

УДК 338.242

В. Б. Криштаносов

Белорусский государственный технологический университет

**ФОРМИРОВАНИЕ ЭФФЕКТИВНОЙ ИНСТИТУЦИОНАЛЬНОЙ
СРЕДЫ УПРАВЛЕНИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИЕЙ ЭКОНОМИКИ**

Проведен комплексный анализ развития цифровой инфраструктуры и соответствующей трансформации экономики Республики Беларусь. С целью обеспечения формирования институциональной модели управления цифровыми рисками и угрозами в условиях цифровой трансформации экономики страны подтверждена целесообразность реализации комплекса мероприятий на уровне надгосударственного регулирования; на национальном уровне; на уровне бизнес-среды. Разработаны показатели оценки экономической эффективности управления цифровыми активами относительно зафиксированных случаев нивелирования угроз; ограничения в управлении киберрисками относительно бюджета организации; стоимость снижения риска; рентабельность инвестиций в обеспечение цифровой безопасности относительно потенциальных потерь. Обоснована необходимость формирования условий для создания национальных кластеров, взаимодействующих на общей цифровой платформе с кластерами ЕАЭС (кросс-кластерное взаимодействие); расширение взаимодействия Республики Беларусь со странами ЕАЭС с целью создания Центра цифровой безопасности ЕАЭС с компетенциями и функционалом, аналогичным Европейской организации кибербезопасности. Аргументирована целесообразность централизации цифровых компетенций и полномочий по цифровой трансформации национальной экономики в едином органе государственного управления (Национальном центре цифровой трансформации при Президенте Республики Беларусь), имеющем соответствующие компетенции по цифровизации и интеграции цифровых систем. Обосновано формирование базиса институциональной модели управления рисками и угрозами цифровой трансформации экономики Республики Беларусь, включающего организационные, институциональные, правовые и технологические элементы, в том числе национальную концепцию построения интегрированной цифровой экосистемы с учетом потенциала выявленных угроз цифровой трансформации традиционных отраслей экономики и в рамках концепции «новой экономики 2.0».

Ключевые слова: цифровая трансформация, институциональная модель управления, цифровая безопасность.

Для цитирования: Криштаносов В. Б. Формирование эффективной институциональной среды управления цифровой трансформацией экономики // Труды БГТУ. Сер. 5, Экономика и управление. 2025. № 1 (292). С. 13–25.

DOI: 10.52065/2520-6877-2025-292-2.

V. B. Kryshtanosau

Belarusian State Technological University

**FORMATION OF AN EFFECTIVE INSTITUTIONAL ENVIRONMENT
FOR MANAGEMENT OF DIGITAL TRANSFORMATION OF THE ECONOMY**

There has been a comprehensive analysis of the development of digital infrastructure and the corresponding transformation of the economy of the Republic of Belarus carried out. In order to ensure the formation of an institutional model for managing digital risks and threats in the context of the digital transformation of the country's economy, there have been justified the feasibility of implementing a set of measures at the level of supranational regulation; at the national level; at the business environment level. Indicators have been developed to assess the economic efficiency of digital asset management relative to recorded cases of threat mitigation; limitations in cyber risk management relative to the organization's budget; cost of risk reduction; return on investment in ensuring digital security relative to potential losses. There has been the necessity of creating conditions for the creation of national clusters interacting on a common digital platform with EAEU clusters (cross-cluster interaction) substantiated; expanding the interaction of the Republic of Belarus with the countries of the EAEU with the aim of creating the EAEU Digital Security Center with competencies and functionality similar to the European Cyber Security Organization. There has been the expediency of centralizing digital competencies and powers for the digital transformation of the national economy in a single government body (National

Center for Digital Transformation under the President of the Republic of Belarus), which has the corresponding competencies for digitalization and integration of digital systems substantiated. There has been the formation of a basis for an institutional model for managing risks and threats to the digital transformation of the economy of the Republic of Belarus substantiated, including organizational, institutional, legal and technological elements, including the national concept of building an integrated digital ecosystem, taking into account the potential of identified threats to the digital transformation of traditional sectors of the economy and within the concept of “new economy 2.0”.

Keywords: digital transformation, institutional management model, digital security.

For citation: Kryshanosau V. B. Formation of an effective institutional environment for management of digital transformation of the economy. *Proceedings of BSTU, issue 5, Economics and Management*, 2025, no. 1 (292), pp. 13–25 (In Russian).

DOI: 10.52065/2520-6877-2025-292-2.

Введение. Обеспечение устойчивости систем производства и управления Республики Беларусь в условиях нарастающих рисков и угроз цифровой трансформации экономики требует разработки эффективной и комплексной модели управления рисками в контексте особенностей развития и направлений цифровой трансформации экономической системы страны [1]. Необходимо 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 отсутствии единого признанного стандарта управления.

Основная часть. Принимая во внимание ограниченность ресурсов страны, представляется целесообразным формирование национальной политики в области регулирования цифровых рисков с учетом данных факторов и потенциала выявленных угроз. *Национальная система управления цифровыми рисками* с точки зрения обеспечения устойчивости развития цифровой трансформации экономики и эффективности принимаемых решений, как показывает международная практика формирования регуляторно-институциональной экосистемы цифровой трансформации экономики, предполагает институционализацию цифровых метатехнологий и концепций, создание соответствующей институциональной инфраструктуры регулирования цифровой трансформации [2]. Международный опыт свидетельствует о формировании специализированных органов управления цифровой трансформации в формате министерства или департамента в зависимости от особенностей структуры правительства той или иной страны [3]. С учетом особенностей высокой степени централизации и значительной роли государства в управлении/регулировании белорусской экономики, необходимости проактивного межведомствен-

