Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

В. Б. Криштаносов

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ РЕСПУБЛИКИ БЕЛАРУСЬ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ КОНЦЕПТУАЛЬНО-АНАЛИТИЧЕСКИЕ ПОДХОДЫ

Монография

В 2-х томах

Том 2

Минск 2023

УДК 338.2-027.45(476)
ББК 65.20
К82

Рассмотрена и рекомендована к изданию редакционно-издательским советом учреждения образования «Белорусский государственный технологический университет».

Рецензенты:
директор Белорусского института стратегических исследований доктор юридических наук *О. С. Макаров*;
проректор по научной работе
УО «Белорусский государственный экономический университет»
доктор экономических наук, профессор *А. А. Быков*

Криштаносов, В. Б.

К82 Цифровизация экономики Республики Беларусь и национальная безопасность: современные концептуально-аналитические подходы : монография : в 2 т. / В. Б. Криштаносов. – Минск : БГТУ, 2023. – Т. 2. – 197 с.

ISBN 978-985-897-064-2.

Во втором томе монографии (первый том вышел в свет в 2023 году) раскрывается проблематика внедрения эффективных механизмов регулирования процессов цифровизации в различных государствах, интеграционных объединениях с учетом экономических условий и национальных особенностей. Приводится анализ становления цифровой экономики в Республике Беларусь, ее адаптации к угрозам и рискам, в том числе в разрезе нарастающей проблематики кибербезопасности.

Материалы монографии могут представлять практический интерес для органов государственного управления в рамках компетенции, при разработке проектов законодательства по регулированию национальной экономики в контексте национальной экономической безопасности.

УДК 338.2-027.45(476)
ББК 65.20

ISBN 978-985-897-064-2 (Т. 2)
ISBN 978-985-897-062-8

ОГЛАВЛЕНИЕ

Глава 3

РЕГУЛИРОВАНИЕ ЦИФРОВОЙ ЭКОНОМИКИ: НЕОБХОДИМОСТЬ И МЕЖДУНАРОДНЫЙ ОПЫТ

В условиях растущих неопределенностей, рисков и угроз экономической безопасности на фоне стремительной цифровизации национальных экономических систем государства стремятся к осуществлению амбивалентной политики, направленной, с одной стороны, на стимулирование технологических инноваций, с другой – на обеспечение безопасности их внедрения. При этом уровень проникновения и гетерогенный характер цифровых систем, их сложность и комплексность воздействия на экономику мотивируют регуляторов и национальные правительства к выстраиванию международного взаимодействия, привлечению опыта и компетенций как на уровне экспертного сообщества, наднациональных институтов, так и наиболее продвинутых в технологическом развитии государств. В данном контексте представляется целесообразным выделить ряд страновых (региональных) особенностей, связанных с регулированием цифровой экономики, ее адаптацией к современным вызовам и угрозам.

3.1. Государственное регулирование экономики в контексте цифровизации: цели, задачи, эволюция

В основе политического регулирования лежат не только социально-политические интересы социальных групп, но и экономические, а политические каналы становятся средством, с помощью которого государство воздействует на экономическую материю в интересах общественной стабильности [880]. Государственное регулирование сопровождает экономических агентов на всем протяжении их жизненного цикла и представляет собой комплекс мер административного, нормативно-правового воздействия на различные сферы экономики и общества для достижения общественно значимых целей [881].

Государственное регулирование носит институциональный характер, при этом необходимость трансформации соответствующих инструментов обоснована «законом необходимого разнообразия» Эшби, который гласит, что разнообразие управляющей системы должно быть не меньшим, чем разнообразие управляемой системы [882]. Открытая система, чтобы минимизировать вероятность своего разрушения, должна быть достаточно разнообразной, чтобы справляться со всеми изменениями окружающей среды. В этой связи цифровизация экономики, на наш взгляд, меняет традиционные отрасли производства, следовательно, государственное управление в части методов и инструментов должно соответствующим образом меняться и трансформироваться. Как отмечает Ходжсон, динамичная новаторская система требует структурированного сочетания разнообразия и неэластичности, статического равновесия и изменений, централизованного руководства и децентрализованной автономии. Вопрос заключается в том, как и по какому критерию делать структуризацию в данном случае в цифровой экономике [883].

Классические цели государственного регулирования экономики, как правило, имеют амбивалентный характер и сводятся к стабилизации экономической ситуации и повышению эффективности экономической системы. В государственно оформленной рыночной системе для сохранения динамического равновесия необходим стабилизирующий механизм, основанный на ограничении как внешних (со стороны других рыночных и нерыночных систем, выступающих внешней средой по отношению к данной рыночной системе), так и внутренних случайностей [884].

Как отмечает И. П. Воробьева [885], к целям государства следует также отнести обеспечение социальной стабильности, повышение эффективности конкурентной среды, обеспечение внешнеэкономической стабильности. Соответственно к задачам государственного регулирования можно отнести обеспечение экономического роста, поддержку конкурентной среды и развития перспективных отраслей (предприятий), устойчивости курса национальной валюты, занятости и социальной защиты (преодоление «цифрового разрыва»). Цель государства, по мнению И. В. Новиковой [884], – нивелирование воздействия сил (элементов), дестабилизирующих систему, выводящих ее из состояния равновесия, – монополий, социальных конфликтов, экономических (деловых) циклов, внешних эффектов, асиммитричности информации.

Соответственно, среди объектов государственного регулирования экономики выделяют отрасли и сектора экономики, регионы, а также отдельные явления и условия социально-экономической развития страны.

Р. Хелбронер выделил 3 фазы в развитии отношений между государством и экономическими субъектами: 1) государство – покровитель, 2) государство – регулятор, 3) государство – гарант. В условиях глобализации выделяют 4-ю фазу – дерегулирование (не уход из экономики, а смещение фокуса регулирования).

В экономической литературе [885, 886] выделяют административные, правовые, прямые и косвенные формы и методы экономического регулирования[1].

Причинами государственного вмешательства в экономику, как правило, являются: недееспособность рыночных механизмов на микроуровне (фиаско рынка), включая сокращение конкуренции, внешние эффекты, асимметричность информации, потребность общества в соответствующих товарах (так называемых общественных товарах), экологических стандартах, социальной стабильности общества.

Таким образом, можно выделить следующие традиционные направления деятельности государства в сфере экономики [885]:

1) формирование правовых рамок функционирования экономики и обеспечение исполнения законодательных норм и практик;

2) бюджетно-налоговое регулирование;

3) денежно-кредитное регулирование;

4) микроэкономическое регулирование, включая обеспечение равного доступа экономических агентов к информации;

---

[1] Административные методы – выдача лицензий, разрешающих определенную деятельность, установление квот на экспорт и импорт и др. Основой правового регулирования служит гражданское и хозяйственное законодательство, устанавливаемая ими система норм и правил. Важную роль в системе правовых мер регулирования действия рыночного механизма играет антимонопольное законодательство. К прямому экономическому регулированию относится безвозвратное адресное финансирование секторов, областей, территорий и отдельных предприятий, осуществляемому в форме субвенций и субсидий, разного рода дотаций, доплат из специальных бюджетных и внебюджетных фондов различного уровня, а также предоставляемых экономическим субъектам льготных кредитов и налоговых льгот, государственных гарантий. Посредством регулирования денежной массы, определения условий предоставления централизованных кредитов и ставок процента, налоговой, валютной, таможенно-тарифной политики осуществляется косвенное экономическое регулирование [886].

5) антимонопольное регулирование (формирование конкурентной среды, препятствующей развитию монополий в том числе на рынке ИКТ);

6) стимулирование инноваций [887];

7) проведение контрциклической (стабилизационной) политики, включая антиинфляционные мероприятия и борьбу с безработицей;

8) формирование должного уровня и поддержание соответствующей социальной инфраструктуры и социальной защиты населения.

При этом следует отличать государственное управление экономикой и государственное ее регулирование. Так, государственное управление главным образом направлено на находящиеся в государственной собственности экономические объекты либо процессы с целью получения заданных на уровне органов управления результатов, а также перераспределение ресурсов. Государственное регулирование экономики направлено на процессы воспроизводства для достижения определенных национальных социально-экономических задач с использованием, как правило, косвенных экономических методов. Государственная экономическая политика – комплекс мероприятий, проводимых государством в сфере производства, распределения, обмена, потребления, накопления, экспорта и импорта. Соответственно, государственная экономическая политика подразумевает одновременное осуществление органами власти как регулирования экономических процессов, так и управления ими. При этом важно отметить, что в зависимости от экономической ситуации соотношение между регулированием экономики и управлением ею может быть разным: управленческие аспекты могут преобладать при проявлении макроэкономической нестабильности, а в условиях стабилизации экономической ситуации государственное регулирование экономики становится наиболее приемлемым способом воздействия на объекты.

Ввиду многогранности экономики государственная экономическая политика разбивается на отдельные направления, включая инвестиционное, структурное, научно-техническое, бюджетное, экологическое, жилищное, социальную политику и пр. Выделение таких направлений политики позволяет уточнить проблемы, определить способы воздействия на объекты, применить наиболее эффективные инструменты. К объектам государственной экономической политики следует отнести экономический цикл, инвестиции, занятость, денежное обращение, платежный баланс, цены,

условия конкуренции, социальные отношения, образование, здравоохранение и др. [885]. Макроэкономическое регулирование обеспечивается, главным образом, с помощью денежно-кредитного и бюджетно-налогового механизмов.

Формой государственной экономической политики, имеющей долгосрочный характер, является государственная экономическая стратегия. Преобразовательные характеристики государственной экономической политики фактически задают основы концепции направляемой эволюции с соответствующим набором инструментов, объектов воздействия и их последовательности.

Важно отметить также эволюцию развития различных подходов к роли государства в экономике. По словам Вебера, первой выработанной системой государственной хозяйственной политики явился меркантилизм [888], в котором важнейшую роль играли политические институты, осуществлявшие активную поддержку торговли и промышленности посредством обеспечения возвращения кредитов и выполнения соглашений, защиты прав собственности, поддержки создания правовых норм, отвечавших потребностям предприятий, заложения основ развития инфраструктуры (систем образования, транспортных систем), защиты национальной промышленности от иностранных конкурентов, обеспечения стабильности валюты [884]. Независимость торговли и производства от политических институтов наблюдается только на последнем кратковременном этапе становления западноевропейского капитализма конца Х1Х века.

В ХХ веке произошел поворот рыночных государственно оформленных систем, находившихся на стадии зрелости, к формированию мировой рыночной системы, что сопровождалось возникновением и развитием системы государственного регулирования. Основоположник новой теории Дж. М. Кейнс предложил два базовых подхода к регулированию (подход «утечек и инъекций»): государство должно вмешиваться в воспроизводственный цикл с помощью косвенных методов регулирования (кредитно-денежного и бюджетно-налогового механизмов) и воздействовать на платежеспособный спрос посредством дополнительной эмиссии, которая в условиях неполной занятости ведет к росту предложения товаров и услуг, а не только цен. В условиях закрытой экономики это стимулирует инвестиции, а не инфляцию.

С 50-х годов XX века в результате втягивания мирового хозяйства в рынок и тесного переплетения национальных экономик, создания единой рыночной экономики и ее инфраструктуры, модификации национального суверенитета государств происходит глобализация, конечная цель которой – формирование мирового хозяйства, работающего как единый организм и его новой структуры. В ряде государств внедряются индикативное планирование и программирование, направленные на преодоление проблем отсталой структуры экономики и низкой конкурентоспособности, получившие на уровне концепции название «государственного дирижизма» [885].

С 80-х годов XX века происходит изменение парадигмы государственного регулирования в направлении захвата и удержания лидирующих позиций на мировых рынках, усиливается необходимость межгосударственного регулирования, создания межправительственных органов, координирующих условия воспроизводства в региональных рыночных системах, единой мировой рыночной системе[2] [884]. В рамках государственно оформленных рыночных систем роль государства направлена на формирование и поддержку глобальных игроков (ТНК, МНК), которые могут стать драйверами развития национальной экономики. В контексте данных задач модифицируется государственное регулирование, которое приобретает неоконсервативный характер: происходит поступательный переход от бюджетного регулирования к денежно-кредитному. Внешнеторговое регулирование ограничено механизмами ВТО. Происходит переход от государственного регулирования к государственно-частному партнерству. В целом следует отметить, что проводимые с 1980-х годов институциональные и нормативные реформы были направлены на ускорение внедрения цифровых технологий [889].

Кроме того, в современной экономике отмечается тенденция замещения регуляторных функций государства саморегулированием негосударственных институтов либо сорегулированием одновременно государственных и негосударственных организаций [890]. Модифицируются и усложняются формы и методы государственного регулирования, среди которых выделяются программное управление,

[2] Примером можно считать принятие в 2021 году на саммите G20 решения о введении минимального 15%-го налога на прибыль ТНК с доходом от 750 млн евро в год (в том числе ИКТ компаний) (Туда же и Даблин. – Режим доступа: https://www.kommersant.ru/doc/5028324. – Дата доступа: 11.10.2021).

социально-экономическое изучение, стратегическое прогнозирование и планирование, направленные на решение долгосрочных задач [886]. Государство формирует гибкую институциональную среду для поступательного и устойчивого развития экономической системы.

Таким образом, роль государства в рыночной системе хозяйства поступательно меняется: происходит отход от прямого влияния на участников экономической деятельности в пользу изменения условий функционирования предприятий и рынков, или, другими словами, от концепций реформы регулирования или дерегулирования к управлению регулированием, а в последнее время и к регулированию управления [887]. В развитие данной тенденции ОЭСР в 2011 году предложила модель регуляторной политики, направленной на обеспечение качества регулирующей структуры, а не реагирование на сбои в регулировании [891]. И. В. Новикова выделяет следующую эволюцию рыночных систем [884]: рынок (стадия возникновения), рыночная экономика (стадия становления), экономика рыночного типа (стадия зрелости), рыночно-индустриальная (стадия регрессивных преобразований) и индустриальная экономика (стадия исчезновения).

Важную роль в системе государственного регулирования экономики играет стимулирование прогрессивных структурных сдвигов, развития высоких наукоемких технологий. Выделяют инновационный тип развития экономики страны, предполагающий постоянную разработку, освоение и использование научно-технических нововведений и технологий для повышения конкурентоспособности [885]. Основными принципами регулирования государственной инновационной политики должны являться: определение государственных приоритетов инновационного развития и формирование соответствующей нормативно-правовой базы.

В рамках структурной политики государство осуществляет поддержку высокотехнологических отраслей, стимулирует сворачивание «грязных» и устаревших производств и отраслей, формирует эффективную конкурентную среду, благоприятную для развития инноваций. Совокупность стратегических и тактических целей, задач и направлений по развитию научно-технического потенциала, эффективному его использованию в интересах социально-экономического совершенствования общества составляет государственную научно-техническую политику.

Следует отметить, что цифровизация является объективным процессом, который характеризует развитие современной экономики. Вместе с тем данный процесс может происходить независимо от национальных приоритетов государства, под диктатом глобальных ИКТ-компаний, либо станет объектом государственного регулирования.

В контексте цифровизации важнейшими элементами развивающей роли государственного регулирования является создание инфраструктуры (физической и нефизической), формирующей новые возможности роста экономики, а также развитие НИОКР. Успешная образовательная политика является предпосылкой будущей занятости населения, оказывает глубокое влияние как на формирование корпуса квалифицированной рабочей силы, так и на способность населения усваивать новые знания и приобретать новые навыки [45, 892, 893]. Государство создает экономические и политические условия, которые позволяют компаниям и частным лицам брать на себя риски, связанные с развитием продуктов и услуг, и в то же время разумно ожидать финансовой отдачи от принятия рисков.

Реализация различных мониторинговых функций осуществляется посредством государственных органов власти, соответствующих регуляторов. Распределительная роль государства включает такие подходы, как «формирующие предложение» (подход «технологического толчка» – проведение собственных исследований и разработок, стимулирующих распространение технологий) и «формирующие спрос» (государство формирует спрос через закупку определенных технологических решений и инноваций) [221, 894].

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

1) разработка и установление норм и стандартов управления и планирования исследовательским процессом;

2) разработка и установление правил, регулирующих создание цифровых инноваций и функционирование инновационной экосистемы;

3) финансирование исследований и цифровых инноваций;

4) разработка и внедрение процедур оценки экономического потенциала внедрения технологий и ее результативности на всех уровнях и этапах;

5) предоставление сертификатов качества;

6) способствование взаимодействию между государственным и частным секторами на всех уровнях;

7) поддержка образования и обучения.

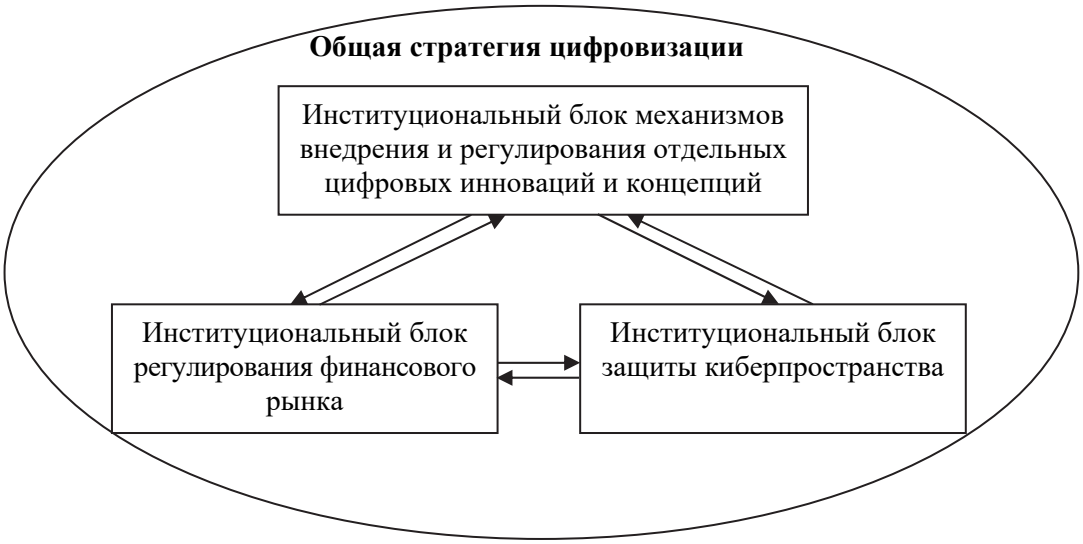
С целью реализации структурных сдвигов, развития и внедрения наукоемких технологий с учетом технологического уровня государств, текущей структуры экономики, уровня государственного регулирования и финансовых возможностей используют такие методы долгосрочного регулирования, как прогнозирование, планирование и программирование.

Бауэр [167] выделил ряд важных ограничений использования государственного регулирования в отношении цифровой экономики, отметив, что актуальные теория и практика регулирования не соответствуют новой реальности рынков ИКТ ввиду недостаточного учета возрастающей взаимосвязанности и взаимозависимости современных средств коммуникации. В данном контексте предлагается использовать три базовые концепции государственного регулирования цифровой экономики: экономику регулирования, экономику платформ и экономику экосистем.

Большая часть экономики регулирования основывается на анализе статического равновесия, часто ориентированном на узкоопределенные рынки. Экономика платформы побуждает аналитиков учитывать соответствующие взаимозависимости между игроками, связанными с платформой. Экосистемный подход учитывает более широкие взаимозависимости, которые влияют на характер и интенсивность конкуренции. Он предполагает, что в динамичной, взаимозависимой системе регулирование не полностью контролирует результаты и часто имеют место непреднамеренные, положительные или отрицательные последствия. Кроме того, экосистемный подход обостряет представление о множестве механизмов, которые существуют для управления такими динамическими системами. Оба последних подхода используют адаптивное управление, в котором непрерывный мониторинг результатов применяется для тонкой настройки политики.

Анализ подходов к трактовке понятия «экосистема» в отношении цифровой экономики позволяет рассматривать ее не только как совокупность правил и норм, регулирующих взаимодействие населения, хозяйствующих субъектов, органов государственного регулирования в отношении становления и развития цифровой экономики, но и как определенную алгоритмизацию, последовательность

принимаемых норм и правил, которые позволяют наращивать темп и трансформационные формы развития. Элементами программ и стратегий цифровизации, как правило, выступают институциональные блоки: механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; регулирования финансового рынка; защиты киберпространства (рисунок).



Элементы институциональной экосистемы цифровой экономики (разработано автором)

Государственное регулирование всегда носит институциональный характер. Необходимость трансформации инструментов государственного регулирования обоснована «законом необходимого разнообразия» Эшби, который говорит, что разнообразие управляющей системы должно быть не меньшим, чем разнообразие управляемой системы [882]. Открытая система, чтобы минимизировать вероятность своего разрушения, должна быть достаточно разнообразной, чтобы справляться со всеми изменениями окружающей среды. В этой связи цифровизация экономики, как представляется, меняет традиционные отрасли производства, следовательно, государственное управление в части методов и инструментов должно соответствующим образом меняться и трансформироваться. Как отмечает Ходжсон, динамичная новаторская система требует структурированного сочетания разнообразия и неэластичности, статического равновесия и изменений, централизованного руководства и децентрализованной автономии. Вопрос заключается в том, как и по какому критерию делать структуризацию в данном случае в цифровой экономике.

Источником многих важных технологических нововведений являются институты, в значительной степени пользующиеся финансовой поддержкой государства (например, университеты в развитых странах). В целом, по мнению институционалистов, необходимо как минимум наличие таких централизованных институтов, как та или иная форма индикативного планирования в сочетании с интервенционистской промышленной политикой, направленной на координацию экономической деятельности и установление приоритетов [883].

Витт [168] разработал принципы для регулирующих действий на основе структуры, названной emergence economics (формируемой экономикой), которая опирается на отдельные положения экономики инноваций, теории сложных адаптивных систем и экономики экосистем. По его мнению, адаптивная государственная политика цифровизации должна быть стимулирующей, а не «диктующей», поддерживать инновации, способствовать институциональному и инфраструктурному развитию, создавать стимулы и доверие, а также обеспечивать прозрачность и измеряемость.

Отражением функции цифрового взаимодействия государства и граждан (субъектов) хозяйствования является концепция E-Government. Данный подход знаменует переход от «аналоговых» механизмов государственного регулирования к цифровым. Среди причин цифровизации правительства выделяют: сокращение расходов, содействие экономическому развитию, повышение прозрачности и подотчетности, улучшение предоставления услуг, улучшение государственного управления, содействие электронному обществу [260, 719].

Современный проактивный подход в концепции государственного регулирования [121] предполагает не столько реакцию государства на цифровую трансформацию, сколько ее активное формирование. Во-первых, государства имеют возможность использовать цифровые инновации для более быстрого реагирования на технологические изменения, усиления своего мандата (например, использование систем AI для выявления мошенничества). Во-вторых государства имеют возможность влиять на установление стандартов цифровых технологий, которые вводят определенные регламенты для участников отраслей и экосистем.

Цифровые технологические [60] стандарты обеспечивают фундаментальные платформы, на основе которых конкурирующие

предприятия создают свои продукты и услуги. Понимание стандартов и их разработка важны для развития цифровых платформ и экосистем. Стандарты появляются как в результате рыночной конкуренции и принимаются де-факто, так и разрабатываются под эгидой, как правило, специализированных органов стандартизации (ETSI и IEEE). С точки зрения государственного регулирования важно различать установление стандартов и их разработку: модель «установление стандартов» направлена в первую очередь на обеспечение совместимости и не предполагает создания новых технологий; модель «разработка стандартов» связана с развитием технологий, а также имеет значение для формирования дополнительной стоимости «первооткрывателя технологии».

Заключение

Таким образом, государственное регулирование в результате объективной эволюции претерпело ряд трансформаций и изменений касательно методов, направлений, инструментария проведения регуляторной политики. В условиях цифровизации отмечается поступательный переход от бюджетного регулирования к денежно-кредитному, от государственного регулирования к государственно-частному партнерству, модифицируются и усложняются формы и методы государственного регулирования: происходит отход от концепций реформы регулирования или дерегулирования к управлению регулированием.

Успешная цифровизация тесно связана с инновационным развитием экономики страны, включающим формулирование и реализацию национальных приоритетов, формирование соответствующей нормативно-правовой базы. В этой связи выделяем экосистемный подход, который в наибольшей степени учитывает взаимозависимости, влияющие на характер и интенсивность развития конкуренции в сфере ИКТ.

Предложена авторская модель институциональной экосистемы цифровой экономики, включающая институциональные блоки: механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; регулирования финансового рынка; защиты киберпространства.

Обоснована необходимость стимулирования государством разработки и внедрения стандартов цифровых технологий, которые вводят определенные регламенты для участников инновационных отраслей и экосистем.

3.2. Страновые особенности и подходы к формированию и регулированию цифровой экономики

Государственное регулирование является необходимой формой воздействия на экономический механизм страны, направленной на стимулирование разработки и внедрения цифровых инноваций, структурных измений. Вместе с тем реализация структурных сдвигов, развитие и внедрение наукоемких технологий осуществляются на национальном уровне с учетом технологического уровня отдельных государств, текущей структуры их экономики, уровня государственного регулирования и финансовых возможностей.

В экономической литературе выделяют три отличительные формы управления национальными цифровыми экосистемами и институциональными структурами [90].

1. Система, непосредственно управляемая государством, для которой характерны централизация управления и государственное финансирование. Государственно-частное партнерство также является одной из форм финансирования крупных проектов, что позволяет разделить риски, связанные с разработкой и внедрением цифровых инноваций [73][3]. С целью усиления «массового предпринимательства» и создания динамичной инновационной экосистемы

[3] Типичным примером государственной системы является система Китайской Народной Республики (КНР). Центральное правительство устанавливает правила, цели, средства и процедуры, а также осуществляет финансирование большинства видов экономической деятельности, включая инновации. Уникальной особенностью системы КНР является параллельное существование сильного и динамично развивающего частного сектора, который функционирует в рыночных условиях, под контролем и целеуказанием со стороны правительства. Китай использует государственные средства для создания механизма поддержки стартовой экосистемы, «мультиплицируя» эффект через мобилизацию частных инвестиций и стимулирование коммерциализации приоритетных цифровых технологий. Финансирование осуществляется за счет средств Руководящего фонда технологических инноваций (децентрализованная система управления фондами funds-of-funds (FOF). В целом, прямое государственное финансирование составляет всего 20% от общих расходов на исследования и разработки [73]. В сфере искусственного интеллекта Министерство науки и технологий КНР назначило компании Baidu, Alibaba, Tencent и iFlyTek для руководства четырьмя национальными платформами открытых инноваций в области искусственного интеллекта в области автономного вождения, интеллектуальных городов, медицинской диагностики и обработки голоса. Министерство промышленности и информационных технологий КНР совместно с Китайской академией исследований в области телекоммуникаций (CATR) в 2016 году создали Индустриальный интернет-альянс с целью ускорения развития промышленного интернета в Китае [206].

государство инвестирует в стартапы и МСП в соответствии с приоритетами политики, посредством сделок с акциями, венчурного капитала и компенсации рисков. Государство сотрудничает с существующими частными фондами, позволяя инвестировать государственные средства в соответствии с рыночными механизмами. Как соинвестор, государство участвует с частью капитала (около одной трети) в инвестиционном проекте, принимает непропорциональную долю риска, обеспечивает политическую поддержку и, в некоторых случаях, гарантирует минимальный доход для партнера частного инвестора [895].

2. Рыночная система, предполагающая наличие развитого рынка и инновационных экосистем, участники которых осуществляют взаимодействие в условиях развитых и стабильно функционирующих финансовых сетей и систем. Государственное вмешательство ограничивается установлением правил в отношении инвестиций, интеллектуальной собственности, разработки и обеспечения соблюдения правил, регулирующих продажу и эксплуатацию инноваций, а также деятельности по сертификации и оценке технологий. Максимальное государственное вмешательство и финансирование характерно для исследований и цифровых инноваций, имеющих последствия для национальной безопасности.

3. Смешанная, или гибридная, система, сочетающая в себе структуры и режимы, которые допускают как рыночные, так и централизованные формы деятельности в области цифровизации. Она предполагает активное участие как государственного, так и частного секторов. Национальные органы власти финансируют проекты и исследовательские программы в области цифровых инноваций.

Всемирный экономический форум (WEF) в отношении государственного регулирования, в том числе цифровых инноваций, предлагает подход, называемый «гибким регулированием» (Agile Regulation), суть которого заключается в фокусировании на конечном результате, стимулировании самоорганизации вместо навязывания правил [896][4].

[4] Так, Министерство земли, инфраструктуры, транспорта и туризма Японии (MLIT) внедряет данный подход к регулированию, охватывающий: использование системы исключений, позволяющих проводить испытания автономных транспортных средств, которые не соответствуют обычным нормативным требованиям; совместную разработку добровольных технических требований в промышленности (для испытаний автономных транспортных средств); адаптацию технических требований на основе данных испытаний с упором на международную гармонизацию (в рамках Всемирного форума ЕЭК ООН по гармонизации правил в области транспортных средств – WP29).

