальном уровнях для нивелирования последствий кибератак, в особенности в отношении критической инфраструктуры;

б) обеспечение комплексного операционного реагирования на кибератаки, включая:

– разработку планов кризисного реагирования на внешние цифровые угрозы, включая создание единой государственной системы цифрового мониторинга с целью 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);

– 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;

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

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

– введение ответственности в отношении выбора частными предприятиями оптимальных в контексте безопасности технологий[7];

– разработку и внедрение профессиональных стандартов по кибербезопасности для сотрудников, обеспечивающих защиту цифровых систем объектов критической инфраструктуры[8];

в) обеспечение кибербезопасности объектов критической инфраструктуры, включая:

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

– разработку и имлементацию 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;

– мониторинг на технологическом уровне таких систем, как ИТ, управление производством, киберфизические и подключенные устройства в целом, включая IoT;

– подготовку 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, включая:

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

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

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

г) 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), включая:

а) содействие развитию 5G как основы развития цифровой инфраструктуры; обеспечение и стимулирование разработки и поставки цифровых решений для регионов с низкой технологичной инфраструктурой;

б) разработку 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;

в) стимулирование внедрения AI в целях национального развития в таких областях, как промышленность, сельское хозяйство, здравоохранение, энергетика, образование, коммунальное хозяйство, логистика и транспорт с поступательным переходом к полноценной реализации концепций, характерных для «новой экономики 2.0»: Smart City, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, Intellectual Transport Systems, E-Commerce, Telemedicine;

г) разработку национального законодательства, направленного на обеспечение безопасности технологий AI, сведение к минимуму алгоритмической предвзятости при разработке 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 критически важными для национальной безопасности системами;

д) создание национальной лаборатории AI/ML;

е) повышение цифровых навыков населения, развитие учебных программ и платформ образовательных технологий[9], направленных на противодействие тенденциям высвобождения малопроизводительной рабочей силы в условиях цифровой трансформации экономики[10].

Важнейшим элементом системной цифровой трансформации экономики, реализацию которой целесообразно осуществлять с учетом комплексного подхода, с использованием как рабочих, так и функциональных групп, является разработка и внедрение полноценной платформы E-Government, предполагающей на внешнем контуре оказание основных государственных услуг гражданам и предприятиям через онлайн-каналы в режиме реального времени. Эффективная реализация данной концепции на внутреннем контуре требует максимального агрегирования цифровых данных (все услуги должны быть доступны в одном приложении в отличие от множества разных цифровых каналов), выработки оценочных показателей (таких как удовлетворенность пользователей, проникновение услуг или желаемый уровень автоматизации, повышение эффективности), внедрения эффективных способов мониторинга этих показателей, а также их использования в государственном управлении. Кроме того, технологические требования современной ИТ-архитектуры концепта E-Government предполагают ее масштабируемость и модульность (в том числе для повторяющихся элементов сервисных транзакций, таких как системы цифровой идентификации и платежи), что позволяет ускорить процесс оцифровки и сократить государственные расходы[11], сформировать эффективные совместимые и гибкие решения, в том числе с использованием облачных технологий.

С точки зрения современных тенденций имплементации E-Government важным элементом является коммерциализация данной концепции, предполагающая предоставление возможности доступа (в том числе платного) юридических и физических лиц к государственным деперсонифицированным (очищенным) цифровым данным (на примере КНР[12]).

Реализация концепции E-Government может стать важным драйвером для развития малого и среднего предпринимательства (МСП) в Республике Беларусь. Поступательное внедрение цифровых технологий в государственном управлении позволит оптимизировать цифровой документооборот для платежных сервисов и налогообложения, бухгалтерский учет, отчетность; обеспечить контроль над финансовыми операциями со стороны compliance office, а также гарантировать надежность и равенство доступа субъектов хозяйствования к информации.

В рамках цифровой трансформации национальной экономики важнейшим системным элементом является формирование конкурентоспособного цифрового финансового сектора. В этой связи с учетом современных тенденций внедрения инноваций в цифровую среду финансовых регуляторов по всему миру, теоретических и практических разработок представляется целесообразным предложить ряд подходов к адаптации банковской среды Республики Беларусь к технологиям CBDC с учетом выявленных угроз и рисков.

Как показал ряд исследований [1], наиболее безопасным с точки зрения сохранения стабильности денежно-кредитной системы является поступательное введение цифрового белорусского рубля и его временное обращение совместно с наличными денежными знаками. Это позволяет адаптировать все составляющие финансовой инфраструктуры к новым вызовам и выявить ее возможные уязвимости и недостатки, требующие дополнительной адаптации и доработки.