ного взаимодействия *институциональная инфраструктура* государственного регулирования цифровой трансформации может быть представлена *Национальным центром цифровой трансформации* при Президенте Республики Беларусь (НЦЦТ), имеющим соответствующие компетенции по трансформации и интеграции цифровых систем, включающих:

1) разработку и внедрение системы формализации оценки цифровых рисков (совместно с Оперативно-аналитическим центром при Президенте Республики Беларусь (ОАЦ)) [4];

2) 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, а автоматизация данных процессов позволит внедрить новый инструментарий с меньшими затратами, обеспечить раннее выявление и устранение угроз и рисков;

3) использование «упреждающего регулирования», направленного на прогнозирование изменений в экосреде на ранних этапах с целью их учета при формировании текущих и будущих стратегий регулирования;

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

Важнейшим аспектом успешной реализации государственных программ является *образование системных горизонтальных и вертикальных связей* как на уровне компетентных органов государственного управления, так и на уровне привлеченных организаций в рамках государственно-частного партнерства. На низовом уровне представляется целесообразным формирование специализированной управленческой структуры, состоящей из ответственных за минимизацию рисков цифровой трансформации [5] сотрудников на уровне отраслей и конкретных предприятий (рис. 1).

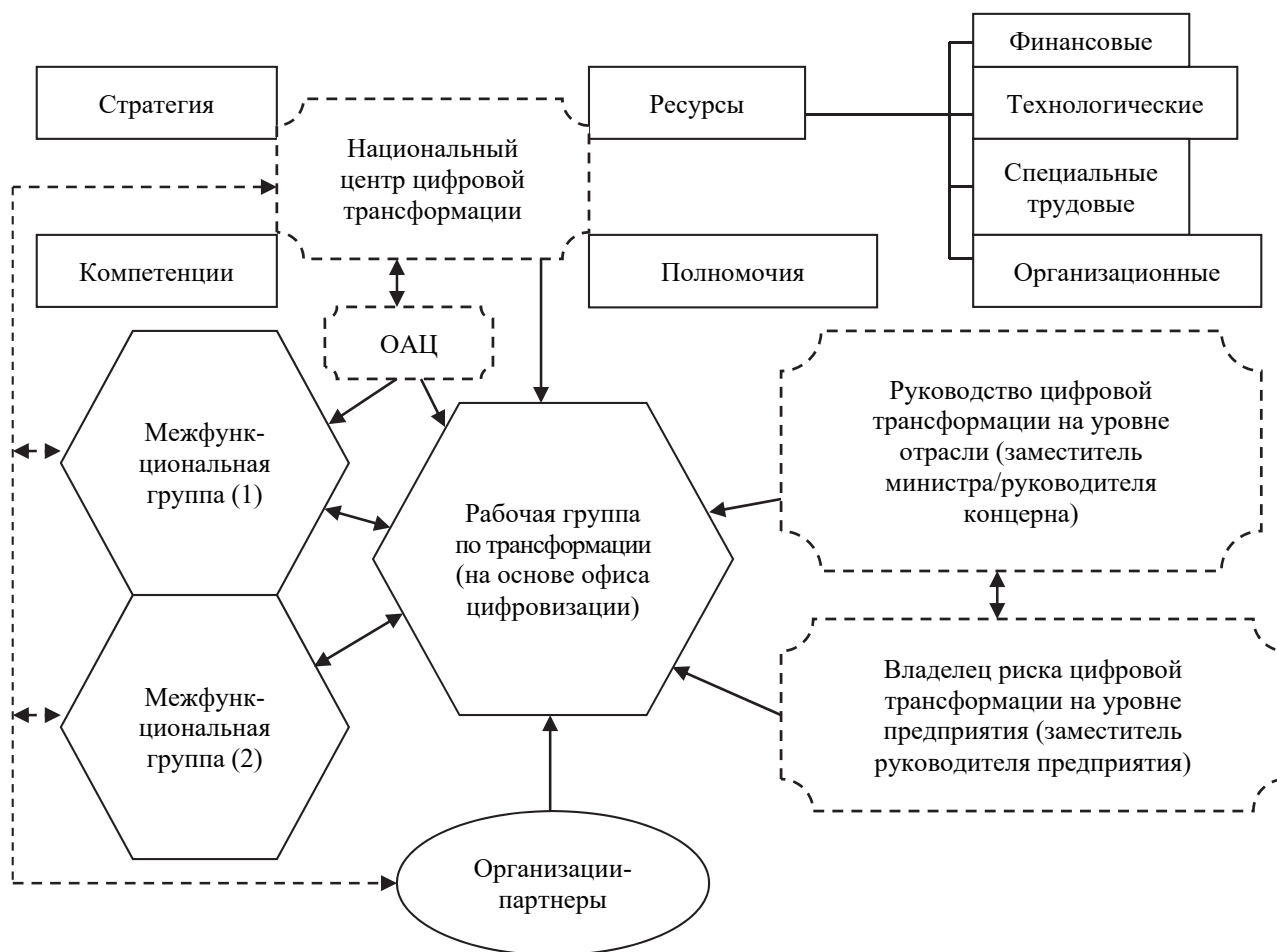


Рис. 1. Организационная схема взаимодействия уполномоченных органов государственного управления по осуществлению цифровой трансформации (разработана автором)

Данная организационная структура должна включать:

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

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

- рабочие группы по трансформации (на основе офисов цифровизации с усиленным функционалом цифровой безопасности, с учетом возможностей, предоставленных ОАЦ Указом № 40 от 14 февраля 2023 г.) с участием компетентных сотрудников НЦЦТ, 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), которые смогут проработать направления взаимодействия с использованием механизмов «Национальной цифровой лаборатории»¹);

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

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 цифровой трансформации* 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 цифровой трансформации. Профилирование позволит выявить и определить приоритетность реагирования на цифровые риски и угрозы, что в сочетании с анализом результатов регуляторных экспериментов и инноваций, а также мониторингом и оценкой на основе BDA может стать основой 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. Для управления рисками НЦЦТ, как показывает анализ международного опыта, представляется целесообразным использование *поэтапной модели цифровой трансформации*, в рамках которой на первом этапе осуществляется цифровое зондирование и формирование цифровых сценариев для подготовки цифрового исследования и соответствующей формализации. На втором этапе проводится 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, в том числе инфраструктуры и административных процессов, а также управление персоналом и развитие цифровых компетенций.