В международной практике используется также подход, основанный на концепции «упреждающего регулирования», который предполагает выявление изменений в окружающей экосреде за определенный период и рассмотрение последствий этих изменений в рамках текущих и будущих стратегий регулирования. Анализ показывает распространение данного подхода посредством создания специализированных подразделений, консультирующих регулирующие органы по вопросам воздействия технологических инноваций и связанной с этим необходимости реформ. Примером служит Внешний консультативный комитет Канады по регуляторной конкурентоспособности, Шведский комитет по технологическим инновациям и этике и Совет по горизонтам регулирования Соединенного Королевства. Так, Правительство Швеции в 2018 году учредило Комитет по технологическим инновациям и этике с миссией помочь правительству ускорить разработку политики, связанной с цифровыми технологиями. Задача комитета – выявить любые противоречивые цели, нормативные проблемы и препятствия на пути ответственного использования новых технологий и предложить способы их решения. Комитет опубликовал информационные бюллетени по новым технологиям, таким как искусственный интеллект, машинное обучение, 5G, синтетическая биология и Блокчейн, ряд отчетов, в том числе о нормативных барьерах, предложениях по проведению экспериментов и моделям для продвижения ответственных инноваций.

В 2020 году Министерство технологических инноваций и цифровизации Италии представило правовое положение «Право на инновации» (Diritto a Innovare), которое позволяет отступать от правил, препятствующих появлению новых идей, продуктов или бизнес-моделей, с целью развития, распространеня и использования новых технологий и высокотехнологичных инициатив. Новаторы, в том числе компании, стартапы, университеты и исследовательские организации, которые выявляют нормативное препятствие, могут запросить у правительства разрешение на проведение экспериментов путем временного отступления от законодательных норм. Министерство оценивает факторы, включая осуществимость предложения, уровень технологических инноваций и их потенциальное экономическое, социальное и экологическое воздействие, совместно с другими соответствующими органами. Аналогичный подход к экспериментированию был введен в Японии. В Республике Корея

при разработке концепции и технологий Smart City предложены национальные пилотные проекты в г. Седжонге и Пусане. В рамках этой инициативы в 2019 году правительство ввело нормативные механизмы «регуляторной песочницы» (кластера, на который не распространяются отдельные действующие законодательные, организационные, административные, технические нормы и ограничения), которые позволяют вносить изменения в определенные области регулирования в рамках данных проектов. Регулирующие льготы подлежат рассмотрению комитетом, местными органами управления и могут предоставляться на срок до шести лет. После местных испытаний принимаются решения о том, как адаптировать регулирование в других регионах или в целом по стране. В 2020 году закон о «регуляторных песочницах» подписан в России. В его рамках регионам разрешено вводить льготы для инновационных компаний, временно отменять законодательные требования и запреты в цифровой сфере, в том числе федеральные [897]. Особые правовые режимы применяют в США, Австралии, Сингапуре, ОАЭ, Великобритании.

Важным принципом, который отмечается в экономической литературе, является использование технологически нейтрального подхода к регулированию цифровых технологий. Растущее число стран, в том числе Дания, Япония и Соединенное Королевство, открыто поощряют принятие данного подхода[5]. На его основе Управление по развитию информационных технологий Сингапура разработало модель управления искусственным интеллектом, которая не зависит от секторов, технологий и алгоритмов и переводит этические принципы в реализуемые методы внедрения AI. В России анонсирована цифровая трансформация страны в ближайшие 10 лет. Подготовлены проекты законов об экспериментальных правовых режимах в сфере искусственного интеллекта, о доступе разработчиков AI к Big Data агрегированным государствам[6] [899].

---

[5] Свобода отдельных лиц и организаций выбирать наиболее подходящую технологию для их нужд и требований для разработки, приобретения, применения или коммерциализации, вне зависимости от знаний, используемых в качестве информации или данных [898].

[6] В России вложения в федеральные проекты по цифровизации увеличились в 2020 году на 60%, до 149 млрд российских руб. Аналитики полагают, что эти инвестиции сохранятся на уровне 195–230 млрд российких руб. в год. Пойдут в основном на государственные системы, информационную безопасность и создание общей инфраструктуры (Доденьжения народного хозяйства. – Режим доступа: https://www.kommersant.ru/doc/4838194?tg. – Дата доступа:02.06.2021).

Экстраполяция основных составляющих стратегий и институциональных блоков формирования современной экосистемы цифровой экономики на примере США, КНР и Российской Федерации позволяет сформировать различные институциональные матрицы национальных экосистем цифровой экономики (табл. 3.1, 3.2, 3.3).

Таблица 3.1

Институциональная матрица экосистемы цифровой экономики на уровне программ США (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый + первый уровни (2000–2014 годы)	СЦ	—	—	—
	ИБЦИ	Стэнфордский индустриальный парк (Силиконовая долина), 1951	МОВ	Производство высокотехнолгической продукции (полупроводниковой на начальном этапе)
		Закон «Об энергетической независимости и безопасности», 2007	Ко	Политика страны по модернизации электросетевой инфраструктуры. Развертывание и интеграция распределенных ресурсов и генерации, внедрение «умных» технологий (в режиме реального времени, автоматизации, интерактивных технологий, которые позволяют оптимизировать физическую работу приборов и бытовой техники) для учета измерений, коммуникаций
	ИБФР	Закон «О финансовой модернизации» (Закон Грэмма – Лича – Блайли) Gramm–Leach–Bliley Act, 1999	Ко, FTC	Требование от финансовых учреждений – компаний, предлагающих потребителям финансовые продукты или услуги, разъяснения клиентам своих методов обмена информацией и обеспечения защиты конфиденциальных данных

Продолжение табл. 3.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый + первый уровни (2000–2014 годы)	ИБФР	Закон «Быстрый старт для вашего бизнеса» (JOBS Act), 2013	Пр, Ко	Использование механизмов Crowdfunding для выпуска ценных бумаг
		Закон «О реформировании Уолл-стрит и защите потребителей» (Додда – Франка), Dodd – Frank Wall Street Reform and Consumer Protection Act, 2010	Пр, Ко, SEC	Снижение рисков финансовой системы, защита потребителей финансовых услуг, регулирование системообразующих финансовых институтов
		Совет по надзору за финансовой стабильностью (FSOC), 2010	Пр, Ко	Регулирование деятельности всех системообразующих холдинговых компаний и небанковских финансовых организаций
	ИБЗК	Федеральный закон «О компьютерном мошенничестве и злоупотреблении» (CFAA), 1986	Пр, Ко	Киберпреступления, включая взлом, вымогательство (программы-вымогатели)
		Закон «О защите электронных коммуникаций» (ECPA), 1986	Пр, Ко	Защита сообщений при хранении и передаче
		Закон «О переносимости и подотчетности медицинского страхования» (HIPAA), 1996	Пр, Ко	Требования кибербезопасности, применимые к защищенной медицинской информации
		Закон «О защите конфиденциальности детей в Интернете» (COPPA), 1998	Пр, Ко	Защита конфиденциальности и безопасности детей в Интернете
		Закон «О медицинских информационных технологиях для экономического и клинического здоровья» (HITECH), 2009	Пр, Ко	Продвижение и расширение внедрения информационных технологий в здравоохранение
		Директива президента «О политике безопасности и устойчивости критически важной инфраструктуры» (Presidential Policy Directive/ PPD-21), 2013	Пр	Устанавливение национальной политики безопасности и устойчивости критически важной инфраструктуры

Продолжение табл. 3.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	СЦ	—	—	—
	ИБЦИ	Руководство по архитектуре «Киберфизической системы CPS», 2016	NIST	Техническая информация, определение и классификация по категориям, связанным с IoT: эталонная архитектура; кибербезопасность и конфиденциальность; тайминг и синхронизация; совместимость данных; варианты использования
		Федеральная политика в области автоматизированных транспортных средств, 2016	NHTSA	Руководства по сбору и обмену Big Data с подключенных датчиков в автономных транспортных средствах
	ИБФР	Требования к кибербезопасности финансовых услуг (NYDFS) шт. Нью-Йорк, 2017	ДФУ	Регламетация деятельности сервисов денежных переводов, проблематики кибербезопасности
		Закон «О “нормативной песочнице” в сфере финансовых технологий шт. Аризона» (HB 2434), 2018	МОВ	Отдельное гибкое регулирование для сектора FinTech
		Закон «О “песочнице” финансовых технологий шт. Вайоминг» (HB 57), 2019	МОВ	Отдельное гибкое нормативное регулирование для тестирования инновационных финансовых продуктов и услуг, в том числе Блокчейн
		Совет по регулированию финансовых услуг и инноваций Вашингтона, округ Колумбия, 2019	МОВ	Подготовка регулятивных послаблений нормативной среды для FinTech
	ИБЗК	Закон «О защите конфиденциальности потребителей», 2015	Пр, Ко	Принципы сбора, использования и обработки личной информации операторов сетей, открытости, информированного согласия

Продолжение табл. 3.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	ИБЗК	Национальный план защиты инфраструктуры (NIPP). 2016 (затем в 2017, 2018)	CISA, NIHS	Содействие в разработке технологий, инструментов, процессов и методов, направленных на долгосрочную безопасность и отказоустойчивость критически важной инфраструктуры
		Агентство по кибербезопасности и безопасности инфраструктуры (CISA), 2018	Пр, DHS	Управление снижением рисков для национальной кибернетической и физической инфраструктуры
		Национальный центр управления рисками США (NRMC), 2018	DHS, CISA	Создание безопасной и отказоустойчивой критически важной инфраструктуры в 16 важнейших секторах (включая связь, энергетику, транспорт и водоснабжение). Взаимодействие с частным сектором, государственными учреждениями, использование динамического межотраслевого процесса управления рисками для выявления, анализа, определения приоритетов и управления наиболее значительными рисками – кибернетическими и физическими
		Концепция улучшения кибербезопасности критически важной инфраструктуры, 2018	NIST	Национальный стандарт «разумной кибербезопасности»
		Разъясняющий Закон «О законном использовании данных за рубежом» (The CLOUD Act), 2018	Ко	Предоставление права правоохранительным органам получать доступ к определенной информации, хранящейся у поставщика услуг (даже если эти данные находятся в другой стране)

Продолжение табл. 3.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
	ИБЗК	Положение о брокере данных шт. Вермонт, 2019	МОВ	Регулирование деятельности любого коммерческого субъекта, который собирает и обрабатывает информацию о потребителях с целью продажи или лицензирования данных
Третий уровень (2020 – н. в.)	СЦ	Закон «О цифровизации» (DIGIT Act), 2020	С_ТЕС	Национальная государственно-частная стратегия развития IoT
	ИБЦИ	Закон «О Национальной инициативе в области AI» (NAIIA), 2020	Пр, Ко, ФА	Обеспечение лидерства США в области AI, исследований и разработок; интеграции систем AI во все секторы экономики и общества
		Национальное управление инициативы в области AI (NAIIO), 2020	OSTP	Обмен технической и программной информацией о деятельности, связанной с AI, между ФА, промышленностью, академическими кругами, некоммерческими организациями, профессиональными сообществами и пр.
	ИБФР	Проект Закона «О регулировании стейблкоинов», в стадии согласования	Пр, FDIC, OCC	Регулирование рынка стейблкоинов
	ИБЗК	Закон «О повышении кибербезопасности IoT» (IoT Cyber-security Improvement Act), 2020	Пр, Ко, NIST	Предписание поставщикам IoT, обслуживающим федеральное правительство, обеспечивать долгосрочную поддержку безопасности для устройств IoT
		Консультативный совет по критическому инфраструктурному партнерству, 2020	DHS, CISA	Взаимодействие представителей государства с владельцами и операторами критической инфраструктуры в каждом секторе

Окончание табл. 3.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н. в.)	ИБЗК	Закон шт. Калифорния «О конфиденциальности потребителей» (CCPA), 2020	МОВ	Классифицирует типы персональной информации, агрегируемой компаниями, предотвращает возможность продажи своих персональных данных третьей стороне
		Закон шт. Нью-Йорк «О предотвращении взломов и улучшении безопасности электронных данных» (SHIELD Act), 2020	МОВ	Требует реализации программ кибербезопасности и защиты информации
		Проект «Рекомендации для производителей устройств IoT: основные направления деятельности и базовый уровень возможностей кибербезопасности основных устройств», 2020	NIST	Развитие надежных и защищенных IoT систем во всех секторах экономики

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства; Пр – Президент США; Ко – Конгресс США; FTC – Федеральная торговая комиссия США; NHTSA – Национальное управление безопасности дорожного движения США; CISA – Агентство по кибербезопасности и безопасности инфраструктуры; NIHS – Национальный институт безопасности городов; DHS – Министерство национальной безопасности США; OCC – Управление валютного контролера США; SEC – Комиссия по ценным бумагам и биржам США; FDIC – Федеральная корпорация страхования депозитов США; NIST – Национальный институт стандартов и технологий; C_TEC – Центр по взаимодействию с технологиями Торговой палаты США; OSTP – Управление научно-технической политики Белого дома; ФА – федеральные агентства; МОВ – местные органы власти; ДФУ – Департамент финансовых услуг штата.

Анализ табл. 3.1 показывает, что сложившаяся экосистема регулирования цифровой экономики США направлена, главным

образом, на обеспечение доступности инноваций, создание условий для получения новых технологий производителями промышленной продукции (на основе развития технопарков), налаживание взаимодействия на уровне государственно-частного партнерства. В стране практически отсутствуют государственные стратегии цифровизации, за исключением принятого в 2020 году Закона «О цифровизации», направленного, в первую очередь, на развитие технологий IoT.

Институциональный блок регулирования финансового рынка дефрагментирован на регуляторные практики федерального уровня и уровня штатов, распространяются подходы «регуляторных песочниц» в отношении FinTech, защиты персональной и конфиденциальной информации. Вместе с тем поступательно осуществляется развитие, систематизация и разработка стандартов в институциональном блоке механизмов внедрения и регулирования отдельных цифровых инноваций и концепций, включая AI, IoT, автоматизированные транспортные средства, Smart Grid и пр. Наибольшее внимание в институциональной экосистеме цифровой экономики США акцентировано блоку защиты киберпространства: кибербезопасности и безопасности критической инфраструктуры. Таким образом, в США управление национальной цифровой экосистемой и институциональными структурами носит ярко выраженную рыночную форму, согласно которой государство, главным образом, обеспечивает соблюдение правил функционирования рынков (рассматривает возможность ужесточения антимонопольного регулирования в отношении цифровых платформ [900]), регулирует реализацию и эксплуатацию цифровых технологий, осуществляет деятельность по сертификации и стандартизации, а также обеспечивает стабильность функционирования критической инфраструктуры и кибербезопасность.

В КНР (табл. 3.2) государственное регулирование носит всеобъемлющий характер и связано не только с критической инфраструктурой и кибербезопасностью, стандартизацией и сертификацией.

Посредством реализации крупных инфраструктурных технологических проектов КНР задает магистральные направления развития экономики и общества, повсеместной интеграции цифровых инноваций.

Таблица 3.2

Институциональная матрица экосистемы цифровой экономики на уровне программ КНР (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (1998–2010 гг.)	СЦ	Программа «Факел», 1998	ЦО КПК, МНТ	Создание баз освоения высоких технологий; подготовка кадров для высокотехнологичного сектора производства; создание инкубаторов, технопарков, центров трансфера технологий; создание сети посреднических услуг; привлечение финансов; формирование государственной инновационной политики, включая предоставление налоговых льгот
		Государственная стратегия по развитию информатизации, с 2006 по 2020 год	ЦО КПК, МНТ	Создание организационных структур для регулирования деятельности в сфере IT, определение основных направлений развития Интернета. Шестнадцать национальных мегапроектов (на сумму около 75 млрд долларов), включая сектор «нового поколения телекоммуникационного оборудования», цель которых – обеспечение полной ИКТ независимости страны
	ИБЦИ	—	—	—
	ИБФР	Правила осуществления административных мер для платежных услуг, предоставляемых нефинансовыми организациями, 2010	РВС	Регламентация предоставления услуг онлайн-платежей небанковскими компаниями

Продолжение табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (1998–2010 гг.)	ИБЗК	Центр оценки безопасности информационных технологий Китая (CNITSEC), 1997	ЦО КПК	Мониторинг состояния кибербезопасности государственных учреждений
		Постановление по защите Интернет-пространства, 2000	ЦО КПК, ВСНП	Введение классификации вероятных информационных и киберугроз, разработка мер по обеспечению безопасности в этой сфере
		Постановление государственной информатизированной руководящей группы по работе в области укрепления информационной безопасности, 2003	ЦО КПК	Защита важной и стратегической инфраструктуры, проведение мониторинга интернет-пространства, привлечение квалифицированных специалистов в области информационной безопасности и защиты технического оборудования
		Запуск проекта национального файервола «Золотой щит», 2003	БОИНСБ, ЦО КПК	Проект представлет собой интегрированную, многоуровневую систему, включающую технические, административные, а также службы национальной безопасности, – технологический барьер, предназначенный для предотвращения несанкционированного или нежелательной коммуникации между компьютерными сетями или узлами Сети (хостами)
		Создание специального полицейского ведомства для контроля за Интернетом, 2006	ЦО КПК	Отслеживание содержания сайтов, онлайн-форумов и социальных сетей

Продолжение табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2011–2014 годы)	СЦ	—	—	—
	ИБЦИ	—	—	—
	ИБФР	Требование в отношении коммерческих банков и торговых компаний закрыть счета в Биткойнах, 2014	РВС	Ограничение рынка криптовалют
		Закон «О ценных бумагах», 2014	РВС	Регулирование сферы краудфандинга
		Проект запуска «цифрового юаня», 2014	РВС	Изучение возможности замещения фиатной национальной валюты цифровым аналогом
	ИБЗК	Положения о кибербезопасности были внесены в национальное уголовное законодательство, 2011	ЦО КПК	Регулирование сферы кибербезопасности
		Постановление о продвижении информатизации и развитии действующей защиты информационной безопасности, 2012	ЦО КПК	Контроль над Интернет-приложениями, виртуальными сделками в торгово-экономической сфере, информационно-вещательными услугами; утверждение лиц, отвечающих за мероприятия по обеспечению безопасности в регионах
		Положения о кибербезопасности были внесены в Закон «О защите прав и интересов потребителей», 2013	ЦО КПК	Защита цифровых прав
		Администрация киберпространства Китая (CAC), 2014	ЦО КПК	Мониторинг и регулирование национального киберпространства

Продолжение табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	СЦ	Программа «Сделано в Китае 2025», 2015	ЦО КПК	Модернизация китайской промышленности в рамках концепции I4.0
	ИБЦИ	—	—	—
	ИБФР	План развития финансовой интеграции на 2016–2020 годы	PBC, CBSC, CSSC, CISC, SAIC	Национальная стратегия развития цифровой финансовой доступности. Содействие финансовой интеграции с помощью инновационных финансовых продуктов и услуг, стандартизация различных форм финансирования в Интернете, содействие устойчивому развитию FinTech и усиление государственного контроля
		Совершенствование нормативного регулирования в части FinTech, включая правила администрирования регистрации данных посредников по одноранговому кредитованию; временные меры по управлению деятельностью посредников по предоставлении информации в Интернете; руководство для депозитарного бизнеса одноранговых кредитных фондов; руководство по раскрытию информации по онлайн фондах однорангового кредитования, 2016–2017 годы	CBSC, PBC	Нормативная база для FinTech компаний, занятых в сфере онлайн-кредитования

Продолжение табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	ИБФР	Дополнительные ограничения циркуляции криптовалют на рынке КНР, 2017	РВС	Запретительные меры в криптовалютной сфере на использование: механизма первичного предложения монет (ICO); криптовалюты как объекта биржевой торговли (с конвертацией юаней в криптовалюты или наоборот); услуги финансовых учреждений и небанковских платежных учреждений по обслуживанию ICO и криптовалют
	ИБЗК	Антитеррористический закон КНР, 2015	ЦО КПК	Дешифровка интернет-трафика, использование административных мер по изъятию у иностранных компаний и предприятий информации при подозрении на ее применение для террористических нужд
		Китайский центр сертификации информационной безопасности (ISCCC), 2015	ЦО КПК	Сертификация базовой кибербезопасности для продуктов, лицензированного персонала, систем управления и услуг информационной безопасности
		Национальная стратегия безопасности в киберпространстве, 2016	САС, БОИНСБ	Защита суверенитета и нацбезопасности страны в киберпространстве, защита основной информационной инфраструктуры, борьба с проявлениями кибертерроризма и преступлениями в Интернете

Продолжение табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	ИБЗК	Закон о кибербезопасности, 2016	ЦО КПК	Мониторинг деятельности в китайском сегменте Интернета; требование о хранении публикуемого контента на территории Китая не менее 6 месяцев; введение понятия «критически важная инфраструктура» и запрет передовать данные о ней за границу; запрет компаниям, предоставляющим услуги онлайн, собирать и продавать персональные данные пользователей
		Национальный центр кибербезопасности (NCC), 2016	CAC	Обучение в сфере кибербезопасности
		Официальное формирование кибервойск в составке армии КНР, 2016	ЦО КПК	Ведение военных действий в Интернет-пространстве
		Индустриальный парк кибербезопасности, 2017	МПИ, ПП	Разработка и производство эффективных продуктов в области сетевой безопасности
		Стратегия международного сотрудничества в киберпространстве, 2017	МИД КНР	Регламентация участия Китая в международном обмене и сотрудничестве в области международной информационной безопасности
		Положение о защите безопасности критически важной информационной инфраструктуры, 2019	ЦО КПК, CAC	Защита критически важной информационной инфраструктуры
		Руководящий комитет по национальной базе кибербезопасности, 2019	ЦО КПК	Контроль за деятельностью NCC

Продолжение табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	ИБЗК	Меры по оценке безопасности облачных вычислений, 2019	ЦО КПК, CAC	Контроль при закупке и использовании продуктов, включенных в каталоги специального оборудования сетевой безопасности; введение более высоких требований безопасности к облачным вычислениям, используемым государственными учреждениями и операторами связи
Третий уровень (2020 – н. в.)	СЦ	–	–	–
	ИБЦИ	Правила цифровых платформ, осуществляющих реализацию товаров в Интернете, 2021	SAMR	Ужесточение регулирования рынка онлайн-продаж
		Национальная дорожная карта внедрения Блокчейн, 2021	ЦО КПК, МПИ	Развитие Блокчейн по таким напралениям, как экономика, финансы, промышленность и госуправление; создание трех системообразующих предприятий и промышленных кластеров на основе Блокчейн; интеграция в сфере финансов Блокчейн, Cloud Computing, AI и Интернета; реализация концепта Smart City; внедрение Блокчейн в государственных услугах
	ИБФР	Ограничения циркуляции криптовалют на рынке КНР, 2021	PBC	Запрет финансовым учреждениям и платежным компаниям предоставлять услуги, связанные с транзакциями с криптовалютой, и предостережение инвесторов от спекулятивной криптовалютной торговли

Окончание табл. 3.2

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н. в.)	ИБЗК	Закон «О защите данных», 2021	ЦО КПК	Предотвращение сбора конфиденциальной информации технологическими компаниями, регулирование проблемы онлайн-мошенничества и кражи данных
		Закон «О защите персональных данных», 2021	ЦО КПК	Предотвращение сбора организациями и индивидуальными лицами, использования, обработки и передачи личной информации, незаконной торговли ею, а также предоставление или раскрытие личной информации других людей
		Создание Национального центра кибербезопасности, 2021	ЦО КПК	Обеспечение защиты в киберпростарнстве

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства; ЦО КПК – Центральные органы Коммунистической партии Китая; ВСНП – Всекитайское собрание народных представителей; МНТ – Министерство науки и технологий КНР; PBC – Народный банк Китая; CAC – Администрация киберпространства Китая; SAIC – Государственная администрация для промышленности и торговли КНР; CISC – Комиссия по надзору за страхованием; CBSC – Комиссия по банковскому надзору КНР; CSSC – Комиссия по надзору за ценными бумагами КНР; БОИНСБ – Бюро общественной информации и надзора за сетевой безопасностью; NCC – Национальный центр кибербезопасности; МПИ – Министерство промышленности и информатизации КНР; SAMR – Управление по регулированию рынка КНР; ПП – правительство г. Пекина.

Для сложившейся экосистемы регулирования цифровой экономики КНР характерно развитие всех составляющих блоков:

стратегии цифровизации, механизмов внедрения и регулирования отдельных цифровых инноваций и концепций, регулирования финансового рынка и блока защиты киберпространства. При этом выделяются рестриктивные практики в отношении защиты внутренеего сегмента Интернета, полной идентификации пользователей и контроля за цифровым контентом, поступательного внедрения запретительных мер в отношении криптовалютного рынка[7]. Таким образом, КНР является примером реализации политики управления национальной цифровой экосистемой и институциональными структурами системы, непосредственно государством. При этом государственно-частное партнерство, как показывает практика, носит очень условный и неравноправный характер. С учетом быстрого развития цифровой экономики китайские власти также столкнулись с проблемой монополизации рынков и недобросовестной конкуренции в Интернете[8]. В этой связи Управление по регулированию рынка КНР (SAMR) опубликовало проект свода правил, направленный на защиту прав потребитлей и ужесточение условий торговли в Интернете [903, 904].

Экосистема регулирования цифровой экономики в Российской Федерации также обладает своими уникальными особенностями. Как показывает анализ табл. 3.3, роль государства в формировании цифровой экономики можно условно разделить на два периода: 1998–2016 и 2017–2021 годы.

Если для первого периода харктерны, в большей степени, признаки рыночной или смешанной системы регулирования, то для современной России роль государства в формировании цифровой экономики является всеобъемлющей и затрагивающей все ключевые блоки экосистемы.

---

[7] КНР поступательно сокращала свободу криптовалютных операций в стране: в 2014 году РВС потребовал от коммерческих банков и торговых компаний закрыть счета в Биткойнах; в 2017 году запрещены операции ICO, криптовалюты как объекты биржевой торговли [901]; в 2019 году объявлено о намерении заблокировать доступ ко всем внутренним и иностранным биржам криптовалют и веб-сайтам ICO; в 2021 году введен запрет финансовым учреждениям и платежным компаниям предоставлять услуги, связанные с транзакциями с криптовалютой [902]. В 2021 году Центральный банк КНР ввел запрет финансовым учреждениям и платежным компаниям предоставлять услуги, связанные с транзакциями с криптовалютой.

[8] В результате антимонопольного расследования в отношении компании Alibaba Народным банком Китая и Комиссией по регулированию банковской и страховой деятельности КНР наложен штраф в 2,8 млрд долларов.