В текущих условиях развития белорусской экономики представляется маловероятным, что Национальный банк станет в авангарде разработки и внедрения цифровой валюты. Вместе с тем с учетом сложности и комплексности проблематики

новой технологии целесообразно выделить риски и возможности, связанные с адаптацией данной концепции в Республике Беларусь и потенциальным влиянием ее внедрения со стороны основного торгового партнера – Российской Федерации, а также ЕС, Украины, Китая или США.

Важно отметить, что наличная иностранная валюта играет важнейшую сберегательную функцию в «ценностной корзине» населения Республики Беларусь. В этой связи возникновение вероятности ограничения, а в дальнейшем отмены свободного обращения наличной валюты государствами-эмитентами приведет к необходимости поиска новых инструментов сохранения сбережений населением Беларуси. Представляется возможным, что в среднесрочной перспективе данная тенденция в целом позитивно скажется на экономике страны, так как вынудит население переводить наличные валютные сбережения в более производительные активы (покупка ценных бумаг, недвижимости, депозиты в национальной валюте и пр.). Это также позволит укрепить курс национальной валюты, сократить оборот серого рынка экономики (в том числе в разрезе расширения налогооблагаемой базы) и усилить мониторинг за располагаемыми активами. Вместе с тем следует ожидать переток части сбережений в сферу новых финансовых инструментов (различных криптоактивов[13]), покупку иностранных ценных бумаг на зарубежных биржевых площадках, что может привести к негативным последствиям для определенных групп населения с учетом недостаточной финансовой грамотности и недооценки возможных рисков. В то же время с учетом особенностей реализации данной концепции белорусские коммерческие банки вынужденно потеряют часть депозитов и счетов, которые домашние хозяйства заменят на цифровые кошельки под прямым контролем Национального банка. С целью замещения данных активов вырастет необходимость во внешнем кредитовании, реализацию которого может взять на себя банковский регулятор страны.

В долгосрочной перспективе в случае полного отказа от обращения наличных денежных средств ключевых торговых партнеров Республики Беларусь, в первую очередь Российской Федерации, банковская система столкнется с необходимостью адаптации к новым внешним вызовам. В первую очередь это затронет необходимость разработки/адаптации инфраструктуры для осуществления валютообменных операций на уровне коммерческих банков. Более того, на уровне банковских регуляторов возникает необходимость разработки совместных двусторонних (или многосторонних) протоколов, затрагивающих многочисленные стандарты и политику безопасности. Реализация данного сценария, очевидно, потребует значительных внутренних инвестиций как на уровне банковского регулятора, так и коммерческих банков, возможно расчетных центров ОАО «Белорусская валютно-фондовая биржа» и внебиржевого рынка. Кроме того, возникает необходимость разработки внутренних регламентов, в особенности в сфере информационной безопасности. Финансовая инфраструктура должна быть устойчива к кибератакам и другим угрозам, иметь эффективную защиту от подделок. При этом важно сохранить цифровую совместимость для обеспечения свободного перетока денежных средств между старыми и новыми системами и их элементами. С учетом изложенного представляется уместным изучение опыта Российской Федерации и КНР как наиболее важных торговых партнеров Беларуси и передовых в отношении разработки CBDC стран с целью адаптации и возможного использования наработок для эффективной адаптации национальной финансовой системы к новым вызовам.

Преимуществами внедрения концепции CBDC в Республике Беларусь являются:

– значительное повышение прозрачности расчетов и снижение рисков отмывания денег;

– низкие (возможно нулевые) тарифы для проведения расчетов;

– улучшение финансовой доступности (банковской инклюзивности) для населения;

– повышение безопасности, надежности и устойчивости банковской системы за счет более современных средств контроля и мониторинга денежных средств;

– повышение технологичности расчетных инструментов;

– обеспечение привлекательности национальных платежных средств в сравнении с соседними странами.

К недостаткам имплементации данной концепции следует отнести:

1) высокую стоимость внедрения;

2) рост потенциальных рисков и угроз, не выявленных на стадии разработки и внедрения концепции;

3) недостаточную избирательность эффективных и устойчивых практик внедрения усиливает риск односторонней зависимости от стандартов CBDC, принимаемых в Российской Федерации в случае, если Беларусь не инициирует общую программу исследования и разработки CBDC, например, на уровне ЕАЭС или Союзного государства. В рамках участия в такой программе страна сможет изучить возможные риски и угрозы функционирования концепта CBDC, разработать и внедрить цифровые инновации, адаптированные к особенностям национальной банковской системы, с учетом наработок и опыта центральных банков Российской Федерации и Казахстана.