Финансирование комплекса мероприятий возможно осуществлять за счет Белорусского инновационного фонда (первый и второй этапы) путем его переподчинения НЦЦТ в части стратегии развития или программы социально-экономического развития, а также собственных средств отраслей и предприятий, участвующих в программе трансформации (третий этап).

Для реализации представленной модели необходимо формировать *универсальную систему управления рисками* как на уровне *центров цифрового развития* (во взаимодействии с ОАЦ), так и на уровне *рабочих групп по трансформации* с учетом их адаптации к условиям и характеристикам отраслей и конкретных предприятий. Это позволяет осуществить ряд оценок, включая:

- 1) экономическую эффективность управления цифровыми активами (затраты $(7 + 8 + 9 + 10 + 11)$ относительно *закрепленных случаев* нивелирования угроз (I) $(3 + 4 + 5 + 6)$);
- 2) ограничения в управлении киберрисками (затраты $(7 + 8 + 9 + 10 + 11)$ относительно бюджета организации);
- 3) стоимость снижения риска (затраты $(7 + 8 + 9 + 10 + 11)$);
- 4) рентабельность инвестиций в обеспечение цифровой безопасности (затраты $(7 + 8 + 9 + 10 + 11)$)

относительно потенциальных потерь (II) $(2, 3, 4, 5, 6)$) (таблица).

На *уровне рабочих групп по цифровой трансформации* представляется возможным также 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.

Для обеспечения комплексности и системности реализации цифровой трансформации видится необходимым в рамках государственно-частного партнерства привлечение коммерческих организаций-партнеров, например компетентных аудиторских компаний, специализирующихся на оценке рисков и киберугроз. При этом задачей НЦЦТ является отбор уполномоченных компаний для участия в программе цифровой трансформации 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 выступает подписание соглашений о конфиденциальности. Условиями эффективности реализации данной модели являются комплексность, системность и цикличность ее имплементации, которые позволяют сформировать скоординированный ответ на возникающие угрозы и риски, выстроить систему взаимодействия на различных уровнях управления. Кроме того, модель позволит осуществить поступательный переход от подхода «управление рисками» к подходу «управление 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 системы².

Экспликация составляющих блоков стратегии цифровизации/цифровой трансформации, регулирования отдельных цифровых инноваций и концепций, финансового рынка, цифровой безопасности на элементы институциональной среды позволяет выделить следующие перспективные направления развития национальной регуляторно-институциональной экосистемы (рис. 2).

Схема управления цифровыми рисками и угрозами на уровне отраслей и предприятий
(разработана автором по результатам исследования)

Перечень возможных рисков и угроз цифровой трансформации	Вероятность наступления	Актуальные (I) и потенциальные (II) потери			Каскадный эффект*	Затраты на управление рисками и угрозами				Стоимость реализации перечня 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 (НЦЦТ – группы трансформации – уровень отрасли – уровень предприятия), так и по горизонтали на уровне конкретного хозяйствующего субъекта.