Таблица 3.3

Институциональная матрица экосистемы цифровой экономики на уровне программ Российской Федерации (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2000–2010 годы)	СЦ	Программа «Электронная Россия» на 2002–2010	Прав, МЦР, Ростел	Ускорение процессов информационного обмена в экономике, построение электронного правительства и на этой основе совершенствование деятельности государственных органов управления
		Стратегия развития информационного общества в РФ, 2008	Прав, МЦР, МЭР	Повышение качества жизни граждан, обеспечение конкурентоспособности, развитие экономической, социально-политической, культурной и духовной сфер общества. Программа «Информационное общество (2011–2020)»
	ИБЦИ	Создание инновационного центра «Сколково», 2010	МЭР, Прав, Пр,	Научно-технологический инновационный комплекс по разработке и коммерциализации новых технологий
	ИБФР	—	—	—
	ИБЗК	Центр реагирования на инциденты в области информационной безопасности (RU-CERT), 1998	РНИИ РОС	Реализация государственной политики в области информационной защиты
		Закон «О персональных данных» (№ 152-ФЗ), 2006	Пр, ГДиСФ, ФСНССИТ, Прав	Обеспечение защиты прав и свобод граждан при обработке персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2011–2016 годы)	СЦ	—	—	—
	ИБЦИ	Национальная технологическая инициатива (НТИ), 2014	Пр, ТПиУ	Долгосрочная программа по созданию новых рынков и обеспечению условий для технологического лидерства России к 2035 году. Одобрено 8 «дорожных карт» по рынкам Аэронет, Автонет, Маринет, Нейронет, Хелснет, Энерджинет, Технет и Кружковому движению, около 500 проектов получили финансирование. Проектным офисом НТИ является Российская венчурная компания (РВК)
	ИБФР	—	—	—
	ИБЗК	Центр реагирования на компьютерные инциденты в информационных системах госорганов (GOV-CERT), 2012	ФСБ	Координация деятельности субъектов критической информационной инфраструктуры Российской Федерации по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты
		Поправки к Федеральному закону «О банках и банковской деятельности», 2013	Пр, ГДиСФ, ЦБ	Обязательство финансовых учреждений, действующих на основании лицензии Центрального банка России, отражать все свои финансовые операции в электронных базах данных, их хранение не менее пяти лет

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2011–2016 годы)	ИБЗК	Создание системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА), 2013	Пр, ФСБ	Прогнозирование опасных ситуаций в области информационной безопасности, обеспечение взаимодействия владельцев IT-ресурсов при решении задач, связанных с обнаружением и ликвидацией компьютерных атак, с операторами связи и другими организациями, осуществляющими деятельность по защите информации; оценка степени защищенности критической IT-инфраструктуры от компьютерных атак и установление причин таких инцидентов
		Поправки к закону «Об информации, информационных технологиях и защите информации» (№ 149-ФЗ), 2014	Пр, ГДиСФ, МЦР, ФСБ, ЦБ	Введены обязательства по идентификации пользователей интернет-услуг в публичных точках доступа
		Закон «О внесении изменений в Федеральный закон «О борьбе с терроризмом» (№ 374-ФЗ), 2016	Пр, ГДиСФ, ФСБ	Обязательство операторов связи и организаторов распространения информации в сети Интернет хранить на территории Российской Федерации текстовые сообщения, речевую информацию, изображения, звуки, видео, другие сообщения пользователей (далее – содержание сообщений) на срок до шести месяцев после окончания их приема, передачи, доставки и (или) обработки
		Центр реагирования и противодействия угрозам в банковской сфере (FinCERT), 2015	ЦБ	Противодействие кибератак в отношении банковских и финансовых организаций

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2017–2019 годы)	СЦ	Национальная программа «Цифровая экономика Российской Федерации», 2017	МЦР, Прав, Пр, МЭР	Система правового регулирования цифровой экономики. В состав программы входят федеральные проекты: «Нормативное регулирование цифровой среды», «Кадры для цифровой экономики», «Информационная инфраструктура», «Информационная безопасность», «Цифровые технологии», «Цифровое государственное управление», «Искусственный интеллект»
		Стратегия развития информационного общества, 2017–2030	МЦР, Прав, Пр, МЭР	Нормативное регулирование, информационная инфраструктура, формирование исследовательских компетенций и технологических заделов, кадры и образование, информационная безопасность. Программа содержит «дорожные карты» мероприятий по таким направлениям, как энергетика, агропромышленный сектор, «умный город», электронная торговля (e-commerce), транспорт и логистика, финансовые технологии
	ИБЦИ	Государственная программа дополнительного образования в сфере цифровой экономики, 2017	МЦР	Подготовка кадров для цифровой экономики (программы обучения в области программирования, государство оплачивает 50% стоимости курсов, 180 тыс. человек до 2024 года)

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2017–2019 годы)	ИБЦИ	Федеральный проект «Цифровое государственное управление», 2017	МЦР	Цифровая трансформация системы государственного управления
		Федеральный проект «Искусственный интеллект», 2017	МЭР	Создание условий для использования продуктов и услуг, основанных на преимущественно отечественных технологиях AI
		Автономная некоммерческая организация (АНО) «Цифровая экономика», 2017	Прав	Обеспечение взаимодействия частных компаний, экспертных сообществ и органов госвласти при реализации программы «Цифровая экономика».
		Российский фонд развития IT, 2017	Прав	Продвижение российского программного обеспечения на внутреннем и зарубежных рынках, организация его тестирования и пилотного внедрения
		Отраслевые рабочие группы по цифровой промышленности, цифровому образованию и цифровому здравоохранению, 2019	АНО «Цифровая экономика»	Создание отраслевых центров компетенции в рамках ведомственных проектов цифровизации
		Дорожные карты по следующим направлениям: промышленный интернет, большие данные, компоненты робототехники и сенсорика, технологии виртуальной и дополненной реальностей, технологии беспроводной связи, нейротехнологии и искусственный интеллект, новые производственные технологии, системы распределенного реестра, квантовые технологии, 2019	РА	Формирование плана совместных действий бизнес-сообщества и органов исполнительной власти по разработке и применению «сквозных» цифровых технологий для достижения технологического лидерства, обеспечения экономического развития и социального прогресса РФ, выхода российских компаний на международные рынки

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2017–2019 годы)	ИБФР	—	—	—
	ИБЗК	Закон «О внесении изменений в отдельные законодательные акты Российской Федерации по вопросам применения информационных технологий в сфере охраны здоровья» (№ 242-ФЗ), 2017	Пр, ГДиСФ, МЗСР	Обязательство в отношении контроллеров данных при сборе персональных данных российских граждан в режиме онлайн хранить и обрабатывать их в базах данных, расположенных на территории РФ; формирование единой государственной информационной системы в сфере здравоохранения
		Закон о безопасности критической информационной инфраструктуры, 2018	ФСБ, ФСТЭК	Объектам критической инфраструктуры присвоены категории в зависимости от потенциального ущерба; обязательство владельцев инфраструктуры подключиться к государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак и передавать в нее информацию обо всех инцидентах
		Национальный координационный центр по компьютерным инцидентам (НКЦКИ), 2018	ФСБ	Обнаружение, предупреждение и ликвидация последствий компьютерных атак, реагирование на компьютерные инциденты
Третий уровень (2020–н. в.)	СЦ	Указ о национальных целях развития страны на период до 2030 года, 2020	Пр	Одной из национальных целей является «Цифровая трансформация», в рамках которой планируется достижение «цифровой зрелости» ключевых отраслей экономики и социальной сферы

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н. в.)	ИБЦИ	Закон «Об экспериментальных правовых режимах в сфере цифровых инноваций в Российской Федерации», 2020	Пр, ГДиСФ, МЭР	Формирование механизмов «регуляторной песочницы» в медицине, транспорте, сельском хозяйстве, финансовой деятельности, торговле, строительстве, предоставлении государственных и муниципальных услуг и осуществлении государственного контроля (надзора) и муниципального контроля, промышленности, связи и иных направлениях
		Концепция развития регулирования отношений в сфере технологий искусственного интеллекта и робототехники до 2024 года, 2020	Прав	Основы нормативного регулирования технологий искусственного интеллекта и робототехники
		Концепция развития технологий машиночитаемого права, 2021	Прав	Систематизированы имеющиеся представления о машиночитаемом праве, а также определены основные направления развития соответствующих технологий
		Стратегия цифровой трансформации российской экономики по 13 направлениям, 2021	Прав	Использование технологий AI и масштабирование отечественных решений в здравоохранении, образовании, госуправлении, строительстве, городском хозяйстве и ЖКХ, транспорте, энергетике, науке, сельском хозяйстве, финансовых услугах, промышленности, экологии, социальной сфере

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н.в.)	ИБЦИ	Дорожные карты по развитию в России Интернета вещей и Блокчейн, 2020	Прав, Ростех	Госкорпорация оценила реализацию проектов развития интернета вещей и Блокчейн в 22,4 млрд и 10,1 млрд руб. соответственно
		Закон о развитии интеллектуальных систем учета электроэнергии, 2020	Пр, ГДиСФ, Минэнего	Внедрение интеллектуальной системы учета элетроэнергии
		Подготовка серии предварительных национальных стандартов Интернета вещей, 2020	ТК, Ростел, ВИС, МПТ	Нормативное регулирование предварительных национальных стандартов IoT
		Утверждение национального стандарта в области больших данных (ГОСТ «Информационные технологии. Большие данные. Обзор и словарь»), 2021	НЦЦЭ, ИРИО	Обеспечение в предметной области «большие данные» взаимопонимания между органами власти, коммерческими компаниями и научно-образовательным сообществом
		Дорожная карта развития технологий передачи электроэнергии и интеллектуальных энергосистем на 2021–2024 годы	Прав, Минэнерго, МЭР	Развитие концепта Smart Grid
		Проект закона «О внесении изменений в Федеральный закон “Об информации, информационных технологиях и о защите информации” и отдельные законодательные акты Российской Федерации», в стадии согласования	МЭР	Базовое регулирование создания юридически значимых электронных дубликатов бумажных документов и создание правовых основ для долговременного хранения документов в электронном виде
		Проект создания госоператора больших данных, в стадии согласования	МЦР	Предоставление Big Data, накопленных министерствами и ведомствами, коммерческим разработчикам AI

Продолжение табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н. в.)	ИБЦИ	Концепция регулирования цифровых экосистем, в стадии согласования	Прав	Стимулирование поэтапной трансформации цифровых сервисов в сторону цифровых платформ и рынка экосистем, координация стратегий крупных цифровых платформ, разработка принципов налогообложения экосистем, а также порядка их слияния и поглощения
		Проект базовых принципов взаимодействия участников цифровых рынков, в стадии согласования	ФАС	Продвижение разумной открытости цифровых платформ, нейтральности отношения к различным сторонам рынка (включая конкурентов), обеспечение самостоятельности пользователей платформ при взаимодействии с ней, обеспечение прав пользователей платформы
	ИБФР	Закон о цифровых финансовых активах, 2020	Пр, ГДиСФ, МЭР, ЦБ	Введение понятия цифровой валюты и запрет ее оборота на территории страны, обязанность государственных служащих декларировать криптовалютные активы, приравнивание криптовалюты к налогооблагаемому имуществу, о котором необходимо уведомлять налоговые органы
		Проект внедрения «цифрового рубля», 2020	ЦБ	Поступательное замещение фиатной валюты цифровой, цифровизация финансовой системы страны
		Создание сервиса «Прозрачный Блокчейн», 2021	РФМ	Отслеживание криптовалютных операций граждан

Окончание табл. 3.3

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н.в.)	ИБФР	Проект основных направлений цифровизации финансового рынка, 2022–2024 годы	ЦБ	Регулирование оборота данных, экосистем и небанковских поставщиков платежных услуг, совершенствование электронного взаимодействия между участниками рынка, государством, гражданами и бизнесом. Продолжится развитие таких инфраструктурных проектов, как «Единая биометрическая система» (ЕБС), «Цифровой профиль», «Маркетплейс» и «Система быстрых платежей» (СБП). Кроме того, планируется внедрение открытых API и создание платформы коммерческих согласий
	ИБЗК	Центр правовой помощи гражданам в цифровой среде, 2021	Прав	Консультирование граждан, ставших жертвами незаконного использования персональных данных
		Проект Федерального закона «О внесении изменений в статью 7 Федерального закона “О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма” в части совершенствования процедур идентификации и упрощенной идентификации», в стадии согласования	МЭР	Расширение возможностей сбора и подтверждения сведений о клиентах (идентификации)

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования

финансового рынка; ИБЗК – институциональный блок защиты киберпространства; Пр – Президент РФ; Прав – Правительство РФ; ГДиСФ – Государственная дума и Совет Федерации РФ; МЦР – Министерство цифрового развития, связи и массовых коммуникаций РФ (Минцифры России); ФАС – Федеральная антимонопольная служба; ФСНССИТ – Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор); Ростел – ПАО «Ростелеко́м»; РА – госкорпорация «Росатом»; МЭР – Министерство экономического развития РФ; ФСБ – Федеральная служба безопасности РФ; Минэнерго – Министерство энергетики РФ (Минэнерго России); МЗСР – Министерство здравоохранения и социального развития РФ (Минздравсоцразвития России); ЦБ – Центральный банк РФ; ФСТЭК – Федеральная служба по техническому и экспортному контролю; МПТ – Министерство промышленности и торговли РФ (Минпромторг России); НКЦКИ – Центр реагирования на компьютерные инциденты в информационных системах госорганов; Ростех – Государственная корпорация по содействию разработке, производству и экспорту высокотехнологичной промышленной продукции «Ростех»; РФМ – Федеральная служба по финансовому мониторингу Российской Федерации (Росфинмониторинг); РНИИ РОС – Российский научно-исследовательский институт развития общественных сетей; ТПиУ – технологические предприниматели, представители университетов и исследовательских центров, крупные деловые объединения России, институты развития, экспертные и профессиональные сообщества; РВК – Российская венчурная компания; ТК – технический комитет «Технический комитет киберфизические системы (ТК 194)», ВИС – Всероссийский институт сертификации; НЦЦЭ – Национальный центр цифровой экономики МГУ; ИРИО – Институт развития информационного общества.

Сравнительный анализ по предложенной модели экосистемы регулирования цифровой экономики показывает общность структуры направлений внедрения цифровых инноваций и ргуляторных практик. Вместе с тем КНР и РФ демонстрируют активное государственное участие в формировании цифровой экономики будущего с широким использованием государственных ресурсов, включая административные, организационные и финансовые; государственно-частное партнерство на данном этапе не имеет четко выраженного характера. Государственное регулирование цифровизации США, главным образом, ориентировано на создание макросреды и базовой инфраструктуры, поддержание стабильности функционирования рынков, а также защиту киберпространства страны с учетом возможностей ее как родоначальника и бенефициара современных цифровых решений.

Правительство США в июне 2021 года выступило с инициативой, направленной на предоставление большего объема правительственных данных для исследователей AI, что является частью

стратегии сохранения передовых технологических позиций страны на мировом рынке[9] [905]. В отличие от США, КНР с 1 сентября 2021 года фактически национализировала Big Data, собираемые не только всеми национальными компаниями, но и иностранными, осуществляющими коммерческую деятельность на территории Китая [583, 906]. Кроме того, закон КНР предполагает диверсификацию данных, собираемых бизнесом, в зависиомсти от их важности для экономического развития государства, национальной безопасности, общественных интересов, а также законных прав и интересов физических и юридических лиц. Государственные органы управления разных уровней дополнительно уполномочены определять, какие именно данные являются важными и усиливать их защиту [907].

Среди направлений государственного регулирования цифровой экономики особое место занимает защита персональной информации. Данная тенденция распространяется как в развитых, так и развивающихся странах. Следует отметить, что Европе и Северной Америке потребители имеют больший контроль над обменом своими личными данными. Более того, государства стремятся обеспечить сохранность цифровых данных своих граждан даже в ущерб коммерческой деятельности технологических гигантов[10]. В Азиатско-Тихоокеанском регионе меньше всего стран имеют законодательство о защите прав потребителей в Интернете – всего 43% региона по сравнению с 73% в Европе и 71% в Америке. В разных штатах США действуют свои законы о конфиденциальности, а это означает, что у компаний разные уровни доступа к личным данным в зависимости от местоположения. Вместо единого национального закона о защите данных различные федеральные

[9] Национальная целевая группа по исследовательским ресурсам в области искусственного интеллекта (The National Artificial Intelligence Research Resource Task Force), включающая представителей академических кругов, правительства и промышленности во главе с должностными лицами из Управления по политике в области науки и технологий Белого дома и Национального научного фонда, разработает стратегию создания исследовательского ресурса в области AI. Предполагается предоставление исследовательсткого доступа к хранилищам анонимных данных о гражданах США – от демографических данных до состояния здоровья и привычек вождения.

[10] Регулятор конфиденциальности Европейского Союза предложил наложить штраф в размере более 425 млн долларов на Amazon, что является частью процесса, который может привести к самому большому штрафу в соответствии с законом о конфиденциальности ЕС [908].

законы регулируют порядок сбора, использования и передачи персональных данных FinTech компаниями[11] [909].

В технологическом разрезе целесообразно выделить следующие направления государственного регулирования цифровизации экономики. Так, США предоставляют технические ресурсы для поддержки IoT, предлагая руководство по разработке стандартов и совместимости [221, 910], разрабатывают и продвигают передовые практики IoT в области кибербезопасности[12]. Анализ показывает децентрализованный характер политики кибербезопасности IoT в США. Так, Министерство внутренней безопасности США (DHS) в 2016 году опубликовало «Стратегические принципы обеспечения безопасности Интернета вещей» (Strategic Principles for Securing the Internet of Thing), Министерство обороны США (DoD) на уровне офиса главного советника по кибернетическим вопросам отвечает за общее управление и регулирование кибердеятельности, связанной с защитой сетей [217].

На уровне технологических проектов в 2015 году Министерство транспорта США (DOT) выделило 42 млн долларов для реализации пилотных программ по подключению транспортных средств для тестирования технологий V2V и V2I в г. Нью-Йорке, Вайоминге и Тампе. Министерство транспорта США в 2015 году запустило проект Smart Cities по использованию связанных технологий для решения муниципальных задач и улучшения государственных услуг[13]. Управление общих служб (GSA) в рамках концепта Smart Buildings осуществляет проекты по модернизации зданий федерального правительства с помощью технологий IoT [224].

---

[11] В том числе Закон Грэмма-Лича-Блайли (GLBA); Закон «О справедливой кредитной отчетности» (FCRA); Закон «О Федеральной торговой комиссии», Закон «О прослушивании телефонных разговоров» и Закон «О конфиденциальности электронных коммуникаций» (ECPA). Ключевые федеральные агентства, которые обладают юрисдикцией по обеспечению соблюдения этих законов, включают: OCC; CFPB; SEC; CFTC; Федеральную торговую комиссию (FTC) [909].

[12] В 2015 году Федеральная торговая комиссия (FTC) опубликовала руководство для предприятий о том, как встроить безопасность в продукты IoT [910].

[13] В рамках инициативы для целей исследования выделено 160 млн долларов, реализован ряд проектов в области подключенных транспортных средств, разработки передовых технологий реагирования на чрезвычайные ситуации [910]. Дополнительно выделена федеральная поддержка в размере 80 млн долларов на проекты, связанные с климатом, транспортом, общественной безопасностью и преобразованием городских служб с использованием технологий IoT .

Великобритания в 2018 году выпустила свод правил IoT[14], призванный снять с потребителей бремя безопасной настройки их устройств и обеспечить надежную защиту встроенных устройств и услуг IoT [175, 911]. В рамках программы исследований «Периферия» (SDTaP) Великобритания инвестировала 30,6 млн фунтов по направлению «Безопасность цифровых технологий». Инвестиции включали в себя открытие в 2019 году Национального центра передового опыта в области кибербезопасности IoT-систем (The PETRAS)[15].

Государственные инициативы по цифровизации экономики, которые осуществляются в Индии в рамках программы «Цифровая Индия», направлены, в том числе на расширение использования AI [321, 912]. Национальный институт по трансформации Индии (National Institution for Transforming – India (NITI) инициирует проекты внедрения AI в целях национального развития в таких областях, как здравоохранение, сельское хозяйство, образование, умные города, инфраструктура и транспорт[16].

КНР продвигает внедрение технологий AI/ML через государственные агентства, которые сотрудничают с компанией Baidu в создании национальной лаборатории глубокого обучения. Разрабатывается гибкая нормативная среда для соответствующих экспериментов (подход «регуляторной песочницы») [559].

Государственное регулирование облачных технологий затрагивает в первую очередь проблематику кибербезопасности их использования в финансовой сфере [913]. Так, в Нидерландах Центральный банк (DNB) в рамках регуляторных практик требует предварительного уведомления о намерении использовать облачные технологии, включая проведение анализа облачного риска. При этом риски должны быть «изучены и смягчены», обеспечены провайдером «прозрачные и контролируемые операции»,

---

[14] Первый в мире кодекс под названием «Secure by Design» (British Government: DDCMS (2018). Code of practice for consumer IoT security).

[15] Национальный центр предполагает сотрудничество между ведущими британскими университетами, в том числе Имперским колледжем Лондона, Бристольским университетом и 150 промышленными предприятиями.

[16] По различным оценкам, на финансирование данных проектов планируется направить инвестиции в 14 млрд долларов с выходом на создание 100 умных городов в Индии.

а использование облачных технологий не должно «препятствовать надзору»[17].

Регулирующие органы выдвигают следующие требования в отношении облачного аутсорсинга:

1) должная осмотрительность в отношении поставщика и его услуг (включая оценку рисков, связанных с безопасностью и другими вопросами соблюдения);

2) банковский контроль и процессы, позволяющие эффективно:

а) соблюдать банком нормативные требования (включая надзор и мониторинг провайдера и процедур в отношении любых проблем безопасности);

б) осуществлять постоянный надзорный контроль со стороны регулятора (включая договорные условия, требующие от провайдера предоставления регулятору определенного доступа);

3) использовать механизм замещения банком облачных аутсорсинговых услуг.

Важно отметить, что регуляторы запрещают размещать банкам в облаке сервисы, связанные с их основной профильной деятельностью. Разрешается выносить на облачный ауторсинг только те сервисы, которые являются вспомогательными и не несут в себе опасности для клиентов.

Ключевое внимание в области цифровизации экономики регулирующие органы уделяют проблематике FinTech [914]. Проблематика регулирования сектора FinTech со стороны государства определяется рядом сложностей.

Во-первых, большинство FinTech компаний не являются финансовыми институтами в традиционном понимании, и поэтому они могут не попадать под контроль надзорных органов. Данная неопределенность статуса может приводить к их неопределенной юрисдикции со стороны нескольких разных регуляторов.

Во-вторых, регуляторы редко являются экспертами в области технологий, что затрудняет им оценку новых бизнес-моделей и практик.

---

[17] Договор предоставления облачных услуг банкам со стороны сторонних провайдеров должен, как минимум, предусматривать: надзор, напрямую или по доверенности, помещений поставщика; взаимный обмен информацией и по запросу, предоставление соответствующей информации для руководителей; правомочность банка модифицировать в любое время выбранным способом выполнение аутсорсинговых процессов; обязательство банков все время соблюдать все нормативные требования; требования к механизму прекращения соглашения.

В-третьих, центральные банки и другие финансовые регуляторы традиционно придерживаются консервативных подходов в оценках, осторожности в отношении цифровых инноваций.

В-четвертых, высокотехнологичные компании требуют со стороны регуляторов дополнительного функционала, следовательно – его ресурсного обеспечения.

В-пятых, новые предприятия могут быть политически ангажированными, что затрудняет выполнение регулирующими органами своих обязанностей независимого надзора.

Выделяют два направления государственного регулирования FinTech: микропруденциальное (поведенческое регулирование этики, соблюдение стандартов, направленных на защиту инвесторов, часто выполняемые регулятором ценных бумаг) и макропруденциальное (мониторинг платежеспособности и ликвидности банков и страховщиков, часто выполняемый Центральным банком) [915].

Модель Twin Peaks делит финансовое регулирование на две широкие части: регулирование поведения на рынке (включая защиту потребителей) и пруденциальное регулирование [916, 917]. Каждая из этих функций финансового регулирования возлагается на отдельного специализированного регулятора[18].

Финансовые регуляторы сосредоточены главным образом на обеспечении стабильности финансовых систем, включая такие компоненты, как финансовая доступность, финансовая целостность и защита финансового потребителя. Регуляторы пытаются разработать нормативную среду, которая одновременно поощряет цифровые инновации и выход на рынок новых игроков, устраняет непредвиденные риски. Среди направлений регулирования выделяют:

1) создание доступной, инклюзивной физической среды для принятия и использования цифровых финансовых услуг, включая

[18] Цель перехода к системе двойного пика финансового регулирования состояла в том, чтобы отделить и усилить поведение рынка и защиту потребителей от другой регулирующей цели, заключающейся в обеспечении более устойчивой, стабильной и надежной финансовой системы. Модель предполагает создание двух регуляторов с конкретными целями и четкими мандатами и позволяет каждому регулятору сосредоточиться на своем основном мандате. Кроме того, специализированные регулирующие органы, скорее всего, будут лучше подготовлены, чтобы идти в ногу с продолжающимся ростом финансовых конгломератов и растущей сложностью финансовых рынков. Если также снизить риск того, что один из аспектов регулирования, такой как пруденциальное регулирование, будет доминировать в сфере регулирования. С другой стороны, эта модель может создавать дублирование регулирования между двумя регулирующими органами и увеличивать риск сбоев обмена информацией из-за проблем сотрудничества и координации между регулирующими органами.

системы идентификации клиентов[19] и широкополосную инфраструктуру;

2) содействие внедрению цифровых финансовых услуг посредством реализации программ, нацеленных на оцифровку государственных платежей[20] и развитие более широкой экосистемы цифровых платежей, в особенности в розничных сетях [583]. Цель регулирования – повышение уверенности, безопасности и доверия к платежным системам посредством улучшения понимания, надзора и, при необходимости, расширения государственного вмешательства для защиты интересов розничных и коммерческих пользователей.

Помимо общей реформы регулирования или более целенаправленных и дифференцированных правил для конкретных видов деятельности, могут быть использованы другие средства, в их числе установление критериев для лицензионных исключений или отказов на основе четких принципов или информирование конкретных FinTech-организаций об отсутствии возражений (запретов) со стороны государства.

Регулирующие органы имеют тенденцию поощрять усиление конкуренции, открывая платежи более широкому кругу поставщиков, потому что барьеры для входа высоки, а обработка платежей требует экономии за счет масштаба. Ряд нормативных актов, таких как инициатива Великобритании по открытому банкингу, продвигают концепцию «платежи как услуга» (PaaS), предоставляя сторонним специалистам больший доступ к банковским данным через открытые API и технологии с открытым исходным кодом [583].

---

[19] Системы идентификации клиентов играют важную роль как в схемах доступа к финансовым услугам, так и в борьбе с отмыванием денег. Потребителям необходимо удостоверение личности для участия в официальных финансовых системах. Некоторые страны реализуют национальные программы идентификации с использованием цифровых и биометрических данных (например, программа Aadhar (Индия). Другие государства создают национальную базу данных, которая связывает все соответствующие существующие системы идентификации и доступна для уполномоченных сторон, таких как поставщики услуг.

[20] Оцифровка государственных потоков платежей позволяет сократить расходы, повысить прозрачность платежей, усилить борьбу с коррупцией и стимулировать граждан к открытию счетов в официальной финансовой системе. Например, Индия оцифровала свою программу субсидирования газа, что позволило сократить расходы на 25%, или 2 млрд долларов. Мексика реализовала программу по оцифровке и централизации всех платежей за 15 лет. Это позволило сэкономить 1,27 млрд долларов в год.

Многие центральные банки разработали (или находятся в процессе разработки) законодательные и лицензионные основы для регулирования новых и традиционных платежных систем [561][21]. В 2010 году в Китае внесены изменения в правила регулирования платежных систем, которые узаконили услуги онлайн-платежей и ввели их в режим государственного регулирования. Более того, Центральный банк КНР подтолкнул китайские банки к созданию общей платформы онлайн-расчетов для конкуренции с Alipay [918][22];

3) создание нормативно-правовой среды и внедрение эффективного надзорного режима, которые могут стимулировать цифровые финансовые инновации без ущерба для безопасности и стабильности системы [586]. Некоторые страны регулируют FinTech (в разрезе краудфандинга) в рамках ранее существовавшей нормативно-правовой базы, в то время как другие разработали индивидуальное регулирование для управления альтернативной финансовой деятельностью, основанной на долгах и акциях. Политики различаются в отношении: а) ограничений на тип инвесторов, которым разрешено инвестировать в предпринимательские стартапы через онлайн-платформы; б) суммы капитала, которые может инвестировать каждый инвестор; в) количества акций, которое бизнес может привлечь с использованием данного механизма в год и в сумме. Некоторые регуляторы рассматривают деятельность платформ P2P как банковскую, в то время как другие рассматривают их как посредников. В некоторых странах платформы P2P-кредитования регулируются регуляторами ценных бумаг, но без обязательного выполнения пруденциальных норм, применяемых к традиционному банковскому кредитованию [564].

В США FinTech-компании не подпадают под действие нормативной базы, специфичной для финансовых технологий, со стороны какого-либо одного федерального или государственного регулирующего

[21] Согласно Закону о платежных услугах Сингапура, вступившего в силу в 2020 году, новая система лицензирования предоставляет центральному банку гибкие средства контроля над различными поставщиками платежных услуг в зависимости от их конкретной деятельности и рисков, связанных с их деятельностью.

[22] Китайский интернет-гигант Alibaba Group Holding Ltdтрафом выплитил штраф в размере 18,228 млрд юаней (2,782 млрд долларов), наложенный Государственным управлением по регулированию рынка КНР (SAMR) по обвинению компании в том, что она злоупотребляла доминирующим положением на рынке услуг онлайн-платформ для розничной торговли в Китае (Alibaba по итогам IV финквартала получил убыток в $836 млн из-за рекордного штрафа. – Режим доступа: https://belretail.by/news/alibaba-po-itogam-iv-finkvartala-poluchil-ubyitok-v-mln-iz-za-rekordnogo-shtrafa. – Дата доступа: 15.05.2021).

органа, не подпадают под действие пруденциальных банковских нормативов для потребительского кредитования. Так, Crowdfunding-транзакции регулируются Комиссией по ценным бумагам и биржам (SEC) [564][23]. В 2015 году SEC издала правила, которые освобождают эмитентов в долевом краудфандинге от требования регистрации в рамках федерального закона о ценных бумагах[24]. Кроме того, в каждом штате существует свой собственный набор правил и положений. На федеральном уровне Бюро финансовой защиты потребителей (CFPB) обладает юрисдикцией в отношении поставщиков финансовых услуг для потребителей. Поскольку многие FinTech-предприятия нацелены на предоставление услуг преимущественно потребителям, CFPB имеет возможность обеспечивать соблюдение ряда законов о защите потребителей (таких как законы о потребительском кредитовании и законы о борьбе с дискриминацией), которые применяются к деятельности таких компаний. Робо-консультанты, являясь подгруппой инвестиционных консультантов, подпадают под требования регистрации SEC для таких консультантов [909]. В 2016 году в нескольких регионах Канады вступил в силу правовой документ, в соответствии с которым было создано правило об исключениях для долевого краудфандинга в Интернете [589][25].

---

[23] Они должны зарегистрировать ссуды, которые они предоставляют как ценные бумаги или Ноты, в SEC и подавать регулярные отчеты. Платформы должны проводить проверки «Знай своего клиента» для заемщиков и инвесторов. К ним относятся подтверждения того, что они являются гражданами США или законными резидентами, которым по крайней мере 18 лет, с действующим банковским счетом и действительным номером социального страхования. Другие проверки на мошенничество и проверку личности также проводятся.