Изучение опыта разработки и внедрения CBDC – необходимое условие для оптимальной адаптации национальной финансовой системы к внешним вызовам, связанным с возможным успешным и скорым внедрением данной концепции странами – торговыми партнерами Республики Беларусь. Важным элементом данной стратегии также является скорейшая разработка и внедрение национальной системы RGTS. В целом регулирование платежных сервисов должно отражать потенциальный риск финансовой стабильности для страны.

Дальнейшее государственное регулирование в отношении FinTech требует, с одной стороны, стимулирования имплементации цифровых инноваций, направленных на повышение качества и разнообразия предлагаемых услуг, их коммерческую привлекательность, интеграцию с мировым финансовым рынком. С другой стороны, критически важным аспектом является обеспечение безопасности (финансовой, экономической, технологической) как на уровне конкретных финансовых организаций, отрасли, так и Республики Беларусь, поскольку данный сектор оказывает как прямое, так и опосредованное воздействие на широкий спектр отраслей и секторов страны. Таким образом, финансовый сектор обладает потенциалом каскадного запуска негативных последствий в экономике страны в целом в результате инициирования в нем рисков и угроз.

С точки зрения обеспечения национальной экономической безопасности представляется целесообразным ужесточение банковского надзора по ряду причин.

Во-первых, ориентированные на потребителя продукты цифрового финансирования могут масштабироваться гораздо быстрее, чем традиционные финансовые услуги, что ограничивает возможности Национального банка Республики Беларусь адекватно их контролировать.

Во-вторых, традиционные регуляторные методы, такие как надзор на местах и требования к периодической отчетности, неадекватны современным характеристикам FinTech в отношении гибкости и скорости адаптации их форм организации.

В-третьих, объем генерируемых цифровых данных растет в геометрической прогрессии, и Национальному банку требуется сложная аналитика данных для их визуализации и анализа. Одним из направлений адаптации Национального банка Республики Беларусь к инновациям в финансовом секторе, позволяющим обеспечить непрерывность мониторинга, получение информации в режиме, близком к реальному времени, является концепция RegTech[14]. Кроме того, данный технологический надзор мог бы стать важным инструментом регулятивного подхода, основанного на оценке риска, который стимулирует доверие потребителей к финансовой организации, обеспечивая прозрачность информации той или иной FinTech компании. Вместе с тем адаптируемые подходы к регулированию с возможностью профилирования рисков позволяют поддерживать финансовую стабильность без чрезмерной имплементации дорогостоящих цифровых инноваций на уровне Национального банка.

FinTech компании, которые имеют системное значение или дестабилизация функционирования которых может привести к каскадным эффектам на уровне страны, должны соответствовать стандартам операционной и финансовой устойчивости. Кроме того, FinTech компании должны подвергаться адекватным требованиям в сфере борьбы с отмыванием денег. С целью формирования более открытого, конкурентоспособного, устойчивого и саморегулируемого финансового рынка в Беларуси представляется целесообразным разработать и закрепить на законодательном уровне требования: к качеству и размеру капитала FinTech компаний, оценке их рисков, раскрытию информации и отчетности.

Законодательного регулирования в Республике Беларусь требует также отдельное направление FinTech – Crowdfunding[15]. По причине отсутствия специального регулирования в отношении Crowdfunding в белорусском законодательстве участники отношений Crowdfunding вынуждены руководствоваться в своих коммерческих взаимоотношениях общими нормами гражданского законодательства об обязательствах и договорах[16]. В данных условиях, как отмечают эксперты, на законодательном уровне в должной мере не обеспечивается защита прав участников подобного рода договоров. С учетом международной практики[17] представляется целесообразным разработка в Беларуси соответствующих нормативных актов, регламентирующих функционирование Crowdfunding, включающих требования о регистрации платформ в финансовых органах для получения соответствующих лицензий на ведение бизнеса, для поддержания определенного минимального уровня капитала и использования банковских учреждений для хранения средств клиентов. Платформы также должны представлять регулярные отчеты об обороте предоставляемых кредитных ресурсов, а также обмениваться с банками информацией о кредитной истории клиентов Crowdfunding площадок.