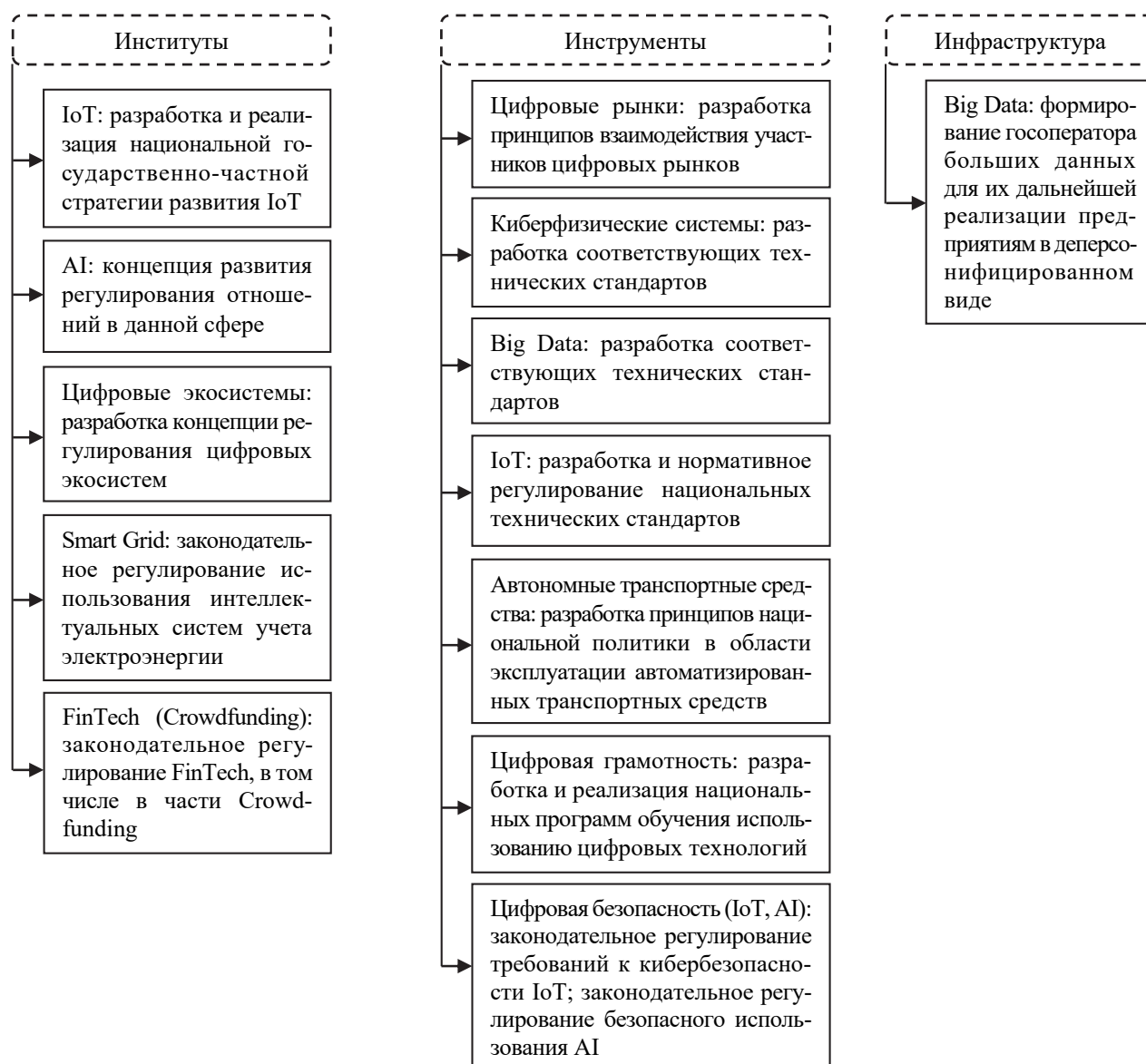


Рис. 2. Перспективные направления развития регуляторно-институциональной экосистемы Республики Беларусь (разработано автором по результатам исследования)

С учетом данных рис. 2 представляется возможным сформировать следующие предложения по нивелированию (минимизации) рисков и угроз цифровой трансформации экономики Республики Беларусь.

1. *Блок стратегии цифровой трансформации:* обеспечение нормативно-правового регулирования в области цифрового развития, в том числе:

- разработка *долгосрочной стратегии национальной цифровой трансформации* (горизонт планирования 20–30 лет), 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, а также *среднесрочной стратегии* (горизонт планирования 5–7 лет). В первом случае осуществляется «визионерство» качественных и количественных характеристик и результатов трансформации национальной экономики с привязкой к актуальным цифровым концепциям Industry 4.0, Agriculture 4.0, Smart City, Smart Grid, Smart Supply Chain, FinTech, CBDC, E-Government, PropTech и пр. Во втором случае разрабатывается план мероприятий по достижению желаемых результатов цифровой трансформации с различными уровнями детализации: для конкретных предприятий (проектов), отраслей или секторов экономики, национальной экономики в целом;

- разработка *концепции* и создание *цифровых кластеров* вокруг крупных реформируемых белорусских предприятий, которые бы вовлекли в процесс цифровой трансформации национальные малые и средние предприятия (МСП), действующих и потенциальных поставщиков комплекующих, финансовые организации, предоставляющие соответствующие услуги, для адаптации (синхронизации) общих цифровых решений производства и управления, что позволит оптимизировать затраты на реализацию комплексных проектов цифровой трансформации, достичь необходимого уровня синергии и повысить тем самым общую эффективность трансформации;

- реализация политики развития *целостных государственных экосистем*, которые позволяют оцифровывать все транзакции и взаимодействия между государством, юридическими и физическими лицами; использование принципа *общей (интероперабельной) платформы* при реализации цифровых проектов межведомственного и межотраслевого характера; приведение действующих платформ к общим стандартам, позволяющим их интегрировать без угроз потери данных и для сохранения безопасности; обеспечение полноты и гарантий достоверности сведений в ГИР (ГИС); создание национальной модели цифровых данных;

- формирование среды для развития цифровых рынков;

- реализация *национальной программы создания цифровых портретов объектов хозяйствования* отраслевого и микроуровня вне зависимости от формы собственности, приоритезируя:

- а) прибыльные предприятия (условно прибыльные, имеющие потенциал роста);

- б) предприятия критической инфраструктуры [6];

- в) флагманские предприятия отраслей и предприятия, входящие в их цепочку поставок;

- интенсификация цифровых преобразований и обмен лучшими практиками в рамках отдельной платформы сотрудничества ЕАЭС по таким направлениям, как:

- а) формирование единого цифрового рынка, развитие общих (интегрированных) онлайн-платформ;

- б) разработка и внедрение общих цифровых стандартов, программ повышения цифровых навыков населения, агрегирование финансовых, технических и кадровых ресурсов;

- в) реализация универсальных подходов к регулированию цифровых финансовых технологий;

- г) разработка общих регламентов и политики имплементации технологий AI;

- д) создание на уровне ЕАЭС организации по вопросам цифровой безопасности (Центра цифровой безопасности ЕАЭС) и распределенной сети национальных координационно-консультационных центров и разработка соответствующей правовой базы;

- е) унификация законодательства в сфере защиты персональных данных;

- ж) создание центра компетенций ЕАЭС в области промышленной, технологической и исследовательской цифровой безопасности и сети национальных координационных центров [7];

- з) повышение конкурентоспособности предприятий за счет цифровой трансформации посредством создания совместного фонда/инкубатора для перспективных стартапов, возможно, на базе Международного евразийского индустриального фонда³.

2. Блок регулирования цифровой безопасности.