[24] В случае, если выполняются следующие условия: 1) количество ценных бумаг, которые могут быть проданы эмитентом в течение 12-месячного периода, предшествовавшего дате такой сделки, не может превышать 1 млн долларов США; 2) в 12-месячный период индивидуальный инвестор может инвестировать в ценные бумаги, проданные эмитентом: «а) на сумму, превышающую 2000 долларов США, или 5% от меньшей годовой прибыли или чистой стоимости инвестора, если годовой доход или собственный капитал составляют менее 100 тыс. долларов США; или б) 10% от меньшей годовой прибыли или чистой стоимости инвестора, не превышающей проданную сумму в размере 100 тыс. долларов США, если как годовой доход, так и чистая стоимость активов составляют 100 тыс. долларов США или более».

[25] Он предусматривает, что освобождение будет доступно только в том случае, если: 1) сумма, привлеченная эмитентом, не превысит 1,5 млн. канадских долларов в течение 12-месячного периода; 2) аккредитованный инвестор не инвестирует более 25 тыс. канадских долларов на одну инвестицию (не более 50 тыс. канадских долларов на все сделки с массовым финансированием в зависимости от освобождения в том же календарном году) или лицо, которое не является аккредитованным инвестором, не нарушает верхний предел суммы инвестиций в 2500 канадских долларов (максимум 10 тыс. канадских долларов для совокупных инвестиционных сумм за один год).

В Азиатско-Тихоокеанском регионе в большинстве стран регулирование FinTech осуществляется в рамках разработанных нормативов и правил. Заметными исключениями являются Малайзия[26], Новая Зеландия и Южная Корея[27], которые создали специальное регулирование для FinTech-отрасли [564]. В 2021 году Комиссией по финансовым услугам Кореи (FSC) предложено пересмотреть надзорный регламент в отношении поставщиков услуг виртуальных активов (криптоактивов) (VASP) в направлении ужесточения ответственности, внедрения новых стандартов штрафов для VASP [919][28].

В Австралии платформы P2P-кредитования регулируются Австралийской комиссией по ценным бумагам и инвестициям (ASIC), на них не распространяются пруденциальные нормативы, поскольку они не принимают депозиты [592]. В 2016 году КНР опубликовал «План реализации для содействия финансовой интеграции», запущена «специальная акция» под управлением Народного банка Китая (PCB), направленная на стандартизацию различных форм финансирования в Интернете, содействие устойчивому развитию FinTech и усиление государственного контроля. FinTech в рамках данного свода правил классифицирован на следующие сегменты: Интернет-платежи, онлайн-кредитование, краудфандинг, продажа Интернет-фондов, онлайн-трасты, страховые услуги и потребительское финансирование в Интернете. Различные сегменты были поставлены под контроль разных страновых регуляторов. Направления регулирования главным образом включают требования к

[26] В Малайзии раздел 34 Закона «О рынках капитала и услугах» от 2015 года предусматривает, что розничные инвесторы могут участвовать в онлайн-краудфандинге на сумму до 5000 RM (около 1200 долларов США) на эмитента с общей суммой инвестиций, не превышающей 50 000 RM (12000 долларов). В то же время компаниям разрешено привлекать до 3 млн юаней (около 715 000 долларов) в течение 12-месячного периода, максимум до 5 млн юаней (около 1,2 млн долларов).

[27] В Южной Корее регулирующие органы проводят различие между тремя типами инвесторов с целью краудфандинга акций: профессиональные инвесторы, инвесторы, удовлетворяющие определенным требованиям в отношении доходов, и общие (розничные инвесторы). Для каждой группы применяются разные ограничения на сумму, которую можно инвестировать в каждый проект и в целом за год.

[28] Согласно пересмотренному положению, финансовые учреждения и VASP подвергнуться штрафам, если будет установлено, что они нарушают обязанности внутреннего контроля (например, неспособность сообщить о подозрительных транзакциях), обязанности по обслуживанию данных (например, неспособность хранить соответствующие данные о подозрительных транзакциях) и обязанности, непосредственно относящиеся к VASP (например, неспособность вести отдельное управление записями транзакций клиентов).

разработке планов, стандартизированных форматов и образовательным мероприятиям для потребителей. Они также включают промежуточные цели, такие как создание новых механизмов координации или контроля. Конечной целью регулирования было заявлено создание системы, которая уравновешивает постоянные инновации, основанные на рыночной конкуренции, с необходимостью ограничить коррупцию.

Комиссия по регулированию банковского дела КНР в 2016 году выпустила подробные руководящие принципы для отрасли P2P, в которых изложены требования о регистрации платформ в местных финансовых органах для получения соответствующих лицензий на ведение бизнеса, для поддержания определенного минимального уровня капитала и использования банков в качестве хранителей для средств клиентов [564]. Платформам запрещено принимать вклады от населения, создавать пулы активов и предлагать гарантированные доходы. Платформы также должны представлять регулярные отчеты с подробным описанием оборота кредитов и ставок по умолчанию в установленную правительством центральную базу данных для онлайн-кредитования.

В Латинской Америке правила, регулирующие массовое инвестирование, разнообразны. В Бразилии сделки с акциями открыты для всех инвесторов, и в настоящее время нет ограничений на количество инвестиций. Краудфандинговые компании могут привлекать до 690 тыс. долларов в год. В Мексике краудфандинг в акционерном капитале разрешен только для аккредитованных инвесторов, которые зарабатывают, по меньшей мере, эквивалент 160 тыс. долларов в год [589].

В Турции подход регуляторов заключается в том, чтобы сравнить деятельность FinTech с другими игроками в финансовой отрасли и навязывать им те же требования [920][29].

Несмотря на то, что были предприняты важные усилия для обеспечения финансовой интеграции в Европе, нормативные положения на рынке краудфандинга остаются крайне фрагментированными. С 2014 года в Великобритании FCA контролирует платформы

[29] Закон «О банках» № 5411, Закон ««О платежных системах и системах расчетов по ценным бумагам, платежным услугам и учреждениям, занимающимся электронными деньгами»» № 6493, Закон «О банках и кредитных картах» № 5464, и их вторичные положения являются основными, они влияют на компании FinTech в сфере банковских и платежных услуг.

P2P, которые ввели режим регулирования, основанный на раскрытии информации, для защиты розничных инвесторов. При этом FCA освобождают от регистрации долевой краудфандинг при условии, что краудфандинговые платформы ограничивают деятельность с клиентами, которые являются опытными инвесторами, состоятельными частными лицами или инвесторами, которые могут получить консультации профессиональных институтов[30]. Правительство Соединенного Королевства также инвестирует деньги в малый бизнес через кредиторов P2P, предлагая налоговые льготы для потребителей, которые намерены инвестировать через кредитные механизмы P2P. С целью стимулирования розничных инвестиций в данный сектор в 2016 году создан Инновационный финансовый индивидуальный сберегательный счет (IFISA), который позволяет потребителям инвестировать до 15 тыс. фунтов стерлингов в год в P2P-платформы, без необходимости выплачивать налоги по своим доходам [564].

Данный подход позволил укрепить сектор FinTech в Соединенном Королевстве, создать в этой стране крупнейший рынок P2P-кредитования в Европе (75% альтернативного сектора кредитования Европы).

В ФРГ все виды исключений по регистрации краудфандингового финансирования прописаны в Законе «О защите мелких инвесторов»,

[30] Для других клиентов, не включенных в вышеуказанную группу, платформы должны гарантировать, что эти клиенты удостоверяют, что они не инвестируют более 10% своих чистых инвестируемых финансовых активов (исключая их основное место жительства, пенсии и страхование жизни). FCA требует, чтобы платформы отправляли тест на соответствие, прежде чем отправлять инвестиционные материалы клиентам, если не предусмотрено иное [564]. В 2014 году Великобритания стала первой страной в мире, которая создала нормативную базу специально для платформ P2P-кредиторов. В соответствии с этим они лицензируются FCA. Лицензия позволяет им выдавать кредиты и быть членом национальных кредитных бюро. FCA также требует, чтобы платформы содержали средства клиентов отдельно от их собственных и содержались на сторонних счетах, чтобы предотвратить смешивание средств клиентов. Это требует от платформ следовать определенным пруденциальным нормам, таким как удержание капитала в условиях финансовых потрясений. Это отдельно от резервного фонда или кредитных резервов, которые некоторые платформы создали добровольно. Помимо обязательных минимальных требований к капиталу и текущих требований к отчетности, платформы также должны иметь механизмы или планы урегулирования для обеспечения продолжения обслуживания займа в случае прекращения существования платформы и обеспечения того, чтобы инвесторы не проиграли.

вступившем в силу в 2015 году [589][31]. Вместе с тем P2P-компании обязаны приобретать банковскую лицензию или сотрудничать с банками. В 2014 году Франция выпустила свод правил и положений о P2P-кредитовании, которые позволяют платформам работать в соответствии с индивидуальными требованиями [564].

FinTech-компании должны подвергаться адекватным требованиям безопасности, защиты потребителей и финансовой стабильности в сфере борьбы с отмыванием незаконно приобретенных средств и финансированием терроризма (ПОД-ФТ по классификации FATF), даже если они являются вспомогательными или аутсорсинговыми поставщиками услуг [583]. Новые технологии и бизнес-модели позволяют FinTech компаниям оказывать финансовые услуги, такие как проведение платежей, минимизируя регуляторный арбитраж[32] и выход за пределы традиционного надзорного инструментария со стороны центрального банка. Нормативно-правовая база и подходы к надзору для банков и других финансовых учреждений применяются к новым игрокам в сфере FinTech в той степени, в которой они соответствуют их профилям рисков и системной значимости. В отличие от банков, они не обязаны хранить резервы под обесценение портфеля в отношении ожидаемых будущих убытков по кредитам. От них также не требуется периодически проводить строгие стресс-тесты, чтобы доказать, что они могут пережить сценарий серьезного спада, как указано регулирующими органами [583]. Несмотря на то, что власти осознают риски, на данном этапе регуляторные меры выглядят маловероятными. Платформы являются многообещающим источником финансирования для малых предприятий, которые не всегда могут получить банковский кредит.

---

[31] Подраздел 1 раздела 2а четко указывает на то, что до тех пор, пока сумма финансирования не превысит 2,5 млн евро, требования к раскрытию информации для эмитента отсутствуют. Наряду с освобождением Закон устанавливает ограничение на максимальные суммы инвестиций для частного акционерного финансирования. Платформы обязаны удостовериться, что каждый инвестор инвестирует только в один инвестиционный проект до 1000 евро (или до 10 тыс. евро, как только инвестор докажет, что имеет более 100 тыс. евро финансовых активов), или его или ее сумма инвестиций не будет более чем вдвое превышать среднемесячный чистый доход.

[32] Регуляторный арбитраж подразумевает под собой одинаковые сделки, которые совершаются разными субъектами и, соответственно, попадают под разное регулирование. Субъекты, задействованные в регуляторном арбитраже, пытаются извлечь выгоду из разницы в правовом регулировании смежных юрисдикций.

Возможные формы усиленного законодательства могут включать требования по сохранению риска, минимальные требования к капиталу, чтобы помочь альтернативным кредитным платформам противостоять финансовым потрясениям (например, в Великобритании), а также повышенным требованиям к раскрытию информации и отчетности.

Нормативные акты могут повысить затраты онлайн-кредиторов, но могут также принести пользу отрасли в долгосрочной перспективе, поощряя более строгие стандарты кредитования и защиту потребителей, тем самым стимулируя более активное участие розничных инвесторов.

Нормативно-правовые и надзорные основы, пруденциальные инструменты для проектирования платежных систем ориентируются на две основные цели в регуляторной политике: 1) безопасность и 2) эффективность. Проблема безопасности включает задачи, связанные с финансовой стабильностью и отказоустойчивостью, а также конфиденциальностью клиентов, тогда как эффективность связана с рентабельностью, конкурентоспособностью и инновационными аспектами платежных систем [100].

Вместе с тем следует также отметить фискальные аспекты регулирования определенной деятельности FinTech, направленные на нивелирование искусственных технологических преимуществ данных компаний, а также обеспечение стабильности финансового рынка. Так, ряд исследований показал, что генерируемые высокочастотной алгоритмической торговлей (HFT) списки заказов могут вводить в заблуждение участников рынка, создавая условия для манипулирования их поведением [176]. В этой связи некоторые регуляторы ввели специальный налог для ограничения больших объемов сообщений и уведомлений. С 2012 года Франция ввела налог на финансовые транзакции в отношении отмененных или измененных в течение полусекундного промежутка времени заказов HFT[33]. Аналогичным образом в 2013 году Италия ввела налог на финансовые транзакции[34]. Налог на соотношение заказов и

[33] Налог в размере 0,01% применяется к измененным или отмененным ордерам французского HFT, когда соотношение заказов к торговле (OTR) превышает 5, даже если в этом случае он не оказывает отрицательного влияния на качество рынка с точки зрения объема торгов, волатильности, спреда и глубины.

[34] Налогом облагаются: 1) передача владения акциями и другими участвующими финансовыми инструментами, 2) операции с производными финансовыми инструментами и другими переводными инструментами, ценные бумаги и 3) HFT.

продаж (order-to-trade ratio, OTR) для ограничения активности HFT введены также в Норвегии, Германии и Канаде [921, 922].

Регулирование государства в криптовалютной сфере имеет четыре цели (связаны с различными наборами интересов).

1. Основная сфера интересов – это заинтересованность:

а) в противодействии отмыванию денег;

б) финансировании преступности;

в) уклонении от уплаты налогов[35].

2. Монополия на выпуск национальной валюты, с учетом интересов коммерческих банков и компаний, которые вовлечены в платежную индустрию[36].

3. Защита интересов своих потребителей. Выделяют три направления регулирования:

а) защита от мошенничества;

б) создание нормативной базы для урегулирования споров при совершении транзакций с криптовалютами;

в) формирование законодательных основ для передачи прав собственности на криптоактивы (например, в случае смерти владельца, если закрытые ключи не будут должным образом храниться и записываться) [923].

4. Построение эффективной системы налогообложения данной сферы, включая:

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

---

[35] В 2020 году в Эстонии Управление финансовой разведки (ПФР) отозвало лицензии у более 1000 криптовалютных фирм на фоне усилившихся опасений по поводу отмывания денег (Estonia Revokes More Than 1,000 Crypto Firms' Licenses This Year. – Режим доступа: https://news.bitcoin.com/estonia-revokes-1000-cryptocurrency-firms-licenses/. – Дата доступа: 15.12.2020). По данным компании Elliptic, объем взысканий США со стартапов и физических лиц в индустрии криптовалют с 2009 по 2021 год составил 2,5 млрд долларов. 55% взысканий связаны с незарегистрированной продажей ценных бумаг (1,38 млрд долларов) и мошенничеством (928 млн долларов). Штрафы за нарушение антиотмывочного законодательства составили 183 млн долларов (Исследование: США взыскали с участников криптоиндустрии $2,5 млрд штрафов. – Режим доступа: https://forklog.com/issledovanie-ssha-vzyskali-s-uchastnikov-kriptoindustrii-2-5-mlrd-shtrafov/. – Дата доступа: 22.06.2021).

[36] Платежные посредники занимаются конкуренцией действующих операторов и пытаются защитить свой бизнес и свое положение на рынке, стремясь к вмешательству государства и регулированию своих конкурентов.

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, до тех пор, пока эта деятельность приносит значительный доход.

Вместе с тем необходимо учитывать децентрализованный, разнообразный и международный характер рынков криптовалют [583]. Дифференцированный подход характерен не только для международного уровня, но и национального. Так, в США цифровые валюты подпадают под регулирующий мандат различных органов в зависимости от их предполагаемой функции и характеристик. Ввиду децентрализованного характера цифровых валют Комиссией по торговле товарными фьючерсами США (CFTC)[37] они (в том числе Биткойн) считаются товаром и находятся под соответствующим надзором и регулированием. В других случаях такие токены, как Ripple[38] или TON's Gram, были определены в 2017 году как ценные бумаги[39] и подпали под нормативные ограничения со стороны

[37] В соответствии с Законом об обмене товарами (The Commodity Exchange Act, CEA), CFTC осуществляет надзор за контрактами с производными финансовыми инструментами, включая фьючерсы, опционы и свопы, которые связаны с товаром. Закон CEA определяет «товар» как включающий сельскохозяйственную продукцию, «все другие товары и предметы» и «все услуги, права и интересы, в которых заключаются контракты на будущую поставку в настоящее время или в будущем. CFTC пришла к выводу, что определенные виртуальные валюты являются «товарами» согласно CEA. CFTC приняла меры к незарегистрированным биржам фьючерсов на Биткойны и фирм, незаконно предлагающим маржинальные или финансируемые розничные транзакции с виртуальной валютой; соблюдению законов, запрещающих фиктивные сделки на платформе деривативов, и законов, требующих от фирм выполнения адекватных процедур по борьбе с отмыванием денег; выпустила пояснительное руководство относительно того, имела ли место «фактическая поставка» в контексте розничных товарных операций в виртуальных валютах; вынесла предупреждения об оценках и волатильности на спотовых рынках виртуальных валют; обратила внимание на мошеннические схемы Понци в виртуальной валюте [924].

[38] Комиссия по ценным бумагам и биржам в 2020 году объявила о подаче иска против Ripple Labs Inc., обвиняя в привлечении более 1,3 млрд долларов через незарегистрированную эмиссию ценных бумаг в форме цифровых активов (XRP) [925]. SEC также определила, что токены, выпущенные DAO, являются ценными бумагами в соответствии с Законом «О ценных бумагах» 1933 года и Законом «О бирже ценных бумаг» 1934 года [580].

[39] Согласно так называемому «тесту Хоуи», основанному на основополагающем решении Верховного суда 1946 года по делу Комиссии по ценным бумагам и биржам против WJ Howey Co., «инвестиционный контракт» существует, если есть вложение денег в обычное предприятие с ожиданием прибыли, полученной от усилий других [924].

Комиссии по ценным бумагам и биржам США (SEC)[40]. Служба внутренних доходов (IRS)[41] рассматривает цифровые валюты в качестве объектов собственности. В 2020 году данное агентство анонсировало запуск специального программного обеспечения, позволяющего анализировать и выявлять операции с цифровыми активами, которые носят подозрительный характер с целью усиления контроля за перемещением средств в криптовалюте [772].

Криптовалютные биржи в США действуют в соответствии с Федеральным законом о банковской тайне (BSA) как регулируемые предприятия [834]. Агентство по борьбе с финансовыми преступлениями Министерства финансов США (FinCEN) осуществляет надзор и несет ответственность за их регулирование. Более того, FinCEN выступает в качестве Подразделения финансовой разведки (ПФР), ответственного за получение и анализ отчетов о подозрительных операциях и другой информации, касающейся отмывания денег, финансирования терроризма и связанных с этим преступлений. FinCEN также регулирует деятельность физических и юридических лиц, занимающихся приемом и передачей конвертируемой виртуальной валюты (CVC)[42].

В 2021 году США подготовлен совместный отчет [926] Президентской комиссии по регулированию финансовых рынков Федеральной корпорации страхования депозитов (FDIC) и Управления валютного контролера США (OCC), в котором рекомендовано незамедлительно принять новый закон, регулирующий механизмы

[40] В контексте виртуальной валюты миссиия SEC заключается в быстром росте рынка «первичных предложений монет» («ICO») и его широкомасштабном продвижении в качестве средства для новых инвестиционных возможностей. В 2017 году Комиссия по ценным бумагам и биржам опубликовала отчет о расследовании, в котором предупредила инвесторов о потенциальных мошенничествах с участием компаний, утверждающих, что они связаны или участвуют в ICO [924].

[41] Служба внутренних доходов (IRS) рассматривает виртуальную валюту как собственность для целей федерального налогообложения США, что означает, что общие принципы налогообложения, применимые к сделкам с недвижимостью, также применимы к операциям с виртуальной валютой. Доходы, включая прирост капитала, от операций с виртуальной валютой подлежат налогообложению, а сами операции с виртуальной валютой должны указываться в налоговой декларации налогоплательщика. Кроме того, заработная плата, выплачиваемая сотрудникам в виртуальной валюте, подлежит налогообложению. Компании, получающие за товары или услуги в виртуальной валюте, должны включать платежи в свой валовой доход [924].

[42] Виртуальная валюта, которая либо имеет эквивалентную стоимость валюты, либо выступает в качестве заменителя валюты и, следовательно, является разновидностью стоимости, которая заменяет валюту.

стейблкоина и уделить особое внимание эмитентам стейблкоинов и поставщикам услуг кастодиальных кошельков[43]. В отчете рассматриваются три категории пруденциального риска в отношении стейблкоинов: а) риск потери стоимости стейблкоинов из-за риска бегства и последующих потенциальных эффектов заражения системы; б) риски платежной системы, связанные с утратой возможностей пользователей совершать платежи с помощью стейблкоинов; в) риски масштаба, включая системный риск, риск чрезмерной концентрации экономической власти и риск антиконкурентных эффектов [927]. Вместе с тем, несмотря на принимаемые регуляторные меры, США занимают в мировом рейтинге принятия криптовалют в 2020 году только шестое место.

Канада на федеральном уровне рассматривает криптовалюту как ценные бумаги, Австралия – как юридические свойства [928]. Япония официально признает Биткойны и цифровые валюты в качестве платежных средств [929].

В Великобритании с января 2021 года в соответствии с правилами борьбы с отмыванием денег введена обязательная регистрация в FCA компаний по производству криптоактивов[44]. С 2021 года работа без регистрации является уголовным преступлением [583, 930]. Кроме того, в апреле 2020 года для социальных сетей и поисковых систем (таких как Facebook и Google) введен налог на доходы от цифровых услуг, в ноябре 2021 года введен 2%-й налог на доходы от цифровых услуг для криптовалютных бирж.

Индия рассматривает предложение о введении 18%-го налога на Биткойн-транзакции[45]. Центральное бюро экономической разведки (CEIB) предложило рассматривать криптовалюту как оборотный актив, а налог на товары и услуги взимать с прибыли от торгов.

---

[43] Кастодиальный кошелек – тип кошелька, ключи от которого находятся во владении торговой площадки, которая отвечает за их сохранность и безопасность пользовательских активов. Кастодиальные кошельки (биржи) работают по принципам, похожим на традиционные финансовые системы.

[44] HMRC не признает цифровые активы финансовым инструментом, и поэтому криптовалютные торговые платформы и обменники не имеют права на финансовые льготы.

[45] Центральное бюро экономической разведки (CEIB), подразделение Министерства финансов Индии, внесло соответствующее предложение в Центральный совет по налогам и таможне. Стоит отметить, что это уже второе предложение, которое связано с налогообложением криптовалютных операций. В начале декабря 2020 года налоговая служба Индии предложила ввести 30%-й налог на прибыль от инвестиций в цифровые активы.

Агентство считает, что в случае введения это налогообложение может помочь сократить предполагаемое использование криптовалюты в незаконной деятельности, а также аккумулировать до 1 млрд долларов в год. В 2018 году Центральный банк страны запретил всем финансовым учреждениям работать с любыми криптовалютными компаниями. Хотя это не был прямой запрет на использование криптовалют, большинство компаний прекратили свою деятельность в стране[46].

Центральный банк Турции в 2021 году запретил использование криптовалют и криптоактивов для покупок, сославшись на возможный «непоправимый» ущерб и риски транзакций [931][47]. Аргентина в 2021 году ввела обязательное ежемесячное уведомление криптобиржами обо всех транзакциях клиентов [932].

Важнейшим регуляторным аспектом цифровизации экономики является проблематика кибербезопасности [922]. Правительства играют важную роль в противодействии киберугрозам, рекомендуя стандарты безопасности в ключевых секторах промышленности (например, NIST Cybersecurity Framework) и усиливая судебное преследование за киберпреступления [933]. В настоящее время в США нет единого закона о кибербезопасности общего применения, за исключением ограничений «недобросовестной» торговой практики, поэтому большинство предприятий должны соблюдать отраслевые федеральные законы и законы штата. Регулирование кибербезопасности осуществляет автономное федеральное Агентство по кибербезопасности и безопасности инфраструктуры (CISA), призванное осуществлять взаимодействие с агентствами национальной безопасности с целью киберзащиты критической

[46] В марте 2021 года Верховный суд Индии признал решение Центрального банка неконституционным.

[47] В апреле 2021 года турецкая криптоплатформа Vebitcoin заявила, что прекратила всю деятельность после того, как столкнулась с финансовыми трудностями, и что она как можно скорее проинформирует клиентов о ситуации. Несколькими днями ранее криптоплатформа Thodex стала недоступна онлайн, а ее генеральный директор и основатель Thodex Фарук Фатих Озер улетел в Албанию, похитив 2 млрд долларов из средств инвесторов. Турция выдала международный ордер на арест Озера. Турецкие власти заблокировали внутренние банковские счета Vebitcoin (A second bitcoin exchange collapses in Turkey amid crackdown on cryptocurrencies. – Режим доступа: https://www.cnbc.com/2021/04/26/turkish-bitcoin-exchange-vebitcoin-collapses-amid-crypto-crackdown.html. – Дата доступа: 26.04.2021).

инфраструктуры[48]. Бюджет страны на противодействие киберпреступности в 2019 году составил 15 млрд долларов [826, 933]. В 2020 году Управление по контролю иностранных активов США (OFAC)[49] объявило о намерении отслеживать все платежи Интернет-вымогателям. Прогнозируется более широкое применение стратегии «постоянного противостояния» в отношении финансовых преступлений. Существует также возможность наложения экономических санкций на организации, территории или даже страны, послужившие исходной точкой для запуска кибератак, за недостаточно эффективное противодействие этим атакам [934]. Правительства могут использовать специальные средства для мониторинга, деанонимизации и перехвата счетов с Биткойнами [857][50].

[48] Каждый из секторов критической инфраструктуры в США имеет свой отдельный режим регулирования. Энергетический, химический, транспортный и другие сектора имеют подробные правила, специфичные для их области. Например, в секторе финансовых услуг организации, предоставляющие финансовые услуги, должны соблюдать GLBA и правила его реализации (Комиссия по ценным бумагам и биржам, другие регулирующие органы и отраслевые группы, такие как Регулирующий орган финансовой индустрии («FINRA») и Национальная фьючерсная ассоциация («NFA»), опубликовали соответствующие руководства по кибербезопасности.

[49] Управление по контролю за иностранными активами Министерства финансов (OFAC) регулирует экономические и торговые санкции и обеспечивает их соблюдение в отношении террористических групп; международных торговцев наркотиками; тех, кто занимается деятельностью, связанной с распространением оружия массового уничтожения, злонамеренной кибердеятельностью, других организаций, представляющих угрозу национальной безопасности, внешней политике или экономике Соединенных Штатов, исходя из целей внешней политики и национальной безопасности США.

[50] В октябре 2020 года Управление по контролю за иностранными активами Министерства финансов США (OFAC) и Сеть по борьбе с финансовыми преступлениями (FinCEN) выпустили отдельные рекомендации, касающиеся осуществления платежей в адрес киберпреступников. Отмечается, что проведение платежей может повлечь санкции и штрафы в отношении как организаций-жертв, так и компаний, с помощью которых осуществляются платежи. Функционирует индустрия консультантов и экспертов в данной области, которые помогают жертвам вымогателей договариваться и платить злоумышленникам. В предупреждении OFAC приводятся примеры создателей программ-вымогателей и злоумышленников, которые были включены в санкционный список OFAC (например, два гражданина Ирана, отмывавшие доходы, полученные от использования программы SamSam). Предупреждение OFAC подкрепляет предыдущие правительственные указания не платить злоумышленникам-вымогателям, поскольку это стимулирует будущие атаки. OFAC предупреждает, что жертвы программ-вымогателей и консультанты, которые помогают им совершать платежи, могут столкнуться с серьезными штрафами, связанными с нарушениями санкций [849].

В принятой в Великобритании Стратегии национальной кибербезопасности (на 2016–2021 годы) подчеркивается политическое, дипломатическое, технологическое, коммерческое и стратегическое преимущество для государственных и негосударственных субъектов в использовании тактики кибератак, при этом «государственный, оборонный, финансовый и телекоммуникационный сектора» становятся основными целями для тех, кто стремится разрушить, дестабилизировать или использовать ресурсы потенциального противника [935]. В уголовном законодательстве Германии определены четыре категории компьютерных преступлений, в том числе преступление, связанное со шпионажем или фишингом данных, преступление, связанное с подделкой данных, а также действия, способствующие компьютерному саботажу [936]. В Уголовном кодексе КНР определены преступления в отношении программного обеспечения или инструментов для незаконного вмешательства в работу систем и манипулирование ими [937]. В 2016 году вступил в действие Закон «О национальной кибербезопасности», который содержит несколько основных принципов и инноваций, таких как суверенитет в киберпространстве, иерархическая система защиты кибербезопасности, система защиты критической информационной инфраструктуры, система оценки безопасности для перекрестного доступа передачи данных и система проверки безопасности для сетевых продуктов и услуг [938, 939]. Закон регулирует ряд направлений, включая защиту данных, конфиденциальность и государственный контроль, уточняя и систематизируя фрагментированный и дезорганизованный режим кибербезопасности страны. Кроме того, законодательство предусматривает, что критически важное сетевое оборудование и продукты кибербезопасности должны соответствовать национальным стандартам и обязательным требованиям, а также проверяться и сертифицироваться квалифицированным учреждением перед продажей или предоставлением [938]. В 2017 году Администрация киберпространства Китая (CAC), ответственная за обеспечение соблюдения Закона «О кибербезопасности», разработала новые административные правила для онлайн-продуктов и услуг. Помимо создания Национального центра кибербезопасности (NCC) осуществляется обучение профессионалов в данной сфере в специальной школе на базе NCC [940]. К инфраструктуре кибербезопасности следует также отнести Китайский

центр сертификации информационной безопасности (ISCCC), Центр оценки безопасности информационных технологий Китая (CNITSEC)[51], Индустриальный парк кибербезопасности[52] [941].