Актуальным компонентом цифровизации финансового сектора и формирования FinTech является использование криптовалют, рынок которых характеризуется динамическим ростом. Составным элементом государственной политики в сфере криптовалют должна стать защита интересов белорусских граждан от мошенничества

путем информационного обеспечения и введения ограничения на транзакции для физических лиц, не обладающих определенной квалификацией, опытом и навыками. В Беларуси представляется важным дальнейшее совершенствование нормативной базы для урегулирования споров при осуществлении транзакций с криптовалютами, а также формирование законодательных основ для передачи прав собственности на криптоактивы[18]. Кроме того, по окончании моратория на налогообложения криптовалютных операций (в 2023 г.)[19] Министерству по налогам и сборам Республики Беларусь необходимо проработать и сформировать эффективную систему налогообложения данной сферы, которая бы включала следующие элементы:

– создание механизмов мониторинга коммерческих транзакций с криптоактивами, особенно трансграничных, в целях налогообложения;

– разработка алгоритмов, позволяющих выявлять криптовалютные транзакции, которые скрывают или маскируют операции, облагаемые общими подоходными налогами или налогами с продаж;

– налогообложение доходов, полученных майнерами;

– предотвращение возможностей несанкционированного подключения майнеров к электросетям общего пользования либо использования льготных тарифов, предоставляемых государством населению (например, путем внедрения технологий Smart Grid).

С учетом наличия системных рисков для стабильного функционирования национальной финансовой системы в перспективе расширения использования криптовалют в платежных сервисах и в качестве инвестиционного инструмента отмечена тенденция разработки регуляторами механизмов, направленных на снижение анонимности учетных записей и персональных данных участников криптовалютного рынка. Для Республики Беларусь ввиду высокой стоимости разработки и имплементации соответствующих механизмов мониторинга и контроля, а также возможности масштабируемости данных систем представляется важным рассмотреть возможность реализации ИТ-решений на уровне Союзного государства (ЕАЭС) за счет аккумулирования финансовых, технологических ресурсов и компетенций стран-членов.

Кроме того, с учетом развития интеграционных процессов на уровне ЕАЭС для интенсификации цифровых преобразований и обмена лучшими практиками представляется целесообразным создание в рамках интеграционного объединения отдельной платформы сотрудничества – Совета по цифровым технологиям ЕАЭС, уполномоченного осуществлять функции продвижения обмена передовым опытом и знаниями в сфере цифровой трансформации и общих стандартов цифровизации посредством:

1) формирования совместимой экосистемы цифровых решений, которые будут предоставлять цифровые данные в режиме реального времени в интересах стран ЕАЭС и их предприятий;

2) разработки и введения стандартов управления данными для обеспечения их совместимости и обмена;

3) разработки рекомендаций по цифровизации отдельных направлений и отраслей (с учетом их приоритетности) в рамках общих программ ЕАЭС;

4) повышения конкурентоспособности предприятий за счет цифровизации с использованием таких механизмов, как:

– создание совместного фонда/инкубатора для перспективных стартапов (возможно на базе Международного евразийского индустриального фонда[20]);

– продвижение двусторонних и многосторонних трансграничных инициатив в поддержку цифровизации МСП;

– формирование общих правовых рамок, устранение искусственных ограничений и барьеров;

– привлечение инвесторов в ЕАЭС путем продвижения данной интеграционной группировки как единого емкого рынка;

5) разработки совместных программ, направленных на развитие цифрового кадрового резерва в странах ЕАЭС;

6) подготовки и реализации совместной программы по привлечению и интеграции цифровых талантов из-за рубежа.

Важнейшими аспектами реализации комплексной программы трансформации национальной экономики являются наличие значительных финансовых ресурсов для решения не только технологических, но и организационных, управленческих задач, привлечение компетентных специалистов в различных областях деятельности, создание контролируемого финансового механизма.

Согласно рекомендациям ОЭСР [2], финансирование цифровизации может осуществляться с использованием следующего инструментария:

– грантов (государственные агентства могут обеспечить МСП доступ к данным финансовым инструментам на приобретение цифровых продуктов и услуг);

– ваучеров (на предоставление менеджменту МСП бесплатных консультаций и специализированного обучения);

– кредитов (облегчение доступа МСП к кредитным финансовым ресурсам за счет обеспечения соответствующих гарантий);

– косвенных финансовых стимулов для цифровизации, включая ускоренную амортизацию

при покупке определенных «цифровых» материальных активов.