2.1. *Развитие нормативно-правового, организационного, технологического и финансового обеспечения национальной цифровой безопасности*, в том числе:

- принятие *основанного на оценке риска подхода к регулированию и надзору*, который соответствует стандартам соразмерности и прозрачности;

- обеспечение *суверенитета* в киберпространстве, предполагающего защиту национальных информационных систем и информационных ресурсов от внешних угроз, вмешательства, атак или ущерба, в том числе благодаря разработке и внедрению *национальных программных продуктов*,

снижению зависимости Беларуси от иностранных поставщиков технологий и цифровых услуг. В качестве механизма стимулирования развития данного направления может стать создание государственного перечня национальных программных продуктов, в отношении закупки которого может применяться более низкая ставка НДС (например, 18%);

– разработка и принятие *закона о национальной цифровой безопасности*, который будет носить комплексный и системный характер, учитывать перечень действующих, а также модели прогнозирования и оценки будущих рисков и угроз, охватывать 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, PropTech, Industry 4.0, Agriculture 4.0, Smart Supply Chain, Smart Grid, E-Commerce, Telemedicine с особым вниманием к проблематике AI, IoT, Cloud Computing, Blockchain, Big Data;

– разработка и внедрение *национальных стандартов* в отношении аккумулирования, хранения, обмена и использования данных, соответствующих принципам безопасности, конфиденциальности, прозрачности и целостности;

– законодательное закрепление определения *«государство – спонсор киберпреступлений»*, предполагающего широкое трактование с включением 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;

– формирование на уровне государства *резервных фондов противодействия цифровым рискам и угрозам* (финансовых, материальных, информационных) на отраслевом и национальном уровнях для нивелирования последствий кибератак, в особенности в отношении критической инфраструктуры;

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

– использование для управления рисками *поэтапной модели цифровой трансформации*, где на первом этапе осуществляются 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;

– разработка *национального законодательства, направленного на обеспечение безопасности технологий IoT и 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.

2.2. Обеспечение комплексного операционного реагирования на кибератаки, в том числе:

– разработка *планов кризисного реагирования* на внешние цифровые угрозы, а также 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;

– введение *ответственности* в отношении выбора частными предприятиями *оптимальных в контексте безопасности цифровых технологий*;

– разработка и внедрение *профессиональных стандартов* по цифровой безопасности для сотрудников, обеспечивающих защиту цифровых систем объектов критической инфраструктуры.

2.3. Обеспечение цифровой безопасности критической инфраструктуры, в том числе:

– разработка *стандартов и критериев, выделяющих и классифицирующих 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;

– разработка и имплементация секторальных и индивидуальных повторяющихся *системных подходов к выявлению, оценке и управлению рисками*

цифровой безопасности, вне зависимости от размера организации, подверженности угрозам или актуального уровня сложности цифровой безопасности;

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

- подготовка ежегодного *специализированного отчета о национальном профиле рисков*, отражающего актуальную оценку существующих и прогнозируемых рисков и угроз в контексте национальной безопасности с учетом цифровой трансформации, критической инфраструктуры, а также важнейших механизмов государственного управления и социального обеспечения.

3. Блок *регулирования отдельных цифровых инноваций и концепций* (главным образом в форме государственно-частного партнерства), в том числе:

- разработка национальной политики в сфере стимулирования развития и регулирования *целостных частных платформенных экосистем, AI, IoT, Big Data и киберфизических систем*;

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

- «разработка комплекса цифровых систем и сервисов, интегрированных в национальную *систему цифровой идентификации* (цифровыми паспортами и ID-картами), обладающих такими характеристиками, как простота, безопасность, надежность и конфиденциальность»;

- 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, PropTech, E-Commerce, Telemedicine;

- разработка национальной политики в сфере *Smart Grid* с учетом ввода в эксплуатацию атомной станции и формирования объединенного рынка энергии с Российской Федерацией;

- создание *Национальной цифровой лаборатории*, проведение комплексных национальных исследований в сфере AI/ML, *цифрового моделирования систем* (BIM, Digital Twins), *IoT, автономных транспортных средств* (в том числе разработка регламентов для их допуска в эксплуатацию);

- разработка национальной политики в сфере развития *цифровых навыков населения*, развитие учебных программ и цифровых образовательных платформ, направленных на противодей-

ствие тенденциям высвобождения малопроизводительной рабочей силы в условиях цифровой трансформации экономики;

- формирование специализированной структуры (на базе Национального центра цифровой трансформации), агрегирующей кадровый потенциал и соответствующие компетенции для реализации функций так называемого *технологического цифрового спецназа*; разработка конкурсных процедур для привлечения данных специалистов на конкретные предприятия с целью проведения цифрового аудита, выработки предложений и инициации проекта цифровой трансформации с подготовкой требуемых специалистов для его проведения на местах и последующего мониторинга и контроля промежуточных результатов;

- 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.

«...Важнейшим условием эффективного внедрения механизмов управления данными на основе концепции E-Government (как и Smart City, PropTech) является обеспечение *качества цифровых данных*, агрегируемых на всех уровнях». Кроме того, технологические требования современной ИТ-архитектуры концепции 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, 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 КНР⁴). Реализация концепции E-Government может стать важным

драйвером для развития 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.