В Японии Закон «О кибербезопасности» принят в 2014 году. В 2018 году Сингапур принял Закон «О кибербезопасности», в котором установлена схема двойного лицензирования, которая налагает различные квалификационные требования для поставщиков услуг кибербезопасности, проводящих расследования, и поставщиков услуг кибербезопасности, не проводящих расследования. Данная дифференциация увеличивает входной барьер для индустрии кибербезопасности и повышает общий уровень безопасности. Вместе с тем данный подход может привести к потере конкурентоспособности на рынке, особенно для малых предприятий, из-за чрезмерных затрат на поддержание безопасности сети.

Проблематика кибербезопасности является важнейшим элементом в контексте защиты критически важной инфраструктуры. В 2011 году Шведское агентство по чрезвычайным ситуациям в гражданском секторе (MSB) опубликовало национальную стратегию защиты важных государственных служб. В 2015 году создан Шведский центр исследований защиты критической инфраструктуры (CenCIP) [759]. В 2016 году MSB опубликовало обновленную версию «Национальной оценки риска», в которой в перечень угроз в отношении критически важных объектов инфраструктуры включены: перебои с энергоснабжением; нарушение электронных коммуникаций; нарушение работы платежной системы; нарушение снабжения продовольствием; нарушение подачи питьевой воды; сбои в транспортной системе; нарушение поставок лекарств. Кибератаки и терроризм перечислены в списке антагонистических угроз. Отмечается, что критическая инфраструктура должна быть надежной и устойчивой, чтобы избежать серьезных каскадных эффектов.

---

[51] Также известный как 13-е бюро Министерства государственной безопасности, которое наблюдает за состоянием кибербезопасности государственных учреждений.

[52] Цель состоит в том, чтобы сконцентрировать бизнес и капитал, привлечь таланты из близлежащих университетов и продвинуть научные исследования в сторону коммерциализации. Индустриальный парк NCC включает в себя штаб-квартиру, частные научно-исследовательские центры, «национальный исследовательский центр кибербезопасности», инновационный и предпринимательский инкубатор, а также «стратегические предприятия в области военно-гражданского слияния и кибербезопасности».

В 2013 году Датское агентство по управлению чрезвычайными ситуациями (DEMA) опубликовало «Национальный профиль риска»[53]. Финская «Национальная оценка рисков»[54] обнародована в 2016 году. Норвежским управлением гражданской защиты в 2012 году подготовлен «Национальный анализ рисков», который был обновлен в 2014 году[55]. Объектом регулирования Закона о национальной кибербезопасности КНР выступает в том числе критическая информационная инфраструктура [937]. Администрация киберпространства Китая (CAC) определяет критическую инфраструктуру как информационные или промышленные системы управления, которые предоставляют сетевые информационные услуги населению или поддерживают работу важных отраслей, таких как энергетика, телекоммуникации, финансы, транспорт, коммунальные услуги и т. д. [942]. Таким образом, это те сети, которые, будучи поврежденными в результате атаки системы кибербезопасности, могут привести к ущербу в национальной политике, экономике, обороне, общественной жизни и собственности[56].

[53] В отчете инциденты классифицируются в зависимости от того, являются ли они искусственными или естественными, природные инциденты подразделяются на экстремальные погодные явления и серьезные инфекционные заболевания, а искусственные инциденты делятся на две подкатегории: аварии и угрозы безопасности. DEMA выбрало десять типов инцидентов для дальнейшего расследования: ураганы, сильные штормы и штормовые нагоны, проливные дожди и облачность, пандемический грипп, болезни животных и зоонозы, транспортные аварии, аварии с опасными веществами на суше, аварии с загрязнением морской среды, ядерные аварии, террористические акты, акты и кибератаки.

[54] На основе оценки более 60 рисков для всестороннего обсуждения был выбран 21 возможный сценарий событий для Финляндии. Риски подразделяются на два типа: широкомасштабные события, влияющие на общество (6 рисков), и серьезные региональные события (15 рисков). Киберриски обсуждаются более подробно в первой категории, в которой проводится различие между использованием кибердомена для парализации систем, жизненно важных для общества, рисками, связанными с киберпреступностью, и рисками безопасности данных при цифровизации.

[55] «Национальный анализ рисков», проведенный в Норвегии в 2014 году, делит опасности на природные явления, крупные аварии и злонамеренные события, а каждая категория далее делится на зоны риска с соответствующими сценариями. Области риска, которые имеют наибольшие последствия для общества, совпадающие с вышеупомянутыми, – это кризисы политики безопасности, землетрясения, экстремальные погодные условия, ядерные аварии, эпидемии, киберпреступления.

[56] Следующие объекты электронного правительства считаются критической инфраструктурой: веб-сайты правительств на уровне округа или выше; бизнес-системы правительственных департаментов на уровне префектур или выше, которые предоставляют государственные услуги; и другие системы электронного правительства, которые могут нанести серьезный ущерб, если они столкнутся с инцидентами кибербезопасности.

В рамках Закона «О кибербезопасности» предполагается, что «государство принимает меры по мониторингу, предотвращению и устранению рисков и угроз кибербезопасности, возникающих как на материковой территории Китая, так и за ее пределами. Государство защищает критически важную информационную инфраструктуру от атак, вторжений, вмешательства и разрушения. Государство наказывает за незаконную и преступную кибердеятельность в соответствии с законом, сохраняя безопасность и порядок в киберпространстве». Это положение подтверждает право Китая на защиту в киберпространстве и позволяет китайскому правительству отслеживать, защищать от иностранных кибератак и угроз и наказывать за них [938]. Кроме того, предусматривается, что в отношении тех, кто совершает нападения, вторжения, помехи, разрушения или другие действия с целью поставить под угрозу критическую информационную инфраструктуру КНР, будь то организации или отдельные лица, если они вызвали серьезные последствия, китайское правительство должно принять меры, в соответствии с законом, по замораживанию активов или другие необходимые карательные меры. Таким образом, реализуется право на самооборону и обеспечивается правовая основа для наказания за кибератаки.

Закон «О кибербезопасности» также нацелен на безопасность сетевых продуктов и услуг, приобретаемых операторами критически важной информационной инфраструктуры. Сетевые продукты или услуги, получаемые операторами критически важной информационной инфраструктуры, которые могут повлиять на национальную безопасность, требуют прохождения проверки национальной безопасности, организованной государственными органами кибербезопасности и соответствующими департаментами Государственного совета [938].

Закон «О сетевой безопасности Сингапура», принятый в 2018 году, дает определение критически важной информационной инфраструктуры и определяет орган, на который возложена ответственность за сертификацию критической информационной инфраструктуры. Закон «О кибербезопасности» специально предусматривает защиту критически важной информационной инфраструктуры, включающую цифровую инфраструктуру в общественных коммуникациях, информационных службах, энергетике, транспорте, водном хозяйстве, финансах, государственных услугах, электронном правительстве

и других критических отраслях и сферах, или другой информационной инфраструктуре, которая является ключевой национальной безопасности и общественных интересов. Сертификация критически важной цифровой инфраструктуры осуществляются Комиссаром по кибербезопасности.

В России, согласно закону «О безопасности критической информационной инфраструктуры», к которой относятся сети связи госорганов, финансовых, телекоммуникационных, энергетических и ряда других компаний, владельцы данных объектов обязаны предоставлять сведения о кибератаках в Национальный координационный центр по компьютерным инцидентам (НКЦКИ) или в Центробанк, если речь идет о финансовой организации. Взаимодействовать с ФСБ владельцы критической информационной инфраструктуры должны через Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак [943]. В 2021 году Министерство цифрового развития, связи и массовых коммуникаций РФ внесло предложение о переводе объектов критической информационной инфраструктуры[57] на использование преимущественно российского ПО с 1 января 2023 года и российского оборудования – с 1 января 2024 года [944]. Согласно исследованию компании «Информзащита», затраты российского госсектора на информационную безопасность в 2020 году достигли 74,3 млрд российских рублей (рост более чем на 10% по сравнению с 2019 годом). Дальнейший рост будут стимулировать российский Закон «О безопасности критической информационной инфраструктуры» и новые требования Федеральной службы по техническому и экспортному контролю [945].

Следует выделить положительную практику государственно-частного партнерства в различных сферах цифровизации экономики. Так, в сфере регулирования криптовалютной сферы в 2020 году SEC заявила о намерении заключить контракт с компанией CipherTrace для анализа транзакций в Блокчейн. В разрезе обеспечения защиты

[57] К владельцам критической информационной инфраструктуры относятся кредитные организации (банки), госорганы, предприятия ТЭК, транспортные, телекоммуникационные и ряд других компаний, повреждение сетей связи которых может привести к серьезным последствиям. Президент Российского союза промышленников и предпринимателей (РСПП) А. Шохин оценил размер затрат российских промышленных предприятий, банков и IT-компаний из-за требований Минцифры в более чем 1 трлн российских руб. [944].

критически важной инфраструктуры государственно-частное партнерство рассматривается в качестве одной из основных проблем [759]. Быстрое развитие сектора ИКТ, находящегося преимущественно в частной собственности, и зависимость от него других секторов усложняют надзор и регулирование. Это, в сочетании с другими критическими взаимозависимостями инфраструктуры привело к довольно неоднозначной ситуации с точки зрения государственных органов управления, поскольку они могут формально или неформально нести общую ответственность за надежное предоставление услуг, но им не хватает полномочий, ресурсов и профессиональных навыков для эффективного выполнения данной функции. В «Национальной оценке риска» Финляндии эта проблема особо отмечена, в частности, в случае киберугроз. В ней говорится, что критическая инфраструктура в Финляндии в основном принадлежит частному сектору, и компании, как правило, следуют коммерческой логике, «которая создает проблему для готовности к кибербезопасности». Законодательство «не предусматривает единого подхода к киберугрозам, а является отраслевым» [759].

Одним из возможных механизмов стимулирования усиления внимания к киберугрозам и рискам в рамках государственно-частного партнерства является навязывание политики киберстрахования [946]. Так, с 2015 года Lloyds Banking Group ввела отдельный код для киберстрахования. В дополнение к крупным страховым компаниям, которые предоставляют услуги по киберстрахованию, также появляются стартапы InsurTech, которые обеспечивают большую осведомленность о рисках, эффективность и более инновационные продукты [947]. Анализ условий и характеристик, предлагаемых крупнейшими страховыми компаниями мира услуг в области киберстрахования InsurTech, свидетельствует о том, что продукты киберстрахования, как правило, предоставляют три основных типа покрытия: ответственность, возникающая в результате кражи данных, исправления и реагирования на нарушения, а также штрафы, связанные с законодательством и нормативными актами. Покрытие кибервымогательства обеспечивает возмещение затрат на расследование, а иногда и самого запроса на вымогательство в случае соответствующего страхования угрозы кибервымогательства[58].

[58] Кибервымогательство – это акт киберпреступников, требующих оплаты через использование или угрозу какой-либо формы злонамеренной деятельности против жертвы, такой как компрометация данных или атака типа DoS.

Отдельно стоит отметить такую особенность частного производства, как возможность осуществления саморегулирования, поскольку на практике только они имеют доступ к необходимым техническим возможностям и информации, относящейся к большей части критической инфраструктуры.

Кроме того, глобализация вывела частные компании за пределы государственных границ, усложнив возможности государственного контроля. Тот факт, что национальная критическая инфраструктура зависит не только от других секторов, но и от ситуации в других странах, усложняет ситуацию, поскольку ни одна страна не может быть защищена от последствий или не может предсказать результаты, если ее соседи страдают от серьезных нарушений инфраструктуры.

Важно отметить использование подхода саморегулирования предприятий отрасли под координацией специализированных ассоциаций или коммерческих объединений. Саморегулирование может включать использование «мягких» норм посредством применения необязательных кодексов поведения или неформальных руководств. Такие нормы не сопровождаются юридическими санкциями за несоблюдение и вместо этого в большей степени полагаются на репутационные санкции и рыночные стимулы для соблюдения. Саморегулирование не следует рассматривать как замену традиционному регулированию через законодательство и формальные правоприменительные правила, а скорее как дополнение к такой правовой базе. Так, в США в 2007 году в результате объединения подразделений по защите прав потребителей NYSE и Национальной ассоциации дилеров по безопасности (NASD) создана саморегулирующая организация финансовой отрасли (FINRA).

Концепция использования интрументария FinTech для создания комплексной системы государственного надзора и мониторинга в банковской сфере (RegTech) представляет собой следующую логическую эволюцию регулирования финансовых услуг [563]. Для регулирующих органов RegTech обеспечивает непрерывный мониторинг, который повышает эффективность благодаря высвобождению избыточного регулятивного капитала и ускорению поиска компаний, не соответствующих требованиям. Однако RegTech предлагает больше: потенциал непрерывного мониторинга, позволяющий получать информацию, близкую к реальному времени, посредством глубокого обучения и фильтров AI, которые выявляют проблемы заранее.

Цифровизация значительно расширила мониторинговый, надзорный, аналитический и прогнозный инструментарий регуляторов [948]. В США Служба внутренних доходов имеет право собирать значительные массивы личной информации[59]

В Великобритании интеграция инструментария прогнозной аналитики с хранилищами Big Data позволила усилить соответствующие возможности налоговой службы (HMRC). Так, имеющаяся цифровая информация о налогоплательщиках предоставляет возможность анализировать схемы поведения, платежей и денежных потоков отдельных лиц и предприятий[60]. Более того, в 2017 году принят Закон «О цифровой экономике», который регулирует вопросы обмена информацией между государственными органами, разрешает разглашение конфиденциальной информации, позволяя HMRC и другим государственным секторам обмениваться личными данными граждан и юридических лиц для предотвращения мошенничества и взыскания долгов.

Следует отметить, что государственное регулирование, включая финансовое содействие развитию цифровизации, становится основанием для роста двусторонней напряженности по линии США, ЕС, Япония – Китай. КНР обвиняется в постоянном предоставлении несправедливых преимуществ местным компаниям и дискриминации по отношению к иностранным компаниям, принуждении к передаче технологий, игнорировании прав интеллектуальной собственности, ограничении или отказе в доступе к определенным рынкам по соображениям национальной безопасности, спонсировании приобретения иностранных технологий, установлении различных отечественных технологических стандартов, ограничении экспорта редкоземельных элементов и т. д. [73].

---

[59] Например, привычки, увлечения людей, предпочтения чтения (где и как долго взгляд налогоплательщика попадает на определенные экраны), религиозная принадлежность, планы поездок, медицинское обслуживание, вес и рекомендации врача по этому поводу и многие другие.

[60] Инструменты HMRC используют около 30 баз данных, которые содержат не только информацию, агрегированную в правительственных департаментах, но и цифровые интернет-данные, включая активность на площадках Airbnb и Ebay, которые с помощью сложных методов профилирования и моделирования позволяют обнаружить налоговые аномалии. Также анализируется цифровой отпечаток, который люди оставляют при использовании сети Интернет, поисковых запросов в социальных сетях, информации о праздниках и предметах роскоши, которая затем используется для формирования профиля образа жизни лиц, которые находятся под следствием по обвинению в мошенничестве с налогами или пособиями. В рамках механизмов KYC запрашиваются данные у третьих сторон, таких как страховые компании и больницы, или устанавливаются по платежам врачам общей практики и стоматологам.

Заключение

Таким образом, построение авторских моделей экосистем цифровой экономики на примере США, КНР и Российской Федерации позволило выделить основные составлюящие современных механизмов регулирования цифровой экономики, проследить их эволюцию и системность, а также выделить общие тенденции и национальные особенности регуляторных практик. С учетом выявленных отличительных форм управления национальными цифровыми экосистемами и институциональными структурами проведена их классификация в отношении США, КНР и РФ.

Выделены ключевые тенденции, характеризующие формирование современных механизмов регулирования цифровой экономики, среди которых защита персональной информации затрагивает не только субъектов хозяйствования, но и граждан соответствующих стран. В целом отмечено, что проблематика кибербезопасности является важнейшим регуляторным аспектом цифровизации экономики в настоящее время, государства стремятся противодействовать киберугрозам, имплементируя новые стандарты безопасности в ключевых секторах промышленности и усиливая уголовное преследование за совершенные киберпреступления. С этой целью правительства активно используют специальные средства для мониторинга, деанонимизации пользователей, создавая специализированные подразделения. Цифровизация значительно расширила мониторинговый, надзорный, аналитический и прогнозный инструментарий регуляторов.

В области государственного регулирования FinTech финансовые регуляторы сосредоточены, главным образом, на обеспечении стабильности финансовых систем, включая такие компоненты, как финансовая доступность, финансовая целостность и защита финансового потребителя. Разрабатывается новая нормативная среда, которая одновременно поощряет цифровые инновации и выход на рынок новых игроков, устраняя риски целостности и стабильности финансовой системы, а также обеспечивает развитие рыночной конкуренции. В данном контексте следующим этапом эволюции методов регулирования финансовых услуг является концепция RegTech, которая обеспечивает непрерывный мониторинг, повышающий эффективность благодаря высвобождению избыточного регулятивного капитала и ускорению поиска компаний, не соответствующих требованиям.

3.3. Наднациональные механизмы выявления и купирования рисков и угроз для национальной экономической безопасности

Четвертая промышленная революция меняет бизнес-модели, создавая не только общие возможности, но и риски в области экономической безопасности, на которые государства вынуждены реагировать. Международное сотрудничество позволяет решать проблемы цифровизации экономики, обеспечения кибербезопасности более эффективно, используя механизмы обмена информацией, экспертизой, объединяя ресурсы и осуществляя совместные действия для достижения целей и задач экономического развития. Особенностью цифровой экономики является ее глобальный характер, который не позволяет нивелировать риски и угрозы в рамках отдельных юрисдикций без наднационального взаимодействия.

Важнейшее значение приобретают координация и сотрудничество между регулирующими и правоохранительными органами для противодействия угрозам цифровизации в условиях, когда в отдельности ни одна юрисдикция не может самостоятельно гарантировать защищенную киберсреду.

С учетом данного условия следует выделить несколько уровней наднационального регулирования рисков и угроз, связанных с цифровизацией экономики:

1) первый – уровень универсальных международных организаций и инициатив;

2) второй – уровень специализированных международных институтов;

3) третий – уровень интеграционных объединений.

Моделирование основных составляющих стратегий и институциональных блоков формирования современной международной экосистемы цифровой экономики на первом и втором уровнях позволяет сформировать следующую институциональную матрицу (табл. 3.4).

Анализ табл. 3.4 показывает, что первый уровень охватывает, главным образом, организации системы ООН, ориентированные на развитие различных областей цифровой экономики. В 2015 году были утверждены Цели устойчивого развития ООН (ЦУР) [949], которые, встраиваются, по мнению ряда исследователей [321], в концепцию цифровизации экономики и внедрения современных цифровых технологий: AI, Smart City, Блокчейн и прочие в различные

сферы производства. Международная стратегия ООН по уменьшению опасности стихийных бедствий (UNISDR) выводит основные критерии оценки устойчивости критической инфраструктуры к внешним шокам [759][61]. Проблематикой адаптации экономических систем к цифровым вызовам занимаются МВФ и Всемирный банк. МВФ в 2021 году выступил с предложениями о необходимости глобального регулирования криптоактивами и формировании глобальной нормативной базы, включающей такие элементы, как лицензирование поставщиков услуг, связанных с криптоактивами, которые выполняют критически важные функции; адаптация регуляторных требований к основным вариантам использования криптоактивов и стейблкойнов. Официальные органы должны предъявлять четкие требования к регулируемым финансовым организациям в отношении их открытых позиций и операций с криптоактивами [950].

Таблица 3.4

Институциональная матрица международной экосистемы цифровой экономики (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Основной объект регулирования в сфере цифровизации
Первый уровень	СЦ	ООН: Цели устойчивого развития (ЦУР), 2015	Расширение внедрения цифровых технологий в экономику
	ИБЦИ	ООН: Международный союз электросвязи (ITU), 1947	Обеспечение всеобщего доступа к информации и связи
		ООН: Всемирный банк, 1944	Адаптация цифровых возможностей для развития экономики и повышения благосостояния населения
	ИБФР	ООН: МВФ, 1944	Подготовка рекомендаций регуляторам в сфере FinTech в разрезе обеспечения стабильности функционирования национальных и международной финансовых систем
	ИБЗК	ООН: Международная стратегия по уменьшению опасности стихийных бедствий (UN ISDR), 1999	Методология оценки устойчивости критической инфраструктуры к киберугрозам

[61] Устойчивость критической инфраструктуры – это «способность системы, сообщества или общества, подверженного опасности, противостоять, поглощать, приспосабливаться к последствиям опасности и своевременно и эффективно устранять их, в том числе путем сохранения и восстановления его основных структур и функций».

Продолжение табл. 3.4

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Основной объект регулирования в сфере цифровизации
Второй уровень	СЦ	—	—
	ИБЦИ	G20: Глобальный альянс Smart City, 2019	Внедрение концепции Smart City, разработка принципов ответственного и безопасного использования технологий
		Всемирный экономический форум (WEF): соглашение Agile Nations, 2020	Международное сотрудничество в условиях четвертой технологической революции, обмен знаниями и лучшими практиками в сфере цифровизации
	ИБФР	Банк международных расчетов (BIS): Базельский комитет по банковскому надзору, 1974	Разработка единых стандартов и методик регулирования банковской деятельности, включая FinTech
		Международная организация комиссий по ценным бумагам (IOSCO), 1983	Агрегирование лучших практик управления рынками ценных бумаг, включая FinTech
		Группа разработки финансовых мер борьбы с отмыванием денег (FATF), 1989	Разработка стандартов и способствование эффективному применению правовых, нормативных и оперативных мер по борьбе с отмыванием денег, финансированием терроризма, распространением оружия массового уничтожения в условиях расширения использования цифровых активов
		Банк международных расчетов (BIS): Комитет по платежам и рыночной инфраструктуре (CPMI), 1990	Разработка единых стандартов в отношении безопасности и эффективности платежных, клиринговых, расчетных и связанных с ними механизмов
		Альянс за финансовую доступность (AFI), 2008	Расширение внедрения FinTech для развития финансовой доступности, поддержка МСП
		G20: Совет по финансовой стабильности (FSB), 2009	Координация национальных финансовых органов и международных органов, устанавливающих стандарты с учетом развития FinTech
		G20: Глобальное партнерство по финансовой доступности (GPFI), 2010	Развитие финансовой доступности, FinTech в условиях обеспечения стабильности финансовых систем

Окончание табл. 3.4

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Основной объект регулирования в сфере цифровизации
Второй уровень	ИБФР	Глобальная сеть финансовых инноваций (GFIN), 2019	Масштабирование новых технологий FinTech в различных юрисдикциях
		Банк международных расчетов (BIS): Центр инноваций, 2019	Выявление критических тенденций в развитии технологий, влияющих на центральные банковские системы, и разработка соответствующих рекомендаций для центральных банков
	ИБЗК	Международная электротехническая комиссия (IEC), 1906	Разработка международных стандартов в области электрических, электронных и смежных технологий (включая IoT)
		Международная организация по стандартизации (ISO), 1947	Разработка международных стандартов в сфере кибербезопасности
		Институт инженеров электротехники и электроники (IEEE), 1963	Разработка стандартов по радиоэлектронике, электротехнике и аппаратному обеспечению вычислительных систем и сетей (включая IoT)
		Международная ассоциация аудита и контроля информационных систем (ISACA), 1967	Сертификация специалистов в области кибербезопасности
		WEF: «Партнерство для киберустойчивости», 2011	Разработка принципов, направленных на повышение системной устойчивости к киберрискам

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства.

Координация по выработке политики и стратегии стабилизации финансовых систем в условиях цифровых рисков также осуществляется на уровне G20 [915][62]. В 2010 году G20 признала

[62] G20, или Группа двадцати – это международный форум для правительств и управляющих центральных банков из 19 стран и Европейского союза. Основанная в 1999 году с целью обсуждения политики, имеющей отношение к содействию международной финансовой стабильности, G20 с 2008 года расширила свою повестку дня, и главы правительств и государств, а также министры финансов, министры иностранных дел и аналитические центры периодически совещались на саммитах с тех пор. Она направлена на решение вопросов, выходящих за рамки ответственности какой-либо отдельной страны.

финансовую доступность в качестве одного из основных столпов глобальной повестки дня в области развития, одобрила План действий по финансовой доступности и создала Глобальное партнерство по финансовой доступности (GPFI)[63] [914]. В 2016 году GPFI выпустило отчет «Органы, устанавливающие мировые стандарты и финансовая доступность: развивающийся ландшафт», в котором отразило последствия развития FinTech относительно защиты потребителей, развития конкуренции и совместимости (проведение транзакций в разных финансовых сетях); защиты персональных данных; краудфандинга; управления риском. Кроме того, опубликованы «Принципы высокого уровня G20 для цифровой финансовой интеграции», призванные способствовать принятию этих принципов для более широкого охвата планирования финансовой интеграции, в частности цифровой финансовой интеграции [785].

Организацией по разработке политики и регулированию финансовой доступности и FinTech является также Альянс за финансовую доступность (AFI)[64], который согласовал подходы в нормативной отчетности, в частности, в области мобильных платежей для центральных банков и банковских надзорных органов [602][65].

В 2020 году семью государствами[66] в рамках Всемирного экономического форума (WEF) подписано соглашение Agile Nations [951], направленное на расширение международного сотрудничества в сфере развития, в том числе цифровых инноваций в условиях

[63] В организации участвуют такие многосторонние организации, как Всемирный банк и Консультативная группа по оказанию помощи бедным (CGAP), Международный валютный фонд (МВФ) и Организация Объединенных Наций.

[64] Членами организации являются центральные банки и другие финансовые регулирующие учреждения из более чем 90 развивающихся стран. Задача организации – сделать финансовые услуги доступными для самых бедных слоев населения. AFI объединяет, поощряет и позволяет директивным органам наращивать потенциал и разрабатывать политические инициативы в областях финансовых технологий (FinTech), защиты потребителей, микрофинансирования, финансирования МСП, финансирования с учетом гендерных аспектов, инклюзивного зеленого финансирования, микросбережений и других общих инициатив финансовой интеграции в Африке, Азии, Европе, на островах Тихого океана, в Латинской Америке, Карибском бассейне и на Ближнем Востоке. Африканская инициатива по политике в области финансовых услуг для мобильных телефонов (AMPI) является одной из инициатив AFI, которая была создана в 2013 году в качестве платформы для учреждений – членов AFI (главным образом, центральных банков и органов финансового регулирования) (African Mobile Phone Financial Services Policy Initiative (AMPI) 2016: Brochure. – Режим доступа: http://www.afi-global.org/initiatives/african-mobile-phone-financial-services-policy-initiative-ampi. – Дата доступа: 08.08.2016).

[65] Членом AFI является НБРБ.

[66] Канада, Дания, Италия, Япония, Сингапур, ОАЭ и Великобритания.

четвертой технологической революции. Основные направления взаимодействия включают обмен знаниями и лучшей практикой во избежание ненужных расхождений в правилах, которые препятствуют трансграничным инновациям и совместным действиям по устранению общих рисков [952].

Регулирующие органы в разных регионах мира находят новые способы сотрудничества в управлении цифровизацией. Многие органы финансового регулирования заключили двусторонние соглашения о сотрудничестве в области регулирования («мосты взаимодействия») для облегчения совместной работы над инновациями [896][67].

В 2019 году создан Глобальный альянс умных городов G20 по управлению технологиями, который объединяет муниципальные, региональные и национальные правительства, партнеров из частного сектора вокруг общего набора принципов ответственного и этичного использования технологий умных городов. Альянс устанавливает и продвигает международные нормы, чтобы помочь ускорить внедрение передовых практик, снизить потенциальные риски и способствовать большей открытости и общественному доверию. Функции секретариата Альянса выполняет Всемирный экономический форум [953].

Уровень специализированных международных институтов представлен в первую очередь Группой разработки финансовых мер борьбы с отмыванием денег (FATF)[68]. В рамках разработки

[67] Например, Валютное управление Сингапура с 2016 года заключило 33 соглашения о сотрудничестве, охватывающие такие виды деятельности, как обмен прогнозами, практикой и поддержкой, направленные на содействие новационным регуляторам ориентироваться в правилах в юрисдикции друг друга.