С учетом ограниченности финансовых ресурсов для проведения комплексной цифровой трансформации экономики страны представляется важным создание следующего механизма финансирования цифровых инноваций:

1) 50% затрат, в первую очередь, на реализацию целей строительства инновационной цифровой инфраструктуры, цифрового правительства, CBDC и RTGS, разработки национальных стандартов может взять на себя государство в форме специально сформированного Фонда цифрового развития, средств Евразийского индустриального фонда, кредитов международных финансовых организаций (МБРР, ЕБРР и пр.). Обоснованность превалирования бюджетного финансирования по названным направлениям обусловлена длительностью окупаемости проектов, их высокой социальной значимостью и влиянием на многие связанные сектора и отрасли в рамках национальной экономики;

2) 35% затрат главным образом на финансирование цифровой трансформации конкретных флагманских предприятий могут взять на себя отраслевые организации и фонды инноваций этих предприятий. Реализация цифровой трансформации данных предприятий несет прямой коммерческий эффект для повышения эффективности их функционирования, обеспечивая повышение конкурентоспособности за счет снижения себестоимости производимой продукции, повышения ее качества и технологичности, а также внедрения современных бизнес-процессов управления организациями и цепочкой реализации производимых товаров и услуг;

3) 15% затрат на развитие экосистем в сферах E-Commerce, Cloud Computing, AI и пр. могут быть покрыты за счет Парка высоких технологий (ПВТ) и частных коммерческих предприятий, заинтересованных в предоставлении соответствующих услуг, участии в тендерах на поставку своей продукции государственным предприятиям и т. д. Данные проекты являются окупаемыми с точки зрения их инвестиционной привлекательности, а участие частных компаний в национальной программе цифровой трансформации позволит встроить белорусские организации в секторе информационно-телекоммуникационных технологий (ИКТ) в производственные и сбытовые цепочки предприятий и обеспечить долгосрочность коммерческих отношений по определенным направлениям.

Заключение. Таким образом, принимая во внимание ограниченность ресурсов страны, представляется целесообразным формирование национальной политики в области регулирования цифровых рисков с учетом потенциала выявленных угроз цифровизации как традиционных отраслей экономики, так и в рамках концепции «новой экономики 2.0».

Национальная система управления цифровыми рисками должна опираться на ряд организационных, институциональных, правовых и технологических элементов, включая национальную концепцию построения интегрированной цифровой экосреды.

Институциональная основа государственного регулирования может быть представлена Министерством цифровизации, имеющим соответствующие компетенции по трансформации и интеграции цифровых систем. Вместе с тем эффективная реализация заданных компетенций возможна при условии формирования низовой специализированной управленческой структуры, состоящей из ответственных за минимизацию рисков цифровой трансформации сотрудников на уровне отраслей и конкретных предприятий, участвующих в программе трансформации.

Условием проведения эффективной национальной политики в области цифровизации является осуществление комплексного последовательного анализа цифровизации на уровне предприятий, отраслей и секторов экономики для формирования национальной карты цифровизации экономики, составленной на основе цифровых портретов (профилирования) субъектов хозяйствования.

Важнейшими направлениями комплекса мероприятий цифровой трансформации в разрезе потенциальных рисков и угроз являются: разработка политики и нормативных актов, направленных на обеспечение безопасного развития цифровых технологий; обеспечение суверенитета в киберпространстве; разработка и внедрение национальных программных продуктов и стандартов; разработка планов кризисного реагирования на внешние цифровые угрозы, включая создание единой государственной системы цифрового мониторинга и групп быстрого ИТ-реагирования; формализованное описание профилей цифровых угроз; развитие страхового инструментария обеспечения гарантий исполнения обязательства в отношении рисков, связанных с киберпреступлениями; разработка стандартов критически важной инфраструктуры с учетом актуальных международных тенденций; формирование привлекательной среды для внедрения цифровых бизнес-моделей; осуществление инвестиций в развитие цифровых навыков.

Технологический аспект требует реализации ряда ключевых инновационных направлений, включая содействие развитию 5G; разработку цифровых систем для имплементации цифровой идентификации; сведение к минимуму алгоритмической предвзятости при разработке и продаже продуктов и услуг на базе искусственного интеллекта.

Предложена авторская модель системного подхода к управлению рисками с последовательным осуществлением комплекса мероприятий по выявлению угроз, адаптации экосистемы, реализации мер противодействия, внедрению эффективного управления и совершенствованию подходов, а также модель поэтапного комплексного осуществления цифровой трансформации на уровне страны.

Государственное регулирование в отношении FinTech требует обеспечения безопасности (финансовой, экономической, технологической) как на уровне конкретных финансовых организаций, отрасли, так и Республики Беларусь, поскольку данный сектор оказывает как прямое, так и опосредованное воздействие на широкий спектр отраслей и секторов страны. Одним из направлений адаптации Национального банка Республики Беларусь к инновациям в финансовом секторе, позволяющим обеспечить непрерывность мониторинга, получение информации в режиме, близком к реальному времени, является концепция RegTech. Одним из элементов цифровой финансовой инфраструктуры Беларуси может стать CBDC. Введение национальной цифровой валюты потребует значительных внутренних инвестиций как на уровне банковского регулятора, так и коммерческих банков, возможно расчетных центров ОАО «Белорусская валютно-фондовая биржа» и внебиржевого рынка.