4. Блок регулирования финансового рынка, в том числе:

- формирование привлекательной среды для внедрения цифровых бизнес-моделей в финансовом секторе (FinTech), возможно, путем организации «правовой песочницы» для данного вида деятельности;

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

- обеспечение на законодательном уровне проблематики цифровой безопасности в финансовом секторе (FinTech, CBDC, RTGS, Crowdfunding, Mobile Money, InsurTech, Blockchain, Cryptocurrency, RegTech, цифровая идентификация);

- адаптация белорусской банковской системы к технологиям CBDC с учетом выявленных угроз и рисков. Как показал ряд исследований [8, с. 12–13], оптимальным механизмом имплементации технологии CBDC в разрезе обеспечения стабильности функционирования денежно-кредитной системы, цифровой безопасности финансовых цифровых систем, облегчения адаптации концепции цифровых валют населением и субъектами хозяйствования является эмиссия цифрового белорусского рубля при параллельном временном обороте наличных денежных знаков. Данный подход позволит выявить возможные уязвимости финансовой системы как с точки зрения организационных проблем, так и устойчивости цифровой инфраструктуры. Преимуществами эмиссии национальной CBDC могут быть:

- а) рост прозрачности платежей и расчетов, снижение рисков ПОД-ФТ;

- б) низкие (возможно нулевые) тарифы для проведения расчетов;

- в) новый уровень финансовой доступности для населения;

- г) улучшение устойчивости банковской системы;

- д) продвижение и популяризация цифровых расчетных механизмов;

- е) сохранение привлекательности белорусских платежных инструментов в сравнении с государствами-соседями.

Недостатками концепции являются:

- а) значительный объем капиталовложений для развертывания системы CBDC;

- б) риски и угрозы трансформации финансовой системы, не выявленные на проектной стадии;

- в) потенциальная зависимость от стандартов CBDC, принимаемых в Российской Федерации в случае, если Беларусь не инициирует общую программу исследования и разработки CBDC, например, на уровне ЕАЭС, Союзного государства или в сотрудничестве с КНР [9, с. 13–20];

- специальное законодательное регулирование Crowdfunding, отсутствие которого, как отмечают эксперты, в должной мере не обеспечивает защиту прав участников подобного рода договоров [10]. С учетом международной практики представляется целесообразным разработать в Беларуси соответствующие нормативные акты, регламентирующие функционирование Crowdfunding, включающие требования о регистрации платформ в финансовых органах для получения соответствующих лицензий на ведение бизнеса, поддержания определенного минимального уровня капитала, использования банковских учреждений для хранения средств клиентов, предоставления регулярных отчетов об обороте предоставляемых кредитных ресурсов, обмена информацией о кредитной истории клиентов Crowdfunding площадок с банками;

- защита интересов белорусских граждан от мошенничества на рынке криптоактивов путем информационного обеспечения и введения ограничения на транзакции для физических лиц, не обладающих определенной квалификацией, опытом и навыками. Представляется целесообразным дальнейшее совершенствование нормативной базы для урегулирования споров при осуществлении транзакций с криптовалютами, а также формирование законодательных основ для передачи прав собственности на криптоактивы. Министрству по налогам и сборам Республики Беларусь необходимо проработать и сформировать систему налогообложения данной сферы, которая бы включала следующие элементы:

- а) создание механизмов мониторинга коммерческих транзакций с криптоактивами, в особенности трансграничных, в целях налогообложения;

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

- в) налогообложение доходов, полученных майнерами;

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

С учетом наличия системных рисков для стабильного функционирования национальной финансовой системы в перспективе использования криптовалют в платежных сервисах и в качестве инвестиционного инструмента необходима разработка и реализация механизмов, направленных на снижение анонимности учетных записей и персональных данных участников криптовалютного рынка. Для Республики Беларусь представляется целесообразным рассмотреть возможность реализации такого рода ИТ-решений на уровне Союзного государства (ЕАЭС) за счет аккумуляции финансовых, технологических ресурсов и компетенций стран-членов;

– *ужесточение банковского надзора и требований в отношении FinTech* организаций и банковских продуктов, поскольку, 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 к инновациям в финансовом секторе, позволяющим обеспечить непрерывность мониторинга, получение информации в режиме, близком к реальному времени, является концепция *SupTech*. В-четвертых, 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 и адекватным требованиям в сфере борьбы ПОД-ФТ. В-пятых, 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.

Важнейшим аспектом реализации комплексной программы трансформации национальной экономики является 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 [11, с. 102–104], финансирование цифровой трансформации может осуществляться с использованием следующего инструментария:

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

б) ваучеры – на предоставление менеджменту МСП бесплатных консультаций и специализированного обучения;

в) кредиты – облегчение доступа МСП к кредитным финансовым ресурсам за счет обеспечения соответствующих гарантий;

г) косвенные финансовые стимулы для цифровой трансформации, в том числе ускоренная амортизация при покупке определенных «цифровых» материальных активов.

В Республике Беларусь для целей финансирования инноваций функционируют три механизма: *фонд ГКНТ* (Белорусский инновационный фонд, БИФ), *фонд универсального обслуживания связи и информатизации*, *местные фонды инноваций*. В рамках Белорусского инновационного фонда функционирует венчурный фонд, а также отдельный совместный белорусско-российский венчурный фонд. Таким образом, основными механизмами финансирования БИФ являются целевые займы (50% от ставки рефинансирования), венчурное финансирование, гранты. Кроме того, в рамках Указа Президента № 381 «О цифровом развитии» от 29 ноября 2023 г. источником финансирования экспертизы в сфере цифрового развития определены средства, поступающие государственному учреждению «Секретариат Наблюдательного совета Парка высоких технологий». С учетом ограниченности финансовых ресурсов для проведения комплексной цифровой трансформации экономики страны целесообразно создание следующего механизма финансирования цифровых инноваций:

– *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* (аккумулирующего инвестиционные и венчурные ресурсы ГКНТ и Минсвязи) за счет средств Евразийского индустриального фонда и 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;

– 35% *затрат* главным образом на финансирование цифровой трансформации конкретных флагманских предприятий могут взять на себя *отраслевые организации и фонды инноваций этих предприятий* (в том числе местные фонды инноваций). 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;

– 15% *затрат* на развитие экосистем в сферах E-Commerce, Cloud Computing, AI и пр. могут быть покрыты за счет *средств ПБТ и частных коммерческих предприятий*, заинтересованных в предоставлении соответствующих услуг, участия 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 ИКТ организации в производственные и сбытовые цепочки производственных предприятий и обеспечить долгосрочность коммерческих отношений по определенным направлениям. Предложенные механизмы направлены, в первую очередь, на реализацию ключевых мероприятий государственной программы цифровой трансформации. Вместе с тем с целью агрегирования значительных финансовых ресурсов и повышения финансовой доступности для *стартапов* требуется *модернизация механизмов государственно-частного партнерства*. Представляется целесообразным в этой связи сфокусировать деятельность на приоритетных направлениях цифровой трансформации с учетом их инновационности и социальной значимости, например, *сформировав фонд MedTech*. Кроме того, необходим механизм создания *пула государственных и частных фондов* для финансирования крупных инновационных проектов.