[68] Группа разработки финансовых мер борьбы с отмыванием денег (FATF) – межправительственная организация, основанная в 1989 году по инициативе «Большой семерки» министрами стран-участниц с целью установить стандарты и способствовать эффективному применению правовых, нормативных и оперативных мер по борьбе с отмыванием денег, финансированием терроризма, распространением оружия массового уничтожения и другими соответствующими угрозами целостности международной финансовой системы. Как орган, устанавливающий стандарты и определяющий политику, FATF работает над созданием технического понимания и необходимой политической воли для проведения национальных законодательных и регулирующих реформ, которые должны быть максимально согласованы между юрисдикциями. FATF рассматривает методы и меры борьбы с отмыванием денег и финансированием терроризма; предоставляет форум для обмена передовым опытом; выделяет области, вызывающие общую озабоченность; продвигает и отслеживает прогресс своих членов в принятии и реализации мер регулирования во всем мире. В сотрудничестве с другими международными заинтересованными сторонами, FATF также работает над выявлением уязвимостей на национальном уровне в рамках процесса экспертной оценки с целью защиты международной финансовой системы от неправомерного использования, а также над созданием стандартов для передовой национальной практики.

рекомендаций по выявлению и купированию рисков для национальной безопасности стран-членов, данная организация осуществляет анализ современных тенденций, в том числе в области цифровизации экономики в целом и финансовых систем в частности. На основе обмена опытом стран-участниц по выявлению и купированию рисков, связанных с внедрением технологий Блокчейн, использованием криптовалют для осуществления противозаконных действий, направленных, в первую очередь, на отмывание денег и финансирование терроризма (ПОД/ФТ). Таким образом, данный институт является ключевым в международном регулирующем пространстве в области разработки стандартов ПОД/ФТ.

FATF разработала серию «Рекомендаций», которые признаны международными стандартами по борьбе с отмыванием денег, финансированием терроризма и распространением оружия массового уничтожения. Это обеспечивает основу для скоординированных международных ответных действий, направленных на противодействие этим угрозам целостности мировой финансовой системы [924]. В 2015 году FATF выпустила глобальное руководство как часть поэтапного подхода к устранению рисков отмывания денег и финансирования терроризма, связанных с продуктами и услугами для оплаты виртуальных активов.

В 2018 году FATF опубликовала отчет, в котором изложены обязательства FATF по борьбе с незаконным финансированием с использованием виртуальных активов[69]. В 2019 году FATF приняла Пояснительную записку к Рекомендациям, которая дополнительно разъясняет и расширяет поправки FATF к стандартам, касающимся виртуальных активов, и описывает, как страны и финансовые организации должны соблюдать соответствующие Рекомендации по предотвращению неправомерного использования виртуальных активов для отмывания денег, финансирования терроризма и распространения оружия массового поражения. Предложен рискориентированный подход к виртуальным активам, а также рекомендации по применению спектра превентивных мер по противодействию отмыванию денег и финансированию терроризма (ПОД/ФТ), включая

[69] В Рекомендациях, касающихся новых технологий, отмечается, что для управления и снижения рисков, связанных с виртуальными активами, странам следует обеспечить, чтобы поставщики услуг виртуальных активов регулировались в целях ПОД / ФТ, были лицензированы или зарегистрированы и подпадали под действие эффективных систем мониторинга и обеспечения соблюдения соответствующих мер, предусмотренных в Рекомендации FATF.

надлежащую проверку клиентов, ведение документации, отчетность о подозрительных транзакциях и проверку транзакций на соответствие целевым финансовым санкциям.

Фокусом мониторинга FATF также являются элементы цифровой инфраструктуры, включая криптобиржи. Так, в рамках борьбы с криминальным применением цифровых валют в отчете организации в 2020 году рекомендовано обязать биржи сформировать базы данных трейдеров [954], а также детально идентифицировать держателей криптовалюты (KYC)[70]. Более того, FATF рекомендовала регуляторам и биржам создавать профили криптовалютных пользователей для выявления преступной деятельности. При этом отмечены специфические модели поведения и характеристики криптовалютных пользователей, которые являются подозрительными[71] [955]. FATF также рекомендует регуляторам следить за пользователями, которые обменивают криптоактивы общедоступных и прозрачных Блокчейн на конфиденциальные криптовалюты, например, Monero или Zcash [956]. В 2021 году опубликован доклад с рекомендациями регуляторам по мониторингу цифровых активов и введению

[70] KYC относится к процессу проверки личности клиента, включает проверку личности физического или юридического лица на основании официальных документов. KYC является частью процесса регистрации клиентов. На втором этапе деятельность KYC включает проверку транзакций и отслеживание денежных средств, а также агрегирование информации о «клиентах вашего клиента» (know your customer's customer KYCC). Другим аспектом KYC является определение пригодности клиента для торговли определенными продуктами. Банки обязаны заботиться о своих клиентах и убедиться, что их клиенты обладают достаточной квалификацией при приобретении определенных финансовых продуктов или услуг. На практике эти продукты могут быть предложены только после анализа клиента. Требования KYC различаются в зависимости от юрисдикции, но общая тенденция заключается в более тщательном изучении регистрации клиентов и отслеживании дополнительной информации и документации по счетам [957].

[71] Один из основных методов, предложенных в отчете, – это сравнение активности транзакций пользователя с аналогичным показателем в его профиле. Сюда могут входить случаи, когда сумма депозита или транзакции несовместима с финансовым положением пользователя или исторической финансовой активностью, что может свидетельствовать об отмывании денег или мошенничестве. Например, может быть подозрительно, если молодой пользователь, не имеющий известных деловых интересов, начал получать крупные суммы от разных людей по всему миру. Другие подозрительные признаки включают наличие у пользователя судимости или активности на веб-сайтах и форумах, связанных с незаконной деятельностью, отправку криптовалют на биржи без проверок ПОД/ФТ или отправку транзакций, размер которых чуть ниже суммы, подлежащей проверке регуляторами по более ранним рекомендациям FATF.

соответствующих стандартов в отношении виртуальных активов и их поставщиков[72] [958].

Надзор за деятельностью банков, разработка методологий оценки платежеспособности, установление стандартов банковского регулирования на глобальном уровне осуществляются через Базельский комитет по банковскому надзору Банка международных расчетов [915][73]. Комитет по платежам и рыночной инфраструктуре (CPMI)[74] Банка международных расчетов (BIS) совместно с Международной организацией комиссий по ценным бумагам (IOSCO)[75] представил в 2021 году Принципы инфраструктуры финансового рынка (PFMI)[76] в отношении международного стандарта для платежей, клиринговых и расчетных систем, а также Руководство по соответствию механизмов стейблкоинов международным стандартам. Данные принципы применяются ко всем системно значимым платежным системам, центральным депозитариям ценных бумаг, системам расчетов по ценным бумагам, центральным контрагентам и торговым репозиториям. В дополнение к этим стандартам

---

[72] Поставщиком услуг виртуальных активов (Virtual Asset Service Provider – VASP) охватывается широкий круг физических и юридических лиц, выступающих в качестве финансовых посредников VASP. Это могут быть криптобиржи, поставщики кошельков, поставщики финансовых услуг в связи с выпуском, предложением и продажей виртуальных активов и другие возможные бизнес-модели.

[73] Для пруденциального регулирования Базельская система решает вопросы арбитража на мировом рынке, возлагая глобальный надзор за многонациональными банками на страны, где они находятся [380].

[74] Это международная организация, которая устанавливает стандарты, продвигает, контролирует и дает рекомендации относительно безопасности и эффективности платежных, клиринговых, расчетных и связанных с ними механизмов, тем самым поддерживая финансовую стабильность и экономику в целом. CPMI также служит форумом для сотрудничества центральных банков в соответствующих вопросах надзора, политики и операционных вопросов, включая предоставление услуг центрального банка.

[75] Международная организация комиссий по ценным бумагам (IOSCO) осуществляет агрегирование лучших практик управления рынками ценных бумаг с 1983 года. Мандат IOSCO заключается в том, чтобы выступать в качестве международного органа, объединяющего мировых регуляторов ценных бумаг. Это стандартная система мирового уровня для сектора ценных бумаг. Членство в IOSCO отвечает за регулирование более 95% мировых рынков ценных бумаг в более чем 115 юрисдикциях.

[76] Изданные PFMI являются частью набора из 12 ключевых стандартов, которые международное сообщество считает необходимыми для укрепления и сохранения финансовой стабильности (Principles for Financial Market Infrastructures (PFMI). – Режим доступа: https://www.bis.org/cpmi/info_pfmi.htm. – Дата доступа. 08.02.2020).

CPMI и IOSCO опубликовали ряд связанных документов и дальнейшее руководство по внедрению стандартов[77].

IOSCO взаимодействует с G20 и Советом по финансовой стабильности (FSB)[78] в рамках глобальной программы реформ регулирования [665]. FSB, объединяющий центральные банки и финансовые регуляторы из G20 совместно с МВФ, Всемирным банком, Банком международных расчетов, подготовил в 2020 году проект рекомендаций в отношении влияния стейблкоинов на эффективность трансграничных розничных платежей [719]. В рамках своей координирующей роли FSB должен разработать основу, включающую стандарты для регулирования криптоактивов, целью которой должно стать обеспечение комплексного и согласованного подхода к управлению рисками для финансовой стабильности и поведению на рынке, который может последовательно применяться в различных юрисдикциях, и при этом сведение к минимуму возможностей для регулятивного арбитража или переноса деятельности в юрисдикции с менее строгими требованиями. Кроме того, Базельский комитет BIS дорабатывает документ с требваниями к банковской системе в отношении резервного капитала банков, которые используют критовалюты[79].

---

[77] Включает восстановление инфраструктуры финансового рынка (ИФР): предоставляет соответствующее руководство о методологии разработки планов, позволяющих восстанавливаться после угроз стабильности функционирования и финансовой устойчивости. Дальнейшее руководство по PFMI направлено на повышение устойчивости путем предоставления рекомендаций по принципам и ключевым соображениям в PFMI в отношении управления финансовыми рисками. Руководство по киберустойчивости для инфраструктур финансового рынка содержит руководство по подготовке и мерам, которые ИФР должны предпринять для повышения своих возможностей киберустойчивости, чтобы ограничить нарастающие риски, которые киберугрозы представляют для финансовой стабильности. Применение принципов для инфраструктур финансового рынка к ИФР центральных банков заключается в предоставлении руководства по применению ИФР к инфраструктурам финансового рынка, которые принадлежат центральным банкам и управляются ими.

[78] Основной целью организации является выявление слабых мест в области мировой финансовой стабильности, разработка и применение регулирующей и надзорной политики в этой сфере. В частности, одним из направлений деятельности FSB стало составление и регулярное обновление списков системообразующих банков и страховых компаний, к которым предъявляются повышенные требования устойчивости и надежности, а также применяются усиленные меры надзора за их деятельностью.

[79] Обновленный регламент будет выпущен к середине 2022 года (Базельский комитет доработает руководство для банков по работе с криптовалютами. – Режим доступа: https://plusworld.ru/daily/cat-kriptovalyuty/bazelskij-komitet-dorabotaet-rukovodstvo-dlya-bankov-po-rabote-s-kriptovalyutami/. – Дата доступа: 10.11.2021).

Проблематика регулирования криптоактивов находится в повестке дня Большой семерки (G7) на уровне министров финансов, управляющих центральными банками, с участием Европейской комиссии, руководителей МВФ, Всемирного банка и Совета по финансовой стабильности [959]. На саммите G20 в 2021 году была принята декларация [960], в которой страны-участницы поддержали предложение ОЭСР по введению минимального глобального налога для транснациональных корпораций на уровне 15%. Кроме того, отмечена значимость политики, направленной на создание раскрывающей потенциал, инклюзивной, открытой, поддерживающей честную конкуренцию цифровой экономики, которая способствует применению новых технологий, позволяет бизнесу и предпринимателям процветать, защищает и дает права потребителям. Отмечена приверженность ведущих промышленных государств международному сотрудничеству, направленному на цифровую трансформацию производства, процессов, услуг и бизнес-моделей, в том числе с помощью основанных на консенсусе международных стандартов и совершенствования защиты потребителей, развития цифровых навыков и грамотности. Выражена необходимость решения возросших проблем безопасности в цифровой среде, в том числе от программ-вымогателей и других форм киберпреступности, а также готовность укрепления двустороннего и многостороннего сотрудничества для защиты национальных ИКТ, устранения общих уязвимостей и угроз и борьбы с киберпреступностью. По результатам встречи G20 руководители государств призвали CPMI, Центр инноваций BIS, МВФ и Всемирный банк продолжить углубление анализа потенциальной роли CBDC в расширении трансграничных платежей и их более широких последствий для международной валютной системы. МВФ разработана операционная стратегия по дальнейшему выполнению мандата с учетом роста государственных и частных цифровых денег [961].

В 2019 году 29 регулирующих органов создали Глобальную сеть финансовых инноваций (GFIN). Среди прочего, сеть тестирует среду, которая позволит одновременно испытывать и масштабировать новые технологии в нескольких юрисдикциях [896][80].

[80] GFIN – это сеть из 50 организаций, активно настроенных на поддержание финансовых инноваций в интересах потребителей. GFIN старается обеспечить более эффективный способ для инновационных фирм с целью взаимодействия с регуляторами, помогая им лавировать между странами, поскольку они имеют склонность

Важным направлением международного регулирования цифровизации является разработка и внедрение стандартов. Международная электротехническая комиссия (IEC) на международном уровне разрабатывает стандартизированные решения и практики для обеспечения методологии систематической оценки безопасности компонентов цифровых систем, чтобы гарантировать их надежную и безопасную работу [814][81]. Рабочая группа Сектора стандартизации электросвязи Международного союза электросвязи (ITU) разрабатывает стандарты «умного города», каждый из которых ориентирован на различные аспекты его инфраструктуры, такие как архитектура, совместное использование данных и безопасность. Аналогичным образом рабочая группа Института инженеров электротехники и электроники (IEEE) создала группу интеллектуальных городов [175][82]. Группа технологических и финансовых компаний объявила в 2017 году о работе над стандартом для защиты приложений IoT с помощью Блокчейна [962][83]. На уровне платежной отрасли в 2009 году установлены стандарты безопасности индустрии платежных карт (PCI DSS)[84], рекомендованные организациям,

---

взвешивать новые идеи. Сюда относится пилотный проект для фирм, желающих протестировать инновационные продукты, услуги или бизнес-модели на территории более чем одной юрисдикции. Она также направлена на создание новой базы для сотрудничества между регуляторами финансовых услуг по темам, связанным с инновациями, делясь различным опытом и подходами (Глобальная сеть финансовых инноваций (GFIN). – Режим доступа: https://afsa.aifc.kz/ru/global-financial-innovation-network-gfin/. – Дата доступа: 08.02.2021).

[81] Например, IEC 62351 является отраслевым стандартом, направленным на повышение безопасности в системах автоматизации в области энергосистем. Он содержит положения, обеспечивающие целостность, подлинность и конфиденциальность для различных протоколов, используемых в энергосистемах. В частности, IEC 62351 касается безопасности в системах и протоколах, которые преимущественно используются в системах автоматизации в области распределения электроэнергии.

[82] В настоящее время они разрабатывают «Стандарт P4213.1 для эталонной архитектуры умного города (RASC)». Другие группы, разрабатывающее IoT-архитектуры и цифровые стандарты, включают рабочие группы IEEE P4213, IEEE P4213.1, техническую консультативную группу IEEE 802.24 (TAG).

[83] Компании, входящие в группу, включают Cisco, производителя приложений Bosch, Bank of New York Mellon Corp., Foxconn Technology, CS-компанию Gemalto и стартапы Блокчейн Consensus Systems, BitSE и Chronicled. Целью группы было создание протокола цепочки блоков в качестве общей платформы для разработки устройств, приложений и сетей IoT.

[84] Payment Card Industry Security Standards Council, PCI SSC, учрежденным международными платежными системами Visa, MasterCard, American Express, JCB и Discover. Стандарт представляет собой совокупность 12 детализированных требований

которые хранят, обрабатывают или передают финансовые данные карт [877]. В 2019 году Международная организация по стандартизации (ISO) выпустила руководящие принципы, призванные помочь предприятиям соблюдать правила конфиденциальности и защиты данных в различных юрисдикциях [583].

На третьем уровне наднационального регулирования следует выделить регулирование в рамках цифровой экономики в рамках ЕС [192].

Экстраполяция основных составляющих стратегий и институциональных блоков формирования современной экосистемы цифровой экономики на примере Европейского союза как региона с наиболее развитой институциональной средой позволяет сформировать институциональную матрицу современной экосистемы цифровой экономики (табл. 3.5).

Таблица 3.5

Институциональная матрица экосистемы цифровой экономики на уровне стратегических программ ЕС (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2000–2009 годы)	СЦ	—	—	—
	ИБЦИ	Директива об электронной торговле, 2000	ЕК	E-Commerce; электронные договора
	ИБФР	—	—	—
	ИБЗК	Конвенция о киберпреступности (Будапештская), 2001	СЕ	Противодействие киберпреступлениям
		Европейская программа защиты критической инфраструктуры (EPCIP), 2004	ЕК	Защита критической инфраструктуры
		Европейская сеть предупреждений о критической инфраструктуре (CIWIN), 2004	ЕК	Защита критической инфраструктуры

по обеспечению безопасности данных о держателях платежных карт, которые передаются, хранятся и обрабатываются в информационных инфраструктурах организаций. Для обеспечения соответствия PCI DSS Стандарты требуют непрерывного трехэтапного процесса и предоставляют Независимых квалифицированных оценщиков безопасности для мониторинга и проверки соответствия. Несмотря на то, что PCI DSS устанавливает всеобъемлющие отраслевые стандарты, каждый крупный бренд платежных карт поддерживает свою собственную программу соответствия.

Продолжение табл. 3.5

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2000–2009 годы)	ИБЗК	Агентство Европейского союза по кибербезопасности (ENISA), 2004	ЕК	Сертификации кибербезопасности продуктов, услуг и процессов ИКТ
		Европейский надзорный орган по защите данных (EDPS), 2004	ЕК	Обеспечение соблюдения европейскими учреждениями и органами права на конфиденциальность и защиту данных при обработке персональных данных и разработке новых политик
		Рамочное решение Совета о нападениях на информационные системы (2005/222/JHA), 2005	СЕ	Международное сотрудничество в области уголовного правосудия в отношении киберпреступлений
		Директива по EPCIP по идентификации и обозначению европейской критической инфраструктуры и оценке необходимости улучшения ее защиты (2008/114/EC), 2008	СЕ	Защита критической инфраструктуры
Первый уровень (2010–2014 годы)	СЦ	Europe 2020, 2010	ЕК	Цифровая инфраструктура; единый цифровой рынок
		Horizon 2020, 2011	ЕК, EIC, Евратом, EIT	Исследования и разработки цифровых технологий, цифровой инфраструктуры; цифровые промышленные технологии; энергетика; автономный транспорт
	ИБЦИ	—	—	—
	ИБФР	Регламент инфраструктуры рынка (EMIR), 2012	ЕП, СЕ, ЕК, ESMA	FinTech
		Директива о рынках финансовых инструментов (MiFID II), 2014	ЕП, СЕ, ЕК, ESMA	FinTech
		Регламент о рынках в финансовых инструментах (MiFIR), 2014	ЕП, СЕ, ЕК, ESMA	FinTech

Продолжение табл. 3.5

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2010–2014 годы)	ИБЗК	Стратегия кибербезопасности ЕС. Коммюнике ЕС об устойчивости, сдерживании и защите, 2013	ЕК	Защита цифровой безопасности граждан, продуктов и услуг
		Европейский центр киберпреступности при Европоле (EC3), 2013	ЕК	Международное сотрудничество в области уголовного правосудия в отношении киберпреступлений
		Совместная целевая группа по борьбе с киберпреступностью (J-CAT), 2014	ЕК	Противодействие киберпреступлениям
Второй уровень (2015–2019 годы)	СЦ	Единый цифровой рынок, 2015	ЕК	E-Commerce, НДС, авторские права, телекоммуникации, онлайн-платформы, кибербезопасность и защита персональных данных; экономика данных; стандарты; цифровые навыки
	ИБЦИ	Инициатива «Гигабитное общество», 2016. Европейский кодекс электронных коммуникаций	BEREC, ЕК	Телекоммуникации
		Инициатива по цифровизации европейской промышленности (DEI), 2016	ЕК	Промышленность
		Коммюнике Европейской комиссии о платформах (COM (2016) 288/2), 2016	ЕК	Платформизация
		Стратегия внедрения облачных технологий (ECDS), 2019	ЕК	Облачные технологии
	ИБФР	Руководство по комиссиям за обмен по платежным картам (MIF), 2015	ЕП, EBA, CE,	Трансграничные платежи
		Регулирование операций с финансированием ценных бумаг (SFTR), 2015	ЕП, CE, ЕК, ESMA	Рынок ценных бумаг
		Директива о злоупотреблении рынком (MAD), 2015	ЕП, CE, ЕК, ESMA	Рынок ценных бумаг
		Вторая Директива ЕС о платежных услугах (PSD2), 2018	ЕП, CE, ЕК, EBA	FinTech
		Рекомендации по первичным предложениям монет (ICO) и криптоактивам (RTS, ITS), 2019	ESMA	Криптоактивы

Продолжение табл. 3.5

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2015–2019 годы)	ИБЗК	Европейская организация кибербезопасности (ECSO), 2016	ЕК	Оказание содействия в условиях кибератак
		Директива о безопасности сетевых и информационных систем ЕС (NIS), 2016	ЕК, ЕП, СЕ	Защита критической инфраструктуры
		Коммюнике «Прокладывая путь к эффективному и подлинному Союзу безопасности», концепция Союза безопасности ЕС (Security Union), 2016	ЕК	Комплексная киберзащита
		Общий регламент о защите данных (GDPR), 2018	ЕК, ЕП, СЕ, EDPS	Защита персональных данных
		Европейский совет по защите данных (EDPB), 2018		
		Акт о кибербезопасности, 2019	ENISA, ЕК,	Предоставляет агентству ENISA постоянный мандат, поддерживает координацию ЕС в случае крупномасштабных трансграничных кибератак и кризисов.
Третий уровень (2020 – н. в.)	СЦ	–	–	–
	ИБЦИ	Проект регуляторной политики в области AI, 2021	ЕК	Искусственный интеллект
	ИБФР	Новая система электронных платежей (PISA), 2021	ЕСВ	Новый алгоритм надзора за компаниями, эмитирующими и поддерживающими платежные карты, использующими электронные деньги, выдающими кредиты, а также хранящими на своих серверах цифровые токены и электронные кошельки. Создан отдельный канал для транзакций с использованием криптоактивов
	ИБЗК	Стратегия Союза безопасности ЕС, 2020	ЕК	Устранение цифровых и физических рисков комплексным образом во всей экосистеме Союза безопасности

Окончание табл. 3.5

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Третий уровень (2020 – н. в.)	ИБЗК	Директива о безопасности сетевых и информационных систем ЕС (NIS2), 2020	ЕП, СЕ,	Усиление защиты критической инфраструктуры
		Проект создания нового европейского центра компетенций в области промышленной, технологической и исследовательской кибербезопасности и сети национальных координационных центров, в стадии согласования	ЕК	Противодействие киберпреступлениям

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства; ЕК – Европейская комиссия; СЕ – Совет Европы; ЕП – Европейский парламент; EIC – Расширенный Европейский инновационный совет; EIT – Европейский институт инноваций и технологий; BEREC – Орган европейских коммуникационных регуляторов; ESMA – Европейское управление по ценным бумагам и рынкам; EBA – Европейское банковское управление; EDPS – Европейский надзорный орган по защите данных; ECB – Европейский центральный банк

Как показывают данные табл. 3.5, для базового уровня становления цифровой экосистемы ЕС характерны общее стратегическое направление (программа) цифровизации, формируемые институты отдельных цифровых инноваций и концепций, фокусное внимание на противодействие рискам и угрозам, связанным с цифровыми технологиями. Финансовый институциональный блок на данном этапе представлен нишевыми технологиями и не входит в сферу государственного регулирования цифровизации. Для первого уровня формирования институциональной экосистемы ЕС характерно широкое видение направлений развития цифровизации, что выражается в стимулировании развертывания цифровых решений для различных секторов экономики, создание соответствующей инфраструктуры. Институциональный блок цифровых технологий в приоритетах регуляторов уступает место институциональному финансовому блоку с учетом высокой динамики развития рынка криптовалют и в целом FinTech. Блок цифровой безопасности получил

новые организационные институты, призванные предотвратить риски, связанные с киберпреступлениями и усилить международное сотрудничество с учетом их транснационального характера. Второй уровень развития цифровой экосистемы ЕС характеризуется конвергенцией, синергией различных цифровых концепций, их взаимным влиянием, которое накладывает дополнительные требования к комплексному развитию цифровых решений как на технологическом, экономическом, так и социальном уровне. Третий (современный) уровень развития институциональной экосистемы ЕС – общая стратегия цифровизации, находящаяся в стадии формирования. Очевидна определяющая роль киберзащиты в дальнейшей цифровизации различных отраслей и сегментов экономики, социальной сферы и государственных институтов.

Следует отметить, что Европейская комиссия изначально выдвинула ряд политических инициатив по продвижению цифрового сектора, в частности Цифровую повестку дня для Европы, Единый цифровой рынок[85] и Гигабитное общество. В 2000 году ЕС принята Директива об электронной торговле [963], в которой, в том числе, государствам-членам разрешено признание договоров, заключаемых в электронной форме. Стратегии единого цифрового рынка включали ряд инициатив в области цифровых технологий, в том числе инициативу по оцифровке европейской промышленности (DEI) в 2016 году [192]. В 2019 году ЕС подготовил стратегию внедрения облачных технологий до 2022 года (ECDS) «Облако как инструмент цифровой стратегии Европейской комиссии», в которой определены ключевые риски безопасности в условиях внедрения облачных технологий как в государственном, так и частном секторах [964][86].

[85] В рамках Стратегии единого цифрового рынка (Strategy for the Single Digital Market) Европейская комиссия работает над выявлением и сбором данных, позволяющих измерять и характеризовать цифровое общество, включая данные, связанные с оцифровкой производственных процессов [967].

[86] Европейская комиссия продвигает облачные вычисления как для компаний, так и для государственных администраций с момента принятия первой Европейской стратегии облачных вычислений в 2012 году. В соответствии с европейской политикой облачных вычислений в отношении государственных органов, DIGIT стала пионером в экспериментах с облачными вычислениями учреждениями и агентствами ЕС и обобщила полученный опыт в исчерпывающий список извлеченных уроков. Государственные и частные инвестиции, необходимые для реализации Европейской облачной инициативы, оцениваются в 6,7 млрд евро. По оценкам Комиссии, в целом 2 млрд евро из финансирования Horizon 2020 будут выделены на инициативу European Cloud. Оценка требуемых дополнительных государственных и частных инвестиций составляет 4,7 млрд евро в течение 5 лет (The European Cloud Initiative. – Режим доступа: https://ec.europa.eu/digital-single-market/en/european-cloud-initiative. – Дата доступа: 09.02.2021).

Европейская комиссия выступает за разработку открытых стандартов, которые повышают конкуренцию, функциональную совместимость и упрощают обмен данными и доступ к ним между участниками рынка. Коммюнике Европейской комиссии 2016 года (COM (2016) 288/2) о платформах вводит четыре руководящих принципа, которые призваны служить основой дальнейшего регулирования: 1) создание равных условий для сопоставимых цифровых услуг; 2) ответственное поведение онлайн-платформ для защиты основных ценностей; 3) прозрачность и справедливость для поддержания доверия пользователей и защиты инноваций; 4) открытость и отсутствие дискриминации на рынке в экономике, основанной на данных [965].

В ЕС в 2021 году разработан проект регуляторной политики в области AI, который предполагает диверсификацию системы AI на три категории: системы AI с неприемлемым риском, системы AI с высоким уровнем риска и системы AI с ограниченным и минимальным риском[87][966]. Системы, относящиеся к категории неприемлемого риска, в дальнейшем в Европейском Союзе будут запрещены. Системы AI с высоким уровнем риска будут подчиняться самому большому набору требований, включая надзор, прозрачность, кибербезопасность, управление рисками, качество данных, мониторинг и обязательства по отчетности. Правоприменение включает штрафы в размере до 30 млн евро, или 6% от общего дохода[88].

Европейское управление по ценным бумагам и рынкам (ESMA) осуществляет функцию по защите инвесторов, проверке упорядоченных рынков и обеспечению финансовой стабильности [665]. В 2019 году регулятор подготовил рекомендации по первичному предложению монет (ICO) и криптоактивам (в документе отмечен ряд проблем и пробелов в существующей нормативно-правовой базе ЕС) и дал указания директивным органам ЕС, как можно

[87] Организациям предложено использовать классификацию при разработке собственной системы оценки рисков. Важно отметить, что фокусом внимания нормативной базы управления рисками являются исключительно общественные риски, а не более широкий перечень рисков AI для коммерческих организаций.

[88] Применение запрещенных систем и нарушение положений об управлении данными при использовании систем с высоким уровнем риска повлечет за собой самые большие потенциальные штрафы. За все другие нарушения взимается меньший максимум в размере 20 млн евро, или 4% от глобального дохода, а предоставление властям неверной или вводящей в заблуждение информации влечет за собой максимальный штраф в размере 10 млн евро, или 2% от глобального дохода.

разработать нормативно-правовую базу для использования криптоактивов и защиты инвесторов (RTS, ITS) [968].