Для интенсификации цифровых преобразований и обмена лучшими практиками представляется важным создание в рамках интеграционного объединения отдельной платформы сотрудничества – Совета по цифровым технологиям ЕАЭС, уполномоченного осуществлять функции продвижения обмена передовым опытом и знаниями в сфере цифровой трансформации и общих стандартов цифровизации.

---

[1]«Новая экономика 2.0» – авторская концепция, характеризующая среднесрочный этап формирования цифровой экономики, для которого характерны формирование новой экономической среды на основе платформизации и алгоритмизации, экономическими механизмами и институтами, комплексными цифровыми концепциями производства и управления.

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

[3]Как показало исследование McKinsey о современных подходах к минимизации рисков цифровых преобразований, использование комплексного подхода позволяет снизить вероятность угроз, повысить эффективность управления и сократить издержки. Так, по данным американской компании, в результате использования комплексного подхода количество связанных с технологическим риском дефектов снизилось в диапазоне 45–90%, а соответствующие издержки сократились на 90–97%; количество процессов, связанных с технологическим риском, уменьшилось на 40–85%, а соответствующие издержки снизились на 75–90% [3].

[4]Примеры таких правил в этой области охватывают законодательство о защите данных (например, GDPR), схемы облачной сертификации [4].

[5]В этом контексте термины «технологический суверенитет» или «цифровой суверенитет» недавно появились в качестве зонтичной концепции для разработки цифровой политики в Европе [5].

[6]В США осуществляется программа поощрения анонимных информаторов и «белых хакеров», которые за сообщение о террористах могут получить награду. 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 [6].

[7]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 поддерживает прозрачность и сводит к минимуму риски для конфиденциальности, доступности и целостности данных.

[8]Например, в России Центральный банк инициировал разработку стандарта для специалистов информационной безопасности банков, который уже согласован отраслевым сообществом и находится на стадии обсуждения в Министерстве труда Российской Федерации [7].

[9]Как показывает анализ данных о подготовке студентов по техническим и технологическим специальностям в Республике Беларусь за 2013–2020 гг., при незначительном росте доли студентов данной специальности обучения (с 19,7 до 21,6%) в абсолютных числах отмечается сокращение как общего количества студентов белорусских вузов (с 395,3 до 254,4 тыс. человек), так и будущих технических специалистов (с 77,7 до 54,9 тыс. человек) [8, 9].

[10]В отношении среднего образования следует учесть опыт России, в которой Министерство цифрового развития, связи и массовых коммуникаций подготовило программу бесплатного изучения языков программирования на 2-летних курсах учениками 8–11 классов школ с 2022 г.

[11]Например, в Германии полностью интероперабельные и взаимосвязанные правительственные данные позволили сократить время обработки дел для ключевых государственных служб на 60%. Для переписи технологически развитые страны, такие как Нидерланды, полностью извлекают данные из существующих баз данных. Этот подход требует до 99% меньше затрат, чем традиционный метод, основанный на опросах [10].

[12]В 2021 г. начались торги большими данными на Шанхайской бирже данных, на которой представлены 20 информационных продуктов в сфере финансов, транспорта и связи. Участниками биржевых торгов являются свыше 100 организаций. Контроль над осуществлением биржевых операций осуществляет Шанхайский комитет экспертов по транзакциям с данными, в состав которого входит 31 специалист в сфере обработки и безопасности данных, а также финансисты и юристы [11].

[13]По оценкам Triple A в Беларуси владельцами криптовалют являются 352,5 тыс. человек [12].

[14]Предполагает использование цифрового инструментария, включая системы глубокого обучения и фильтров AI [13].

[15]В рамках Государственной программы инновационного развития Республики Беларусь на 2016–2020 гг. краудфандинг интерпретируется как интернет-платформа для взаимодействия потребителей и производителей товаров и услуг, инвесторов и соискателей инвестиций, при этом отдельное законодательство, детализирующее правовые взаимоотношения между поставщиками финансовых услуг, инвесторами и потребителями, в отношении данного концепта отсутствует.