Таким образом, с учетом ограниченности ресурсов страны представляется целесообразным формирование национальной политики в области регулирования цифровых рисков с учетом потенциала выявленных угроз цифровой трансформации как традиционных отраслей экономики, так и в рамках концепции «новой экономики 2.0». Институциональная инфраструктура регулирования цифровой трансформации может быть представлена Министерством цифровой трансформации, имеющим соответствующие компетенции по цифровой трансформации и ин-

теграции 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.

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 [12]; обеспечение суверенитета в киберпространстве; разработка и внедрение национальных программных продуктов и стандартов (в том числе на базе Open Source технологий); разработка планов кризисного реагирования на внешние цифровые угрозы, в том числе создание единой государственной системы цифрового мониторинга и групп быстрого ИТ-реагирования; формализованное описание профилей цифровых угроз; развитие страхового инструментария обеспечения гарантий исполнения обязательств 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. Блок регулирования цифровых инноваций 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 AI. Государственное регулирование в отношении FinTech требует обеспечения безопасности как на уровне конкретных финансовых организаций, отраслей, так и страны в целом [13].

Заключение. Таким образом, институциональная инфраструктура регулирования цифровой трансформации может быть представлена Национальным центром цифровой трансформации при Президенте Республики Беларусь, имеющим соответствующие компетенции по цифровизации и интеграции цифровых систем. Условием проведения эффективной национальной политики в области цифровой трансформации является осуществление комплексного последовательного анализа цифровой трансформации на уровне предприятий, отраслей и секторов экономики для формирования национальной карты цифровой трансформации экономики, составленной на основе цифровых портретов (профилирования) субъектов хозяйствования по

предложенной методике. Управление рисками целесообразно осуществлять по авторской модели системного подхода с последовательным проведением комплекса мероприятий по выявлению угроз, адаптации экосистемы, реализа-

ции мер противодействия, внедрению эффективного управления и совершенствованию подходов, а также по модели поэтапного комплексного осуществления цифровой трансформации на уровне страны.

¹ «Национальная цифровая лаборатория» представляет собой «...зонтичную организацию», осуществляющую регулирование и интеграцию разрозненных проектов разработки цифровых решений для различных секторов и направлений деятельности в рамках университетов, технопарков, ПВТ и т. д.

² На микроуровне отдельных цифровых проектов (без участия государства) порядок их запуска может включать следующие шаги: а) оценка выгод (возможностей) цифровой трансформации бизнеса, выявление цифровых направлений генерирования дополнительной выгоды, оценка текущих возможностей ИТ-службы; б) оценка рисков цифровой трансформации бизнеса; в) оценка затрат на цифровую трансформацию бизнеса; г) определение приоритетов, разработка графика запуска проектов; д) определение источников финансирования, поиск грантов, льготных кредитов на проекты по цифровой трансформации бизнеса.

³ В 2020 г. странами ЕАЭС учрежден Международный евразийский индустриальный фонд, призванный осуществлять финансирование совместных проектов в сфере производственной кооперации и трансфера технологий [14].

⁴ 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» [15].

Список литературы

1. Криштаносов В. Б. Угрозы и риски цифровизации в деятельности корпоративных организаций // Корпоративные стратегии и технологии в условиях ESG – трансформации бизнеса: монография / под ред. И. Ю. Беляевой, О. В. Даниловой. М.: КНОРУС, 2023. 332 с.
2. Новикова И. В., Криштаносов В. Б. Формирование экосистемы цифровой экономики: технологический и институциональный аспекты, международный опыт и имплементация в Республике Беларусь // Белорусский экономический журнал. 2021. № 4. С. 124–137.
3. Криштаносов В. Б. Цифровизация экономики Республики Беларусь и национальная безопасность: современные концептуально-аналитические подходы: в 2 т. Минск: БГТУ, 2023. 2 т.
4. Криштаносов В. Б. Регулирование цифровой экономики: опыт Республики Беларусь // Бизнес. Инновации. Экономика: сб. науч. ст. / Ин-т бизнеса БГУ. Минск, 2022. Вып. 6. С. 60–70.
5. Криштаносов В. Б. Угрозы и риски цифровой экономики на секторальном уровне // Труды БГТУ. Сер. 5, Экономика и управление. 2022. № 1. С. 28–52.
6. Криштаносов В. Б. Безопасность критической инфраструктуры под угрозой // Мир перемен. 2021. № 2. С. 55–69.
7. Криштаносов В. Б. Формирование институциональной экосистемы цифровой экономики в ЕС и ЕАЭС: сравнительный анализ // Социальные новации и социальные науки. 2022. № 2. С. 140–154.
8. Новикова И. В., Криштаносов В. Б. Цифровые валюты центральных банков: современные тенденции и возможности имплементации в Республике Беларусь // Банковский вестник. 2021. № 4/693. С. 13–20.
9. CBDC. Central bank digital currencies: foundational principles and core features. URL: <https://www.bis.org/publ/othp33.pdf> (date of access: 07.01.2022).
10. Бандык О. Профессионально об актуальном. Краудфандинг: понятие и перспективы применения. URL: <https://pravo.by/novosti/novosti-pravo-by/2019/february/32656/> (дата обращения: 04.03.2020).
11. Beyond COVID-19 Advancing Digital Business Transformation in the Eastern Partner Countries. URL: https://www.oecd.org/eurasia/Covid19_%20Advancing%20digital%20business%20transformation%20in%20the%20EaP%20countries.pdf (date of access: 15.11.2021).
12. Криштаносов В. Б. Цифровая экономика: современные направления, динамика развития, вызовы // Труды БГТУ. Сер. 5, Экономика и управление. 2020. № 1. С. 13–30.
13. Криштаносов В. Б. Цифровизация финансового сектора экономики: проблемы и перспективы // Труды БГТУ. Сер. 5, Экономика и управление. 2021. № 1. С. 17–40.
14. ЕЭК зашла в белорусский ПВТ. URL: <https://afn.today/news/i/291110> (дата обращения: 02.09.2020).
15. В Шанхае заработала новая биржа данных. URL: <https://bluescreen.kz/news/10095/v-shankhaie-zarabotala-novaia-birzha-dannykh/> (дата обращения: 26.11.2021).