С акцентом на основной принцип повышения прозрачности и требований к отчетности с целью недопущения подрыва финансовой стабильности в ЕС приняты следующие регуляторные механизмы в отношении современных цифровых финансовых инструментов: Регламент инфраструктуры рынка (EMIR), 2012 год[89], Директивы о рынках финансовых инструментов I, II (MiFID)[90] и Регламент о

[89] Регламент европейской рыночной инфраструктуры (European Market Infrastructure Regulation EMIR) [сокращение от Регламента (ЕС) № 648/2012 Европейского парламента и Совета от 4 июля 2012 года о внебиржевых деривативах, центральных контрагентах и торговых репозиториях, вступивших в силу 16 августа 2012 года]. Ключевым требованием является повышение прозрачности внебиржевого рынка деривативов. EMIR устанавливает новые нормативные требования ко всем типам и размерам организаций, которые заключают производные контракты в любой форме. Новые нормативные требования разделены на три основные категории: отчетность о транзакциях, клиринг и снижение рисков.

[90] Директива о рынках финансовых инструментов (Markets in Financial Instruments Directive MiFID II) с некоторыми из ее основных целей, в том числе с целью перемещения торговли стандартизированными деривативами на биржи или другие организованные торговые площадки в рамках этих площадок (OTF) для охвата небольших сетей брокеров. Кроме того, он призван значительно повысить прозрачность до и после торговли и отчетность по транзакциям. Особое внимание уделяется товарной и высокочастотной торговле, включая ограничение потенциальных позиций или принудительное сокращение позиций [948]. MTF – утвержденная торговая площадка, управляемая инвестиционной фирмой или оператором рынка, и она добавит юридической силы любой криптовалютной бирже, учитывая отсутствие нормативной ясности в отношении торговли цифровыми активами. В тех случаях, когда криптоактивы квалифицируются как финансовые инструменты, ряд операций, связанных с криптоактивами, может квалифицироваться как инвестиционные услуги (действия), такие как размещение, торговля за собственный счет, управление MTF или OTF или предоставление консультаций по инвестициям. В этом случае будут применяться организационные требования, правила ведения бизнеса, а также требования к прозрачности и отчетности, изложенные в MiFID II, в зависимости в некоторых случаях от типа предлагаемых услуг и типа задействованных финансовых инструментов. Предварительное мнение ESMA заключается в том, что там, где криптоактивы квалифицируются как финансовые инструменты, платформы, торгующие криптоактивами с центральной книгой заказов и (или) совпадающими заказами в соответствии с другими торговыми моделями, скорее всего, будут квалифицироваться как многосторонние системы и, следовательно, должны работать как регулируемые рынки (RM), или многосторонние торговые площадки (MTF), или организованные торговые площадки (OTF) (Are platforms trading crypto-assets subject to MiFID II/MiFIR? – Режим доступа: https://www.newrealityblog.com/2019/01/22/are-platforms-trading-crypto-assets-subject-to-mifid-ii-mifir/. – Дата доступа: 24.04.2021).

рынках в финансовых инструментах (MiFIR)[91], 2014 год, Руководство по комиссиям за обмен по платежным картам (MIF), 2015 год, Регулирование операций с финансированием ценных бумаг (SFTR), 2015 год и Статистическая отчетность о денежном рынке (MMSR), 2015 год, Директива о злоупотреблении рынком (MAD)[92], Положение о целостности и прозрачности оптовых энергетических рынков (REMIT)[93].

Вторая Директива ЕС о платежных (PSD2) услугах введена в 2018 году и направлена на значительное снижение барьеров для входа на финансовый рынок, усиление конкуренции. Данный нормативный акт нацелен на реализацию концепции открытого банкинга и регулирует новые платежные платформы, устанавливая

[91] В соответствии с MiFIR требования к отчетности по транзакциям значительно возросли в уровне детализации, и качество этой информации также повысилось. Более того, требования к отчетности значительно расширены и потребуют значительных изменений в бизнес-процессах и технологических системах.

[92] Охватывает раскрытие интересов, отчетность о подозрительных операциях, ведение списков инсайдеров и принятую рыночную практику. В настоящее время он расширен и включает производные и товары с дополнительными функциями, относящимися к санкциям в отношении данных и действиям HFT. Может влиять на MTF и OFT, а также на OTC. MiFID требовала, чтобы фирмы классифицировали клиентов в зависимости от уровня их защиты в отношении продуктов, с которыми они могут столкнуться на рынках; они должны быть в одном из трех типов: приемлемые контрагенты, профессиональные клиенты и розничные клиенты. MiFID ввел требования к указанной информации, которые должны регистрироваться при принятии заказов клиента. Это было целью концепции наилучшей практики исполнения для защиты клиентов, когда речь идет о приоритизации и агрегировании заказов. Новые требования к отчетности существенно повлияли на внебиржевые рынки деривативов, поскольку приемлемые внебиржевые деривативные контракты внезапно стали предметом торговли через место проведения электронных торгов, оформлены через ЦКА и стали предметом требований по отчетности по операциям. Основные цели регулирования MiFID II направлены на снижение системного риска и дальнейшую максимальную прозрачность на рынках, а также на обеспечение надежных уровней защиты инвесторов. Основное внимание MiFID II уделяется внебиржевым рынкам, для которых будут введены новые расширенные требования прозрачности до и после торговли, такие как те, которые в настоящее время применяются к фондовым рынкам для акционерных продуктов [665].

[93] REMIT – это европейский регламент, требующий отчетности по сделкам с деривативами на физические товары. Положения о злоупотреблении рынком для рынков электроэнергии и газа, основанные на MAD. На оптовых рынках энергии используются как производные, так и товарные торги; следовательно, подход к манипулированию рынком и инсайдерской торговле должен быть согласован и совместим между рынками. Обязательство предоставлять подробную информацию об оптовых сделках с энергией.

требования к их работе, на основе трех базовых принципов: 1) доступность капитала для стартапов; 2) новые технологии; 3) новые модели бизнеса [176, 583]. Таким образом, PSD2 представляет собой механизм адаптации финансовой системы ЕС к росту онлайн-платежей и изменениям среды, в которой такие платежи осуществляются.

Важными задачами данной директивы являются повышение доверия клиентов к более эффективным электронным платежам, внедрение эффективной защиты клиентов от мошенничества и других злоупотреблений и ошибок. PSD II содействует развитию двух аспектов FinTech. Во-первых, собирается, агрегируется и анализируется информация из транзакционных платежей клиентов. Директива описывает это как «информационную услугу счета» (AIS). Во-вторых, регулируется «программный мост между веб-сайтом продавца и платформой онлайн-банкинга» клиента, инициирующего платеж через счет продавца.

В Директиве он классифицируется как «служба инициирования платежей» (PIS), которая определена в статье 4 (15) как «услуга для инициирования платежного поручения по запросу пользователя платежной службы в отношении платежного счета, находящегося у другого поставщика платежных услуг». Это безопасная система обмена сообщениями, ни на одном этапе которой поставщик не задерживает платежи клиента. Новые услуги FinTech основаны на инновационном использовании финансовых данных, таких как понимание личных расходов, бюджетирование, инструменты сравнения и индивидуальное финансовое планирование. Поэтому FinTech необходим доступ к данным аккаунтов для реализации своего бизнеса, в то время как традиционные игроки всегда сохраняли строгий и исключительный контроль над этой информацией, чтобы консолидировать свое рыночное влияние. Чтобы помочь FinTech реализовать свой конкурентный потенциал, PSD2 вводит правило доступа к учетной записи, которое позволяет поставщикам услуг по инициированию платежей и информационным службам учетной записи иметь свободный доступ к данным учетной записи пользователя при условии, что они доступны онлайн, и клиент дает свое явное согласие [969]. Таким образом, Директива стимулирует развитие высококонкурентного рынка электронных платежей [948].

Европейское банковское управление (EBA)[94] осуществляет ряд проектов по внедрению PSD II, чтобы обеспечить их безопасность и эффективность [176]: готовится Нормативно-технический стандарт (RTS) о сотрудничестве между государствами, в частности об обмене информацией, включая отдельное руководство по сообщениям о мошенничестве и безопасной аутентификации клиентов (SCA)[95]. Дополнительно разрабатывается набор Внедряющих технических стандартов (ITS) для настройки регистра EBA [970].

Евросистемой разработан и обслуживается ряд сервисов, которые гварантируют свободный поток денежных средств, ценных бумаг и залогового обеспечения по всей Европе (TARGET Services). Эти услуги инфраструктуры финансового рынка включают TARGET2 (для расчетов по платежам в режиме реального времени RTGS), T2S (для расчетов по ценным бумагам)[96], TIPS (сервис для мгновенных платежей) и ECMS (сервис для управления активами, используемыми в качестве обеспечения в кредитных операциях Евросистемы) [971].

В 2020 году BIS объявил об открытии инновационного центра в сотрудничестве с ECB в г. Париже и Франкфурте [583].

Массовое развертывание датчиков в различных средах позволяет собирать явные данные и информацию о людях, а с помощью аналитических инструментов появляется возможность потенциально профилировать и идентифицировать пользователей даже на основе анонимных данных [185].

---

[94] Регулирующее агентство Европейского Союза, деятельность которого включает проведение стресс-тестов европейских банков для повышения прозрачности европейской финансовой системы и выявления слабых мест в структуре капитала банков.

[95] В рамках усилий по защите клиентов и предприятий PSD II требует SCA secure customer authentication, который удостоверяет личность клиента и его право на совершение транзакции, прежде чем можно будет сделать электронный платеж. SCA «основан на использовании двух или более элементов, классифицированных как знания (что-то, что знает только пользователь, например пароль или ПИН-код), владение (что-то, что есть только у пользователя, например карта или устройство генерирования кода аутентификации) и наследственность (например, использование отпечатка пальца или распознавания голоса)».

[96] T2S является панъевропейской платформой для расчетов по ценным бумагам в деньгах центрального банка и представляет собой один из крупнейших инфраструктурных проектов, инициированных Евросистемой. T2S – это европейский регламент, который призван интегрировать и гармонизировать фрагментированную инфраструктуру расчетов по ценным бумагам в Европе, где имеется более 35 центральных депозитариев (Central Securities Depositories (CSDs). T2S руководствуется необходимостью снизить стоимость расчетов и оптимизировать управление ликвидностью и капиталом в ЕС [665].

В этой связи важнейшим направлением государственного регулирования в области цифровизации экономики в ЕС является защита личной информации, обеспеченная принятием в 2018 году Общего регламента о защите данных GDPR [938]. Этот нормативный акт создал правовую основу, которая устанавливает руководящие принципы для сбора и обработки персональных данных[97] в пределах Европейского Союза, а также для всех организаций, обрабатывающих данные пользователей ЕС, независимо от того, где организация территориально располагается [933]. Кроме того, введены штрафные санкции за нарушение данного регламента[98]. Надзорным органом ЕС по обеспечению соблюдения европейскими учреждениями и органами права на конфиденциальность и защиту данных при обработке персональных данных и разработке новых политик является Европейский надзорный орган по защите данных (EDPS) [948].

Важно отметить, что права на переносимость данных, закрепленные в GDPR и PSD2, имеют одно и то же обоснование, которое заключается в том, чтобы стимулировать и поощрять межплатформенную конкуренцию на цифровых рынках, снижая затраты на переключение потребителей и избегая блокировки персональных данных. Если GDPR явно признает индивидуальный контроль над личными данными как цель закона о защите данных, позволяющего потребителям передавать свои данные от одного онлайн-провайдера другому, путем введения правила доступа к учетной записи, PSD2 стремится стимулировать конкуренцию на рынках розничных платежей путем предоставления возможности потребителям использовать свои собственные данные [969].

---

[97] «Персональные данные» означают любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу («субъект данных»). Под идентифицируемым физическим лицом понимается лицо, которое может быть идентифицировано прямо или косвенно, в частности, посредством ссылки на такой идентификатор, как имя, идентификационный номер, данные о местоположении, онлайновый идентификатор или на один или несколько факторов, характерных для физической, физиологической, генетической, психической, экономической, культурной или социальной идентичности этого физического лица. «Контролер» означает физическое или юридическое лицо, государственное управление, агентство или другой орган, который самостоятельно или совместно с другими определяет цели и средства обработки персональных данных [972].

[98] Компании могут быть оштрафованы не более чем на 20 млн евро, или 4% мирового оборота за нарушение конфеденциальности личных данных.

Принятие трех ключевых нормативных актов в области обеспечения платежных услуг: MIF, PSD2, GDPR, создали основу для формирования Единой европейской платежной зоны (SEPA) – инициативы ЕС по интеграции европейской системы розничных платежей с особым вниманием к электронным платежам [559].

Функциональная совместимость в средах IoT является одним из основных направлений программ исследований ЕС. Участие в программах разработки стандартов принимают различные страны, группы предприятий. Примерами рамочных программ ЕС в области разработки стандартов IoT: EU FP7, Horizon 2020 [973][99].

ЕС прорабатывает решения в области кибербезопасности, которые отвечают потребностям стремительно развивающихся цифровых рынков [192]. В 2001 году подписана Конвенция Совета Европы о киберпреступности (Будапештская), которая является первым международным договором о преступлениях, совершенных с помощью Интернета и других компьютерных сетей, включая, нарушение авторского права, сетевой безопасности, мошенничество, связанное с компьютерами[100] [974]. Основная цель конвенции заключается в проведении общей уголовной политики, направленной на защиту общества от киберпреступности, путем принятия соответствующего законодательства и развития международного сотрудничества [975]. В 2005 году подписано Рамочное решение Совета 2005/222/JHA о нападениях на информационные системы, направленное на активизацию международного сотрудничества в области уголовного правосудия против компьютерных преступлений [936].

В 2017 году Европейская комиссия представила пакет инициатив, связанных с кибербезопасностью, которые, среди прочего, включают рекомендации для Европейской организации кибербезопасности (ECSO)[101] по предоставлению помощи государствамчленам в борьбе с кибератаками, а также новую европейскую схему сертификации, которая обеспечит безопасное использование

[99] Одной из целей Horizon 2020 является обеспечение функциональной совместимости данных – обмен и повторное использование между исследователями, учреждениями, организациями, странами и т. д.

[100] Участниками конвенции являются 66 стран мира.

[101] Европейская организация кибербезопасности (European Cybersecurity Organisation ECSO), некоммерческая организация, созданная в 2016 году, является ведущим отраслевым партнером Европейской комиссии по реализации государственно-частного партнерства по кибербезопасности (Cybersecurity contractual Public-Private Partnership cPPP).

продуктов и услуг в цифровом мире[102]. В рамках проекта ЕС H2020 «Упреждающее управление рисками посредством повышения осведомленности о киберситуации» (PROTECTIVE) [976] изучается вопрос о том, как улучшить управление инцидентами и рисками в области кибербезопасности в открытом доступе [214]. В 2013 году основан Европейский центр киберпреступности при Европоле (EC3), который сыграл ключевую роль в создании информационных материалов и отчетов для государств-членов, а также в поддержке расследований онлайн-мошенничества, совершаемого организованными преступными группировками. В 2014 году создана Совместная целевая группа по борьбе с киберпреступностью (J-CAT) с целью трансграничного взаимодействия стран ЕС.

Кроме того, публикуются регулярные отчеты об оценке угрозы организованной преступности в Интернете (IOCTA), которые являются важным источником информации для определения приоритетов в операциях и политике [977]. Отмечается, что переход к безналичной экономике создал широкие возможности для мошенничества и подделки безналичных платежных средств, таких как кредитные карты и инструменты онлайн-платежей, что представляет серьезную угрозу безопасности ЕС.

В документе отмечено, что, несмотря на развитие законодательной базы по борьбе с отмыванием денег и возвращением активов, выявляется лишь незначительная доля операций по отмыванию денег и конфискуется только 1% криминальных активов. Это усугубляется более широким использованием финансовых каналов с более ограниченным надзором, чем банковский сектор, таких как виртуальные валюты. Как подчеркивается в Плане действий по борьбе с отмыванием денег на 2020 год, система ЕС по борьбе с отмыванием денег должна быть значительно улучшена, чтобы устранить серьезные расхождения в способах ее применения и серьезные недостатки в обеспечении соблюдения правил. Финансовые расследования не используются в полной мере отчасти из-за недостаточного потенциала правоохранительных органов

[102] Закон ЕС о кибербезопасности вводит общеевропейскую систему сертификации кибербезопасности для продуктов, услуг и процессов ИКТ. Компании, ведущие бизнес в ЕС, получат выгоду от необходимости сертифицировать свои продукты, процессы и услуги ИКТ только единожды и признания выданных сертификатов во всем Европейском Союзе (The EU Cybersecurity Act. – Режим доступа: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act. – Дата доступа: 03.03.2021).

для проведения этих сложных и обременительных расследований. Как было объявлено в Плане действий по борьбе с отмыванием денег на 2020 год, обеспечение эффективного внедрения существующей системы борьбы с отмыванием денег является приоритетной задачей. В дополнение к текущим усилиям по обеспечению надлежащей реализации, Комиссия подготовила законодательные предложения, направленные на усиление и развитие Рамочной основы ЕС по борьбе с отмыванием денег, создание единого свода правил прямого действия для усиления на уровне ЕС надзора, а также механизма ЕС для координации и поддержки подразделений финансовой разведки. Одновременно необходимо будет улучшить международное сотрудничество в борьбе с отмыванием денег. Государства-члены должны в полной мере использовать возможности, предлагаемые Оперативной сетью по борьбе с отмыванием денег (AMON), Межведомственной сетью Camden Asset Recovery (CARIN), неформальными международной сетью правоохранительных органов по борьбе с отмыванием денег и сетью практикующих сотрудников правоохранительных и судебных органов, специализирующихся в области отслеживания, замораживания, ареста и конфискации активов.

Для усиления европейского потенциала кибербезопасности Комиссия предложила создать новый европейский центр компетенции в области промышленной, технологической и исследовательской кибербезопасности и сеть национальных координационных центров. Предлагаемый центр будет объединять имеющийся у стран опыт и согласовывать европейские разработки и внедрение технологий кибербезопасности. Он будет работать с промышленностью, академическим сообществом и другими участниками над формированием общей программы инвестиций в кибербезопасность и определять приоритеты финансирования исследований, разработки и развертывания решений по кибербезопасности (через программы Horizon Europe и Digital Europe) [933]. Для изучения возможностей в области кибербезопасности в ЕС Комиссия разработала комплексную платформу под названием «Атлас кибербезопасности».

В 2013 году принята Стратегия кибербезопасности ЕС, за которой последовало Коммюнике ЕС об устойчивости, сдерживании и защите, которое представляет собой твердое обязательство по защите цифровой безопасности граждан, продуктов

и услуг [978, 979, 980][103]. В 2016 году вступила в силу Директива о безопасности сетевых и информационных систем ЕС (Директива 2016/1148) (NIS) [981][104], которая совместно с GDPR призвана стимулировать использование облачных технологий в финансовой сфере. Целью директивы является улучшение функционирования внутреннего рынка путем достижения высокого общего уровня безопасности сетевых и информационных систем в пределах ЕС. В рамках требований NIS государства-члены ЕС должны определить операторов «основных услуг» на своей территории на энергетическом, транспортном, банковском, финансовом рынках и в секторах здравоохранения, включая энергетических операторов, осуществляющих поставки, распределение и хранение природных ресурсов (нефтепроводов, нефтеперерабатывающих заводов и буровых установок); поставщиков транспортных услуг (авиаперевозчиков, интеллектуальные транспортные системы или управление движением); банковской сферы (кредитных учреждений); торговли финансовыми инструментами (фондовых рынков); поставщиков медицинских услуг (больниц или клиник) [982]. Директива устанавливает ряд организационных и стратегических обязанностей государств-членов, таких как принятие национальных стратегий и групп реагирования на инциденты компьютерной безопасности (CSIRT).

---

[103] Стратегия единого цифрового рынка (Digital Single Market DSM) признает кибербезопасность и доверие в качестве ключевых факторов успеха инициативы DSM (European Commission (EC). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A Digital Single Market Strategy for Europe. COM(2015) 192 final).

[104] Согласно NIS, если банк включен в список или соответствует определенным критериям, установленным соответствующим государством-членом, и полагается на поставщика для предоставления банку «основных услуг», последний должен будет уведомить соответствующий орган об инцидентах, оказывающих «какое-либо существенное влияние на непрерывность предоставления этих основных услуг из-за инцидента, затрагивающего поставщика, и власти имеют право уведомлять другие органы государства-члена или даже общественность при определенных обстоятельствах. Государства-члены устанавливают национальные наказания за нарушение NIS. «Инциденты», в соответствии с NIS, шире, чем «утечки персональных данных», согласно GDPR. Поэтому банкам следует обеспечить, чтобы контракты с поставщиками содержали условия, достаточные для того, чтобы позволить банкам выполнять их обязательства по уведомлению NIS. Ключевой задачей является уравновешивание этих юридических обязательств с коммерческим стремлением к индустриальному IoT. Директива ЕС о сетевой и информационной безопасности определяет обязательства путем установления минимальных общеевропейских гармонизированных стандартов. Государствам-членам ЕС необходимо принять национальные меры и стратегии реализации, особенно в отношении трансграничного сотрудничества [982].

Директива также налагает требования безопасности на операторов основных услуг, включая меры по управлению рисками, чтобы «идентифицировать любой риск инцидентов, предотвращать, обнаруживать и обрабатывать инциденты и смягчать их воздействие» [977][105]. Директива также распространяется на три конкретных цифровых сервиса: онлайн-рынки, поисковые системы и облачрные сервисы. При этом следующие факторы должны быть приняты во внимание: а) безопасность систем и возможностей; б) обработка инцидентов; в) управление непрерывностью бизнеса; г) мониторинг, аудит и тестирование; д) соответствие международным стандартам. Для определения того, является ли инцидент существенным, сохраняются продолжительность и географическое распространение. Однако также необходимо учитывать влияние на экономическую и социальную деятельность, степень сбоев и количество пользователей, которые полагаются на свои услуги, для предоставления собственных услуг [982].

В 2020 году Европейская комиссия представила новую Стратегию кибербезопасности ЕС (Директива NIS2), которая охватывает безопасность основных служб, таких как больницы, энергосистемы, железные дороги и постоянно увеличивающееся количество подключенных объектов [983]. Стратегия направлена на создание коллективных возможностей для реагирования на крупные кибератаки. В ней также изложены планы работы с партнерами по всему миру для обеспечения международной безопасности и стабильности в киберпространстве, описывается, как совместное киберподразделение может обеспечить наиболее эффективный ответ на киберугрозы, используя коллективные ресурсы и опыт, доступные государствам – членам ЕС. Стратегия содержит предложения по использованию трех основных инструментов: нормативных, инвестиционных и политических инициатив. Они будут направлены на реализацию следующих задач: обеспечение устойчивости, технологического суверенитета и лидерства; формирование оперативного потенциала по предотвращению, сдерживанию и реагированию;

[105] Поставщики облачных услуг несут обширные обязательства по обеспечению безопасности в рамках NIS, а дизайн многих систем IoT ориентирован на зондирование данных, а затем на их агрегирование в облаке для аналитики для предоставления контекстуально-релевантных услуг. Таким образом, когда продукты IoT используют облачные сервисы при обработке личных данных, обязательства NIS и GDPR могут выйти на первый план [982].

осуществление сотрудничества для развития глобального и открытого киберпространства. Отмечается, что ЕС намерен осуществлять реализацию данной стратегии посредством беспрецедентного роста инвестиций в цифровые технологии в течение следующих семи лет (четырехкратное увеличение объема инвестиций).

В 2004 году в ЕС разработаны: Европейская программа защиты критической инфраструктуры (EPCIP) и Европейская сеть предупреждений о критической инфраструктуре (CIWIN), которые включают риски кибератак и террористических нападений [759]. В 2006 году предложен окончательный вариант Директивы ЕС COM (2006) 786[106], которая обязала все государства-члены интегрировать компоненты EPCIP в свое национальное законодательство. В 2008 году принята Директива Совета ЕС по EPCIP по идентификации и обозначению европейской критической инфраструктуры и оценке необходимости улучшения ее защиты (2008/114/EC) [984][107]. В европейской нормативной базе важной частью устойчивости критической инфраструктуры является способность выявлять и анализировать взаимозависимости. Хотя взаимозависимости являются общей чертой систем критической инфраструктуры, которые часто реализуются через кибersоединения с помощью информационных и коммуникационных технологий, многие из них определяются на региональном уровне, поскольку они тесно связаны с географической близостью, географической функциональностью и интегрированными региональными сетями.

В этой связи важно отметить, что в 2016 году в Коммюнике Европейской комиссии «Прокладывая путь к эффективному и подлинному Союзу безопасности» была представлена концепция Союза безопасности ЕС (Security Union). Эта концепция основана на Европейской повестке дня по безопасности 2015 года, в рамках которой был предложен новый подход, базирующийся на совместной

---

[106] Директива ЕС определяет критически важную инфраструктуру следующим образом: «Актив, система или ее часть, расположенные в государствах-членах, которые необходимы для поддержания жизненно важных функций общества, здравоохранения, безопасности, охраны, экономического или социального благополучия населения, и разрушение или разрушение которых окажет значительное влияние на государство-член в результате неспособности сохранить эти функции».

[107] Директива определяет защиту как «все действия, направленные на обеспечение функциональности, непрерывности и целостности критических инфраструктур с целью предотвращения, смягчения и нейтрализации угрозы, риска или уязвимости».

ответственности Европейского союза и стран ЕС[108]. Задачами Союза безопасности ЕС является осуществление следующих действий: убедиться, что политика безопасности ЕС отражает меняющийся ландшафт угроз; обеспечить долгосрочную устойчивость; привлечь институты и агентства ЕС, правительства, частный сектор и отдельных лиц к общесоциальному подходу; объединить множество областей политики, непосредственно влияющих на безопасность [985]. Стратегия Союза безопасности ЕС принята в 2020 году в форме Коммюнике Еврокомиссии [986], в которой отмечено, что защита ЕС и его граждан – это не только обеспечение безопасности в границах ЕС, но и решение внешнего измерения безопасности. Подход ЕС к внешней безопасности в рамках общей внешней политики и политики безопасности (CFSP) и общей политики безопасности и обороны (CSDP) останется важным компонентом усилий по укреплению безопасности внутри ЕС. Сотрудничество с третьими странами и на глобальном уровне для решения общих проблем имеет центральное значение для эффективных и всеобъемлющих ответных мер, при этом стабильность и безопасность в странах-соседях ЕС имеют решающее значение для собственной безопасности ЕС. Стратегия охватывает 2020–2025 годы и устанавливает общий подход к безопасности, который может эффективно и скоординированно реагировать на быстро меняющийся уровень угроз. Она определяет стратегические приоритеты и соответствующие действия по устранению цифровых и физических рисков комплексным образом во всей экосистеме Союза безопасности. Отдельно отмечено, что качество жизни граждан зависит от широкого спектра услуг, таких как энергетика, транспорт, финансы, здравоохранение, которые базируются как на физической, так и цифровой инфраструктуре, что повышает их уязвимость и вероятность сбоев. Это привело к стратегической важности проблематики кибербезопасности технологий. Потенциальный ущерб еще больше умножается из-за взаимозависимости физических и цифровых систем: любое физическое воздействие обязательно затронет цифровые системы, в то время как кибератаки на информационные системы и цифровые инфраструктуры могут привести к остановке жизненно важных услуг. Развитие IoT и более широкое использование искусственного интеллекта принесут новые выгоды, а также новый

[108] В сентябре 2016 года создан специальный портфель комиссаров Союза безопасности при содействии целевой группы, которая опирается на опыт всей Европейской комиссии.

набор рисков. «Киберпреступность как услуга» и подпольная киберпреступная экономика обеспечивают легкий доступ к продуктам и услугам, связанным с киберпреступностью, в Интернете. Обосновывается целесообразность реализации отраслевых инициатив по борьбе с конкретными рисками, с которыми сталкиваются объекты критически важной инфраструктуры, такие как транспорт, космос, энергетика, финансы и здравоохранение. С учетом высокой зависимости финансового сектора от IT-услуг и его высокой уязвимости к кибератакам, первым шагом новой Стратегии станет инициатива по повышению операционной устойчивости финансовых секторов в цифровой среде. В связи с особой чувствительностью и воздействием энергетической системы специальная инициатива будет поддерживать более высокую устойчивость критически важной энергетической инфраструктуры к физическим, кибер- и гибридным угрозам, обеспечивая равные условия для операторов энергетики в разных странах.

Связанные с безопасностью последствия прямых иностранных инвестиций, которые могут повлиять на критические инфраструктуры или критические технологии, также будут предметом оценок, проводимых государствами-членами ЕС и Комиссией в соответствии с новой европейской структурой для проверки прямых иностранных инвестиций.

ЕС также может создавать новые инструменты для поддержки устойчивости критически важных инфраструктур. Страны ЕС должны быть готовы к возможным будущим кризисам, угрожающим безопасности, стабильности и устойчивости Интернета. Обеспечение бесперебойной работы Интернета означает устойчивость к киберинцидентам и злонамеренным действиям в Интернете, а также ограничение зависимости от инфраструктуры и услуг, расположенных за пределами Европы. Это потребует сочетания законодательства с обзором существующих правил для обеспечения высокого общего уровня безопасности сети и информационных систем в ЕС; увеличения инвестиций в исследования и инновации; рассмотрения вопроса о развертывании или укреплении базовой инфраструктуры и ресурсов Интернета, особенно системы доменных имен.