[16]Предусмотренные действующим законодательством договорные конструкции не в полной мере отражают специфику возникающих отношений. При некоммерческом Crowdfunding чаще всего заключаются договоры дарения (ст. 543 Гражданского кодекса Республики Беларусь (далее – ГК)), пожертвования (ст. 553 ГК), предоставления безвозмездной (спонсорской) помощи (п. 5 Указа Президента Республики Беларусь от 1 июля 2005 г. № 300 «О предоставлении и использовании безвозмездной (спонсорской) помощи»). В рамках коммерческого Crowdfunding применяются договоры займа (ст. 760 ГК), купли-продажи с предварительной оплатой (ст. 457 ГК). Если Crowdfunding предусматривает условие о том, что товар будет передан донору (инвестору), независимо от размера его платежа и конечной стоимости самого товара, то применить ст. 457 ГК невозможно. С учетом особенностей возникающих отношений и свободы договора (ст. 391 ГК) стороны могут заключить, например, договор возмездного участия в Crowdfunding [14].

[17]Например, закон Jumpstart Our Business Startups Act (JOBS Act) в США, Закон ЕС о регулировании Crowdfunding для МСП (Regulation (EU) 2020/1053 of October 7 2020 on European Crowdfunding Service Providers for business (Crowdfunding Regulation)).

[18]Например, в случае смерти владельца, если закрытые ключи не будут должным образом храниться и записываться.

[19]Согласно Указу Президента Республики Беларусь от 21.12.2017 № 8 «О развитии цифровой экономики».

[20]С целью финансирования совместных проектов в сфере производственной кооперации и трансфера технологий в 2020 г. государствами Евразийского экономического союза создан Международный евразийский индустриальный фонд, который в 2021 г. стал резидентом белорусского Парка высоких технологий. В ЕАЭС с участием Фонда реализуется [15] проект по созданию цифровой экосистемы для обеспечения взаимодействия хозяйствующих субъектов государств ЕАЭС. Проект будет реализован в 2021–2022 гг. и позволит нарастить производственный потенциал по выпуску инновационной продукции с высокой добавленной стоимостью. На реализацию проекта бюджетом комиссии выделено более 150 млн росс. руб.

Список литературы

1. Beyond COVID-19 Advancing Digital Business Transformation in the Eastern Partner Countries / Organisation for Economic Cooperation and Development. 2021. 116 p. URL: https://www.oecd.org/eurasia/Covid19_%20Advancing%20digital%20business%20transformation%20in%20the%20EaP%20countries.pdf (date of access: 15.11.2021).

2. CBDC. Central bank digital currencies: foundational principles and core features: Bank for International Settlements. 2020. 21 p. URL: https://www.bis.org/publ/othp33.pdf (date of access: 07.01.2022).

3. Boehm J., Smith J. Derisking digital and analytics transformations. Risk Practice // McKinsey Report. 2021. 12 p. URL: https://www.mckinsey.com/business-functions/risk/our-insights/derisking-digital-and-analytics-transformations (date of access: 05.01.2022).

4. Politou E., Alepis E., Patsakis C. Profiling tax and financial behaviour with big data under the GDPR // Computer Law & Security Review. 2019. Vol. 35. P. 306–329. DOI: 10.1016/j.clsr.2019.01.003.

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission (EC): Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN. 2013. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 (date of access: 08.06.2020).

6. Бондарчук Н. Правительство США будет выплачивать информаторам и «белым хакерам» награды в криптовалютах. 2021. URL: https://bits.media/pravitelstvo-ssha-budet-vyplachivat-informatoram-i-belym-khakeram-nagrady-v-kriptovalyutakh/ (дата обращения: 17.08.2021).

7. Ученая степень безопасности // Коммерсантъ. 2022. URL: https://www.kommersant.ru/doc/5183598 (дата обращения: 29.01.2022).

8. Образование в Республике Беларусь / Нац. стат. комитет Респ. Беларусь. Минск, 2021. 40 с. URL: https://www.belstat.gov.by/upload/iblock/5d6/5d62c11490270d88d396c8788f28b95d.pdf (дата обращения: 11.12.2021).

9. Образование в Республике Беларусь (2019/2020 учебный год) / Нац. стат. комитет Респ. Беларусь. Минск, 2019. 48 с. URL: https://www.belstat.gov.by/upload/iblock/eef/eef2ad012db2ea8aaf4dbea2647d5a90.pdf (дата обращения: 11.12.2021).

10. Government data management for the digital age: McKinsey&Company / A. Domeyer [et al.]. 2021. 9 p. URL: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/government-data-management-for-the-digital-age (date of access: 20.09.2021).

11. В Шанхае заработала новая биржа данных. 2021. URL: https://bluescreen.kz/news/10095/v-shankhaie-zarabotala-novaia-birzha-dannykh/ (дата обращения: 26.11.2021).

12. Cryptocurrency information about Belarus. 2021. URL: https://triple-a.io/crypto-ownership-belarus/ (date of access: 20.09.2021).