References

1. Kryshtanosau V. B. Threats and risks of digitalization in the activities of corporate organizations. *Korporativnyye strategii i tekhnologii v usloviyakh ESG – transformatsii biznesa* [Corporate Strategies and Technologies in the Context of ESG – Business Transformation]. Ed. I. Y. Belyaeva, O. V. Danilova. Moscow, KNORUS Publ., 2023. 332 p. (In Russian).
2. Novikova I. V., Kryshtanosau V. B. Formation of the digital economy ecosystem: technological and institutional aspects, international experience and implementation in the Republic of Belarus. *Belorusskiy ekonomicheskii zhurnal* [Belarusian Economic Journal], 2021, no. 4, pp. 124–137 (In Russian).
3. Kryshtanosau V. B. *Tsifrovizatsiya ekonomiki Respubliki Belarus' i natsional'naya bezopasnost': sovremennyye kontseptual'no-analiticheskiye podkhody: v 2 tomakh* [Digitalization of the Economy of the Republic of Belarus and National Security: Modern Conceptual and Analytical Approaches: in 2 vol.]. Minsk, BGTU Publ., 2023. 2 vol. (In Russian).
4. Kryshtanosau V. B. Regulation of the digital economy: the experience of the Republic of Belarus. *Biznes. Innovatsii. Ekonomika* [Business. Innovation. Economy], 2022, issue 6, pp. 60–70 (In Russian).
5. Kryshtanosau V. B. Threats and risks of the digital economy at the sectoral level. *Trudy BGTU* [Proceedings of BSTU], issue 5, Economics and management, 2022, no. 1, pp. 28–52 (In Russian).
6. Kryshtanosau V. B. Critical infrastructure security at risk. *Mir peremen* [World of change], 2021, no. 2, pp. 55–69 (In Russian).
7. Kryshtanosau V. B. Formation of the institutional ecosystem of the digital economy in the EU and the EAEU: a comparative analysis. *Sotsial'nyye novatsii i sotsial'nyye nauki* [Social innovations and social sciences], 2022, no. 2, pp. 140–154 (In Russian).
8. Novikova I. V., Kryshtanosau V. B. Central bank digital currencies: current trends and implementation possibilities in the Republic of Belarus. *Bankovskiy vestnik* [Banking Bulletin], 2021, no. 4/693, pp. 13–20 (In Russian).
9. CBDC. Central bank digital currencies: foundational principles and core features. Available at: <https://www.bis.org/publ/othp33.pdf> (accessed 07.01.2022).
10. Bandyk O. Professionally about the current. Crowdfunding: concept and application prospects. Available at: <https://pravo.by/novosti/novosti-pravo-by/2019/february/32656/> (accessed 04.03.2020) (In Russian).
11. Beyond COVID-19 Advancing Digital Business Transformation in the Eastern Partner Countries. Available at: https://www.oecd.org/eurasia/Covid19_%20Advancing%20digital%20business%20transformation%20in%20the%20EaP%20countries.pdf (accessed 15.11.2021).
12. Kryshtanosau V. B. Digital economy: modern directions, development dynamics, challenges. *Trudy BGTU* [Proceedings of BSTU], issue 5, Economics and management, 2020, no. 1, pp. 13–30 (In Russian).
13. Kryshtanosau V. B. Digitalization of the financial sector of the economy: problems and prospects. *Trudy BGTU* [Proceedings of BSTU], issue 5, Economics and management, 2021, no. 1, pp. 17–40 (In Russian).
14. EEC entered the Belarusian Hi-Tech Park. Available at: <https://afn.today/news/i/291110> (accessed 02.09.2020) (In Russian).
15. New data exchange launched in Shanghai. Available at: <https://bluescreen.kz/news/10095/v-shankhaie-zarabotala-novaya-birzha-dannykh/> (accessed 26.11.2021) (In Russian).

Информация об авторе

Криштаносов Виталий Брониславович – кандидат экономических наук, доцент кафедры менеджмента, технологий бизнеса и устойчивого развития. Белорусский государственный технологический университет (ул. Свердлова, 13а, 220006, г. Минск, Республика Беларусь). E-mail: Krishtanosov@mail.ru

Information about the author

Kryshtanosau Vitaliy Bronislavovich – PhD (Economics), Assistant Professor, the Department of Management, Business Technology and Sustainable Development. Belarusian State Technological University (13a Sverdlova str., 220006, Minsk, Republic of Belarus). E-mail: Krishtanosov@mail.ru

Поступила 05.02.2025