13. Бандык О. Профессионально об актуальном. Краудфандинг: понятие и перспективы применения. 2019. URL: https://pravo.by/novosti/novosti-pravo-by/2019/february/32656/ (дата обращения: 04.03.2020).

14. Arner D., Barberis J., Buckley R. RegTech: Building a Better Financial System // Handbook of Blockchain, Digital Finance, and Inclusion. 2018. Vol. 1. P. 359–373. DOI: 10.1016/B978-0-12-810441-5.00016-6.

15. ЕЭК зашла в белорусский ПВТ. 2021. URL: https://afn.today/news/i/291110 (дата обращения: 02.09.2020).

References

1. Beyond COVID-19 Advancing Digital Business Transformation in the Eastern Partner Countries. 2021. 116 p. Available at: https://www.oecd.org/eurasia/Covid19_%20Advancing%20digital%20business%20transformation%20in%20the%20EaP%20countries.pdf (accessed 15.11.2021).

2. CBDC. Central bank digital currencies: foundational principles and core features: Bank for International Settlements. 2020. 21 p. Available at: https://www.bis.org/publ/othp33.pdf (accessed 07.01.2022).

3. Boehm J., Smith J. Derisking digital and analytics transformations. Risk Practice. *McKinsey Report*. 2021. 12 p. Available at: https://www.mckinsey.com/business-functions/risk/our-insights/derisking-digital-and-analytics-transformations (accessed 05.01.2022).

4. Politou E., Alepis E., Patsakis C. Profiling tax and financial behaviour with big data under the GDPR. *Computer Law & Security Review*, 2019, vol. 35, pp. 306–329. DOI: 10.1016/j.clsr.2019.01.003.

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. European Commission (EC): Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. JOIN. 2013. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 (accessed 08.06.2020).

6. Bondarchuk N. The US government will pay whistleblowers and “white hat hackers” rewards in cryptocurrencies. 2021. Available at: https://bits.media/pravitelstvo-ssha-budet-vyplachivat-informatoram-i-belym-khakeram-nagrady-v-kriptovalyutakh/ (accessed 17.08.2021) (In Russian).

7. Scientific degree of safety. *Kommersant”* [Kommersant]. 2022. Available at: https://www.kommersant.ru/doc/5183598 (accessed 29.01.2022) (In Russian).

8. Education in the Republic of Belarus. Minsk, 2021. 40 p. Available at: https://www.belstat.gov.by/upload/iblock/5d6/5d62c11490270d88d396c8788f28b95d.pdf (accessed 11.12.2021) (In Russian).

9. Education in the Republic of Belarus (2019/2020 academic year). Minsk, 2019. 48 p. Available at: https://www.belstat.gov.by/upload/iblock/eef/eef2ad012db2ea8aaf4dbea2647d5a90.pdf (accessed 11.12.2021) (In Russian).

10. Domeyer A., Hieronimus S., Klier J., Weber T. Government data management for the digital age: McKinsey&Company. 2021. 9 p. Available at: https://www.mckinsey.com/industries/public-and-social-sector/our-insights/government-data-management-for-the-digital-age (accessed 20.09.2021).

11. A new data exchange has been launched in Shanghai. 2021. Available at: https://bluescreen.kz/news/10095/v-shankhaie-zarabotala-novaia-birzha-dannykh/ (accessed 26.11.2021) (In Russian).

12. Cryptocurrency information about Belarus. 2021. Available at: https://triple-a.io/crypto-ownership-belarus/ (accessed 20.09.2021).

13. Bandyk O. Professionally about the actual. Crowdfunding: concept and prospects for application. 2019. Available at: https://pravo.by/novosti/novosti-pravo-by/2019/february/32656/ (accessed 04.03.2020) (In Russian).

14. Arner D., Barberis J., Buckley R. RegTech: Building a Better Financial System. *Handbook of Blockchain, Digital Finance, and Inclusion*, 2018, vol. 1, pp. 359–373. DOI: 10.1016/B978-0-12-810441-5.00016-6.

15. The EEC entered the Belarusian HTP. 2021. Available at: https://afn.today/news/i/291110 (accessed 02.09.2020) (In Russian).

Информация об авторе

Криштаносов Виталий Брониславович − кандидат экономических наук, докторант Белорусского государственного технологического университета (220006, г. Минск, ул. Свердлова, 13а, Республика Беларусь). E-mail: Krishtanosov@mail.ru

Information about the author

Kryshtanosau Vitaly Bronislavovitch − PhD (Economics), post-doctoral student. Belarusian State Technological University (13a, Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: Krishtanosov@mail.ru

Поступила 28.09.2022