Ключевым элементом защиты основных цифровых активов стран ЕС является предоставление критически важной инфраструктуры канала для безопасной связи. Комиссия работает с государствами-членами над созданием сертифицированной безопасной сквозной квантовой инфраструктуры, наземной и космической, в

сочетании с безопасной государственной системой спутниковой связи, изъясненной в Положении о космической программе.

Эти атаки исходят из широкого спектра источников внутри и за пределами ЕС и нацелены на области максимальной уязвимости. Их участниками являются государственные или поддерживаемые государством субъекты, нацеленные на ключевые цифровые инфраструктуры, такие как крупные поставщики облачных услуг. Киберриски также стали серьезной угрозой для финансовой системы[109]. В 2017 году ЕС выдвинул подход к кибербезопасности, в основе которого лежат повышение устойчивости, быстрое реагирование и эффективное сдерживание. Это требует систематизации подходов, ориентированных на институты, агентства и органы ЕС, государства-члены, промышленность, научные круги и отдельных гражданских лиц в отношении приоритетности проблематики кибербезопасности. Этот горизонтальный подход предполагается дополнить отраслевыми подходами к кибербезопасности в таких областях, как энергетика, финансовые услуги, транспорт или здравоохранение.

Изучение новых и расширенных форм сотрудничества между разведывательными службами, Разведывательным и ситуационным центром Европейского союза (EU INTCEN) и другими организациями, занимающимися вопросами безопасности, должно быть частью усилий по повышению кибербезопасности, а также борьбе с терроризмом, экстремизмом, радикализмом и гибридными угрозами.

Также важны общие правила информационной безопасности и кибербезопасности для всех институтов, органов и агентств ЕС. Целью должно быть создание обязательных и высоких общих стандартов для безопасного обмена информацией и безопасности цифровых инфраструктур и систем во всех учреждениях, органах и агентствах ЕС. Эта новая структура должна подкрепить прочное и эффективное оперативное сотрудничество в области кибербезопасности между институтами, органами и агентствами ЕС, сосредоточенное на роли Группы реагирования на компьютерные чрезвычайные ситуации (CERT-EU) для институтов, органов и агентств ЕС.

С учетом глобального характера киберугроз необходимость построения и поддержания прочных международных партнерских отношений приобретает основополагающее значение для дальнейшего предотвращения, сдерживания и реагирования на кибератаки.

---

[109] Международный валютный фонд оценил ежегодные убытки от кибератак в 9% от чистой прибыли банков во всем мире, или около 100 млрд долларов.

Рамки для совместного дипломатического реагирования ЕС на злонамеренные кибердействия («набор инструментов кибердипломатии») определяют меры в пределах Общей внешней политики и политики безопасности, включая ограничительные меры (санкции), которые могут использоваться против действий, наносящих ущерб его политической безопасности и экономическим интересам. ЕС должен также углубить свою работу за счет фондов развития и сотрудничества, чтобы обеспечить создание потенциала для поддержки государств-партнеров в укреплении их цифровых экосистем, принятии национальных законодательных реформ и соблюдении международных стандартов. Это повышает устойчивость всего сообщества и его способность противостоять киберугрозам и эффективно реагировать на них. Это включает в себя конкретную работу по продвижению стандартов ЕС и соответствующего законодательства для повышения кибербезопасности. Для целей финансирования реализации стратегии кибербезопасности в рамках ЕС возможно использование бюджетных средств Евросоюза в размере до 2 млрд евро (в 2021–2027 годах), а также инвестиции стран-членов и специализированных организаций. Кроме того, предлагается использовать антикризисный финансовый механизм в размере около 134 млрд евро [238].

Важным элементом защиты информации является внедрение современных систем идентификации пользователей. Отмечается нехватка надежных и сохраняющих конфиденциальность систем управления идентификацией (Identity Management Systems IdM), которые бы предоставили пользователям полный контроль над персональными данными в различных сценариях, одновременно решая проблемы, связанные с идентичностью. Европейский проект Aries (ReliAble euRopean Identity EcoSystem) внедрил целостную систему управления идентификационными данными, с целью уменьшения случаев мошенничества с этими данными, повышения безопасности при управлении персональными данными идентификации, в онлайн [987][110].

[110] Система предотвращает идентификацию личности и помогает сохранить конфиденциальность пользователя с помощью инновационных механизмов и биометрических методов. Он усиливает связь между физической идентификацией (на основе официального документа, такого как ePasport) и производной цифровой идентификацией (идентификатор мобильного телефона и мобильные анонимные учетные данные), чтобы уменьшить угрозы, связанные с идентификацией. Кроме того, ARIES предоставляет новые возможности проверки личности в деятельности правоохранительных органов (Law Enforcement Authorities LEA) под строгим контролем доступа полностью в руках пользователя, в то время как данные хранятся в компоненте, защищенном анонимностью и шифрованием.

В 2020 году в рамках выполнения Решения (ЕС) (2019/796) относительно ограничительных мер против кибератак, угрожающих Европейскому союзу или его государствам-членам, Совет Европы принял постановление (2020/1125) для совместного дипломатического реагирования на злонамеренные кибердействия [988][111]. Для предотвращения, сдерживания и реагирования на продолжающееся и усиливающееся злонамеренное поведение в киберпространстве шесть физических лиц и три субъекта или организации включены в список субъектов и органов, на которые распространяются ограничительные меры[112]. Более того, в июне 2021 года ЕС совместно с США заявили о запуске инициативы по борьбе с программами-вымогателями[113] [989].

В рамках реализации пакета санкций против Российской Федерации в апреле 2021 года США заявили об укреплении коллективной кибербезопасности, которое включает [990]:

1) продвижение правовой базы ответственного поведения государств в киберпространстве и сотрудничество с союзниками в противодействии вредоносной кибердеятельности. Организуется курс для политиков всего мира по политическим и техническим аспектам наложения ответственности за киберинциденты, открытый в Германии. Активизируются усилия по подготовке юристов и политиков министерств иностранных дел по вопросам применимости международного права к поведению государств в киберпространстве;

---

[111] В 2018 году Совет Европы решительно осудил злонамеренное использование информационных и коммуникационных технологий, в том числе в кибератаках, общеизвестных как «WannaCry» и «NotPetya», которые нанесли значительный ущерб и экономические потери в Союзе и за его пределами. Президенты Европейского совета и Европейской комиссии и Высокий представитель Союза по иностранным делам и политике безопасности выразили серьезную обеспокоенность в совместном заявлении о попытке кибератак с целью подорвать целостность Организации по запрещению химического оружия (ОЗХО) в Нидерландах

[112] Эти лица или организации несут ответственность, оказывали поддержку, или участвовали в них, или содействовали кибератакам либо попыткам кибератак, включая попытку кибератак против ОЗХО и кибератак, общеизвестных как «WannaCry», и «NotPetya», а также «Operation Cloud Hopper».

[113] В совместном заявлении ЕС и США говорится, что ЕС и США будут работать вместе «посредством правоохранительных действий, повышая осведомленность общественности о том, как защищать сети, а также о риске выплаты виновным преступникам, и поощрять те государства, которые закрывают глаза на это преступление для ареста и экстрадиции или эффективного преследования преступников на их территории» [989].

2) укрепление коллективной безопасности в киберпространстве. CYBER FLAG 21-1 создаст специальное сообщество кибероператоров и улучшит общие возможности США и их союзников по выявлению, синхронизации и совместному реагированию на смоделированные вредоносные действия в киберпространстве, нацеленные на критически важную инфраструктуру и ключевые ресурсы.

Таким образом, межгосударственный конфронтационный тренд в сфере кибербезопасности является доминирующим. Вместе с тем важно отметить совместную резолюцию России и США в ООН по кибербезопасности, призванную внедрить добровольные (на первом этапе) правила ответственного поведения государств в Интернете [991].

В региональном разрезе следует также выделить страны Юго-Восточной Азии на примере АСЕАН[114], которые в рамках данного интеграционного объединения приоритетное внимание уделяют развитию сектора информационно-коммуникационных технологий и вопросам цифровой безопасности [992]. План развития АСЕАН в области ИКТ предусматривает формирование динамичной, развитой цифровой экономики. Главная цель инициатив АСЕАН в секторе ИКТ состоит в уменьшении цифрового разрыва путем создания соответствующей инфраструктурной основы. Кроме того, усилия направлены на содействие взаимосвязанности и функциональной совместимости сетей связи для содействия всем секторам экономики [993]. В 2000 году всеми членами АСЕАН подписано соглашение E-ASEAN, направленное на повышение конкурентоспособности сектора ИКТ, сокращение цифрового разрыва между членами, развитие сотрудничества между государственным и частным секторами и либерализацию торговли продуктами и услугами ИТ[115].

---

[114] Ассоциация государств Юго-Восточной Азии (АСЕАН). Устав АСЕАН включает три основных элемента: 1) Сообщество политической безопасности АСЕАН (APSC); 2) Экономическое сообщество АСЕАН (AEC); 3) Социокультурное сообщество АСЕАН (ASCC).

[115] E-ASEAN стремится: 1) содействовать созданию информационной инфраструктуры АСЕАН путем улучшения взаимосвязанности и функциональной совместимости между системами каждой страны; 2) стимулировать электронную коммерцию, создавая доверие посредством реализации законов и нормативных актов, обеспечивая безопасный способ оплаты и защиту личных и уязвимых данных; 3) содействовать торговле и инвестициям в продукты и услуги ИКТ путем подписания MRA, охватывающих сектора ИКТ, с целью создания единого международного стандарта; 4) организовать электронное общество путем распространения знаний об ИКТ среди владельцев малого бизнеса, работников сектора ИКТ и государственных служащих; 5) улучшить предоставление государственных услуг за счет использования современных приложений для облегчения связи между государственным и частным секторами.

Заключение

Таким образом, анализ моделей институциональной международной экосистемы цифровой экономики свидетельствует о ее стрмительной эволюции и системной трансформации ключевых блоков регулирования цифровизации, включая определение общей стратегии; внедрение и регулирование отдельных цифровых инноваций и концепций; регулирование финансового рынка и защиту киберпространства.

В настоящее время с учетом трансграничного характера рисков и угроз как на международном, так и наднациональном уровнях происходит поступательное формирование новой системы регулирования. На международном (первом) уровне данная система включает традиционные институты системы ООН, адаптирующие мандаты, механизмы и инструменты регулирования к современным вызовам цифровизации. На уровне специализированных международных организаций (втором), происходит интенсивная эволюция как традиционных институтов, включая IOSCO, FATF, BIS, IEC, ISO, IEEE, так и формирование новых инициатив и механизмов регулирования, в том числе созданных по решению G20, WEF и др. По причине высокой динамики внедрения новых цифровых механизмов и бизнес-моделей единое регулирование по сферам деятельности к настоящему времени отсутствует. Вместе с тем отмечаем объединение ресурсов и компетенций международных институтов для выработки совместных решений (рекомендаций) в отношении рисков, связанных с цифровыми инновациями.

На уровне интеграционных объединений (третьем) наиболее комплексную систему регулирования цифровой экономики осуществляет ЕС. Данное интеграционное объединение на основе конвергенции, синергии различных цифровых концепций, поступательно формирует нормативно-правовую, ресурсную и организационную базу для адаптации региональной экономики к актуальным и будущим вызовам и угрозам. При этом современный уровень развития институциональной экосистемы ЕС, предполагающий построение общей стратегии цифровизации, также находится в стадии формирования.

С учетом сложности и комплексности стоящих перед международными институтами задач адаптации к соврменным рискам и угрозам цифровой экономики, представляется целесообразным

разработать основы институционализации международных механизмов обмена опытом противодействия киберугрозам и соответствующей экспертизой на государственном и косударственно-частном уровнях, а также общими техническими нормативными актами и стандартами безопасности цифровых решений, включая IoT, Cloud Computing, AI / ML, Big Data, Блокчейн, FinTech и пр.

3.4. Регулирование цифровой экономики в ЕАЭС и Союзном государстве

Интеграционные группировки играют важную роль в регулировании проблем экономического развития и позволяют не только передавать лучшие регуляторные практики между странами-участниками, но и концентрировать аккумулированные финансовые, экспертные, технологические ресурсы на решении актуальных экономических проблем. Опыт ЕС показывает, что на наднациональном уровне возможно эффективно разрабатывать самые передовые регуляторные практики, которые затем имплементируются на страновом уровне.

ЕАЭС в качестве интеграционной группировки, связывающей страны с большим технологическим разрывом, неравномерной цифровой инфраструктурой, достаточно сложная задача разработать общую практику, адаптируемую для государств с разной структурой экономики и технологическим потенциалом.

Так, сравнительный анализ глобальной конкурентоспособности в 2019 году, проведенный WEF [994], в отношении странчленов ЕАЭС (за исключением Республики Беларусь), показал, что, с точки зрения цифровизации самое высокую позицию (43-е место) занимает Российская Федерация, на втором месте – Казахстан (55-е место), затем следуют Армения (69-е место), Киргизия (96-е место). Вместе с тем по сводному показателю адаптации ИКТ позиции стран ЕАЭС более высокие: 22-е место занимает Российская Федерация, Казахстан – 44-е место, затем следуют Армения (59-е место), Киргизия (65-е место). Кроме того, как показал анализ эффективность системы регулирования цифрового рынка, проведенный ITU в 2020 году [995] среди стран ЕАЭС, наиболее высокие показатели имеют Армения (85,5 баллов), Киргизия (74,5 балла), Казахстан (54 балла), Беларусь (44,5 балла), Россия (42 балла). По показателю развития цифрового правительства [996] в 2020 году среди

стран ЕАЭС первое место занимал Казахстан (29-е место в мире), Россия (36-е место), Беларусь (40-е место), Армения (68-е место), Киргизия (83-е место).

ЕАЭС на наднациональном уровне осуществляет разработку институциональной базы цифровой трансформации экономик государств-членов на основе имплементации лучших страновых практик и стандартов. Анализ основных стратегий и институциональных блоков формирования современной экосистемы цифровой экономики ЕАЭС позволяет сформировать следующую институциональную матрицу экосистемы цифровой экономики интеграционной группировки (табл. 3.6).

Таблица 3.6

Институциональная матрица экосистемы цифровой экономики на уровне стратегических программ ЕАЭС (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2016–2018 годы)	СЦ	Заявление о цифровой повестке ЕАЭС, 2016	ВЕЭС	Разработка основных направлений реализации цифровой повестки до конца 2025 года, приоритетов проработки инициатив: цифровая прослеживаемость движения продукции, товаров, услуг и цифровых активов; цифровая торговля; цифровые транспортные коридоры; цифровая промышленная кооперация; соглашение об обороте данных; система «регуляторных песочниц»
		Основные направления реализации цифровой повестки ЕАЭС до 2025 года, 2017		
		О Концепции создания условий для цифровой трансформации промышленного сотрудничества в рамках Евразийского экономического союза и цифровой трансформации промышленности государств – членов Союза, 2018	СЕЭС	Выработка рекомендаций по определению стратегии и инструментария обеспечения цифровой трансформации промышленности

Продолжение табл. 3.6

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2016–2018 годы)	ИБЦИ	Рабочая группа высокого уровня года, 2017	МС	Подготовка основных направлений реализации цифровой повестки ЕАЭС до 2025
		Офис управления инициативами, 2017	МС	Общая организация и координация работы по проработке инициатив в рамках реализации цифровой повестки ЕАЭС
	ИБФР	—	—	—
	ИБЗК	Соглашения о взаимодействии в сфере информационной безопасности между центральными банками стран ЕАЭС, 2018	ЦБ	Исследования вредоносного программного обеспечения, консультирование в случае кибератак
Первый уровень (2019 – н. в.)	СЦ	Концепция трансграничного информационного взаимодействия, 2019	МС	Общие подходы к реализации электронного взаимодействия между бизнесом и государственными органами, регламентация использования электронной цифровой подписи
	ИБЦИ	Проект «Работа без границ», 2019–2021	СЕЭС	Формирование экосистемы трудоустройства граждан ЕАЭС
		Проект «Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий», 2019	МС, СЕЭС, КЕЭК	Создание автоматизированной системы по предоставлению хозяйствующим субъектам стран ЕАЭС механизма подбора наиболее эффективных партнеров, возможности вовлечения предприятий СМБ в производственные цепочки крупных производителей
		Единый реестр программ для ЭВМ и баз данных государств – членов ЕАЭС, 2019	МЦР	Формирование реестра ПО, квалифицированного для участия в госзакупках РФ

Окончание табл. 3.6

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2019 – н. в.)	ИБЦИ	Проект «Экосистема цифровых транспортных коридоров», 2020	МС	Интеграция информации о транспортных средствах, грузах, разрешительных и сопроводительных документах на всех этапах перевозки
		Программа по созданию совместных геоинформационных продуктов стран ЕАЭС, 2020	ЕЭК	Предоставление космических и геоинформационных услуг на основе данных дистанционного зондирования Земли
		Проект создания единой информационной среды научного сообщества государств – членов ЕАЭС, 2021	МЭР	Синхронное развитие цифровых технологий в науке и образовании, повышение общенаучного потенциала
		Проект «Цифровое техническое регулирование», 2021	СЕЭС	Цифровизация процессов формирования обязательных требований к продукции, разработки техрегламентов и перечней международных и региональных стандартов в сфере техрегулирования
		Формирование рабочей группы высокого уровня по вопросам цифровой трансформации, 2021	МС	Проработка соглашения об обороте данных в ЕАЭС
	ИБФР	—	—	—
	ИБЗК	—	—	—

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства; ВЕЭС – Высший Евразийский экономический совет; ЕЭК – Евразийская экономическая комиссия; МС – Межправительственный совет ЕАЭС; СЕЭС – Совет Евразийской экономической комиссии; КЕЭК – Коллегия Евразийской экономической комиссии; ЦБ – Центральный банк РФ; МЦР – Министерство цифрового развития, связи и массовых коммуникаций РФ; МЭР – Министерства экономического развития РФ.

Анализ табл. 3.6 показывает, что наднациональное регулирование цифровой экономики на уровне ЕАЭС имеет ограниченный характер, практически не затрагивающий блоки регулирования финансового рынка и защиты киберпространства. При этом частично институтами регулирования отдельных направлений цифровизации выступают не структуры ЕАЭС, а органы государственного регулирования Российской Федерации на уровне межведомственного взаимодействия.

Стратегические блоки связаны с формированием цифровой повестки ЕАЭС до 2025 года и концепцией трансграничного информационного взаимодействия. Так, направления и ориентиры становления Евразийского экономического союза заложены в Стратегии развития ЕАЭС до 2025 года [997]. Стратегия предполагает выравнивание технологического развития стран-членов и предусматривает 11 направлений и 332 механизма реализации. Особое внимание в стратегии уделяется вопросам образования, здравоохранения, перемещения граждан. Предусмотрено более полное использование промышленного потенциала ЕАЭС, его логистических возможностей, направленных на обеспечение взаимодополняемости экономик [998]. Для сохранения положительной динамики евразийской интеграции одним из векторов ее будущего развития является цифровизация. Актуальность темы цифровой трансформации для стран – участниц ЕАЭС обусловлена объективной необходимостью внедрения цифровых технологий[116].

Основным документом, регламентирующим формирование условий цифровой трансформации промышленного сотрудничества в ЕАЭС, является «Концепция создания условий для цифровой трансформации промышленного сотрудничества в рамках Евразийского экономического союза и цифровой трансформации промышленности государств – членов ЕАЭС» [999]. В ней прописаны цели, задачи цифровой трансформации промышленности, принципы, на основе которых она осуществляется, инструменты, этапы, мониторинг, анализ и координация осуществления цифровой

[116] Документом, отражающим мировые тенденции в рассматриваемой сфере, является доклад о цифровой экономике 2019 ЮНКТАД (Конференция ООН по торговле и развитию) [1000]. В нем особое внимание уделяется международному сотрудничеству в силу многих объективных причин. И тут важно отметить, что именно страновая интеграция является одной из наиболее эффективных форм для подобного взаимодействия.

трансформации промышленного сотрудничества. Среди ключевых технологий – аддитивное производство, высокопроизводительные автоматизированные линии быстрого производства электронной компонентной базы, технологии и ПО роботизированного управления производством, национальные CAD/CAE/CAM-системы, новые технологии сборочного производства, системы управления жизненным циклом изделия, реализация концепции «I4.0».

Согласно данной концепции, цифровая трансформация промышленного сотрудничества осуществляется в три этапа:

1) первый этап (2019–2020 годы) – разработка и запуск общих информационных ресурсов, включая единый реестр промышленных предприятий евразийской сети промышленной кооперации и субконтрактации и единый реестр, содержащий сведения о пользователях евразийской сети трансферта технологий;

2) второй этап (2020–2021) – формирование и реализация серии инициатив и пилотных проектов цифровой промышленной кооперации в рамках ЕАЭС, формирование евразийской цифровой платформы;

3) третий этап (до 2025 года) – полномасштабная разработка и запуск евразийской цифровой платформы, реализация прошедших пилотную отработку проектов цифровой промышленной кооперации в рамках ЕАЭС.

В соответствии с Основными направлениями реализации цифровой повестки ЕАЭС до 2025 года по завершении первого этапа, связанного с моделированием процессов цифровой трансформации, проработкой инициатив и запуском приоритетных проектов, был дан старт следующим проектам:

а) «Цифровая прослеживаемость движения продукции, товаров, услуг и цифровых активов в Евразийском экономическом союзе»;

б) «Разработка концепции экосистемы цифровых транспортных коридоров ЕАЭС». В январе 2020 года Евразийским межправительственным советом утвержден план[117] создания экосистемы

[117] Экосистема будет включать сервисы для расчета маршрутов, электронные путевые листы, электронные международные транспортные накладные, электронные протоколы результатов проверки органами внутренних дел и другие, идут переговоры и с иными иностранными партнерами – для интеграции систем: с китайским Loginc и европейским Fenix. Затраты на экосистему цифровых коридоров ЕАЭС до конца 2025 года могут достичь 5,8 млрд российских рублей – из бюджета ЕАЭС и 4,2 млрд – из бюджетов стран – членов ЕАЭС и средств компаний-участниц. Евразийская

электронных сервисов для грузоперевозок, новых цифровых таможенных, логистических, страховых и финансовых сервисов, а также доработки и интеграции в общую экосистему уже существующих. Общие затраты на проект – 10 млрд российских руб.;

в) «Внедрение и взаимное признание электронных сопроводительных документов в ЕАЭС»;

г) «Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий»;

д) «Унифицированная система поиска “Работа без границ”. Ввод в промышленную эксплуатацию системы «Унифицированная система поиска «Работа без границ»[118] – первого совместного цифрового проекта стран ЕАЭС, состоялся в июле 2021 года [1001]. Запуск совместного цифрового продукта по поиску вакансий и резюме кандидатов будет способствовать увеличению мобильности экономически активного населения ЕАЭС и сбалансированности рынка труда. В результате внедрения системы расширяется взаимодействие рынков труда стран ЕАЭС, которое усилится по мере

экономическая комиссия (ЕЭК, орган ЕАЭС, отвечающий за углубление интеграции и пр.) оценивает экономический эффект от будущей экосистемы в 50–150 млрд рублей к 2025 году. Даст экосистема и побочный эффект – анализ потоков данных, идущих от нее, позволит строить транспортно-экономический баланс, выявлять узкие места, прогнозировать транспортные потоки. Экосистема позволит интегрировать все виды перевозок. По данным ЕЭК, автомобильный транспорт обеспечивает в ЕАЭС 82% перевозок (без трубопроводного транспорта). Цифровые коридоры позволят уже с 2022 года увеличить полезный годовой пробег в пересчете на транспортное средство на 23% за счет снижения непроизводственных простоев, годовая выручка логистических компаний должна увеличиться пропорционально. Цифровые транспортные коридоры будут способствовать развитию торговли внутри ЕАЭС, которое сможет сделать территорию ЕАЭС более конкурентоспособным маршрутом для транзита товаров между Китаем и ЕС (Евразийский союз занялся цифровизацией логистики. – Режим доступа: https://www.vedomosti.ru/business/articles/2020/02/06/822353-evraziiskii-soyuz. – Дата доступа: 06.02.2020).

[118] Проект «Работа без границ» – поисковая система для доступа к информации о свободных рабочих местах и соискателях вакансий, которая содержится в национальных информационных системах стран ЕАЭС. Проект направлен на обеспечение взаимодействия рынков труда в рамках союза с помощью цифровых инструментов, расширение функционала национальных информационных систем за счет добавления возможностей для поиска резюме и вакансий по всем странам ЕАЭС. Одна из особенностей проекта «Работа без границ» – использование распределенной архитектуры, без объединения баз. Применяемая в проекте технология, с одной стороны, обеспечивает необходимый доступ к информации о вакансиях и резюме, а с другой – соблюдение закона о защите персональных данных, так как не происходит трансграничной передачи и хранения информации.

запуска в эксплуатацию разрабатываемых в настоящее время сервисов. Это позволит сформировать полноценную цифровую экосистему по обеспечению трудоустройства и занятости граждан ЕАЭС.

В ежегодном докладе за 2019 год «Будущее Евразийского экономического союза: цифровая трансформация и молодежь» [1002] отмечается, что одним из системообразующих направлений развития ЕАЭС является цифровая повестка Евразийского экономического союза. При активном содействии национального органа – Евразийской экономической комиссии в декабре 2016 года главами государств-членов подписано Заявление о цифровой повестке ЕАЭС [1003], в котором цифровизация обозначена одним из приоритетных направлений интеграции. В рамках проработки приоритетных инициатив и научно-исследовательских работ были созданы и действуют экспертные площадки, формирующие сеть центров компетенций[119].

Внедрение цифровой повестки является экономически оправданным. Согласно подсчетам Группы Всемирного и банка и ЕЭК, экономический эффект от реализации цифровой повестки увеличит ВВП ЕАЭС к 2025 году примерно на 10,6% от общего ожидаемого роста и совокупного ВВП государств-членов, что в абсолютных величинах составит около 46 млрд долларов США. Указанный потенциальный эффект почти в 2 раза превышает возможный размер увеличения ВВП государств-членов в результате цифрового развития без реализации общей цифровой повестки [1004].

Важно отметить о подготовке доклада о развитии цифровой (Интернет) торговли ЕАЭС, формирование плана мероприятий (дорожной карты) по созданию благоприятных условий для развития цифровой экосистемы торговли. Осуществляется подготовка правовых и методических документов обеспечения процесса внедрения модели применения «регуляторных песочниц» в рамках цифровой повестки ЕАЭС, что позволит существенно ускорить получение результатов от реализации проектов[120] [1005]. Новая цифровая технология таможенного оформления товаров электронной торговли, доставляемых почтовыми операторами и экспресс-

[119] В ЕЭК сформирована структура, занимающаяся проектным управлением, создан офис управления инициативами, начали финансироваться цифровые инициативы, касающиеся поддержки и снижения издержек обеспечения таких свобод, как свобода передвижения товара и свобода передвижения трудовых ресурсов.

[120] Регуляторная песочница – это особый режим регулирования, позволяющий компаниям протестировать свои продукты в контролируемой среде, без риска нарушить законодательство. Инициатором создания таких песочниц выступает регулятор.

перевозчиками, будет протестирована в ходе экспериментов, которые планируется провести в странах Евразийского экономического союза[121] [1006].

Ядром цифровой повестки ЕАЭС и достижения эффективности и прозрачности процессов интеграционного строительства призвана стать Интегрированная информационная система. Данная система является флагманским проектом по созданию центрального звена межгосударственного информационного взаимодействия[122].

Аналитический центр при правительстве РФ отмечает, что вопросы развития евразийского интеграционного сотрудничества являются важнейшими для государств – членов ЕАЭС. На передний план в последние годы вышла именно цифровая повестка Евразийского экономического союза, определяющая круг актуальных для ЕАЭС вопросов по цифровой трансформации экономики. Ускоренная реализация цифровой повестки ЕАЭС и формирование высокотехнологичного и инновационного евразийского пространства являются основными приоритетами интеграционного развития [1002]. Запущены и реализуются пилотные проекты по приоритетным направлениям: маркировке меховых изделий[123] и

[121] Одна из целей проекта – обеспечить комфортные условия получения потребителями посылок из иностранных интернет-магазинов. В частности, документы ЕАЭС определяют особенности заполнения декларации на товары для экспресс-грузов и заявления о выпуске товаров до подачи декларации в отношении товаров электронной торговли. Также предусматривается дополнительная категория товаров, которые могут быть заявлены к выпуску до подачи декларации, что ускорит их выпуск и быструю доставку потребителям товаров электронной торговли. Кроме того, комиссия подготовила изменения, направленные на расширение возможностей применения декларации на экспресс-грузы, в том числе в отношении экспортируемых товаров. Это упростит таможенное декларирование экспортируемых экспресс-грузов и может придать определенный импульс развитию внешней электронной торговли, в том числе применительно к экспорту товаров ЕАЭС.

[122] Реализация проекта находится на критически низком уровне готовности. Из планируемых 88 общих процессов внедрено всего 15, а реально работает лишь 4 процесса.

[123] Соглашение о реализации в 2015–2016 годах пилотного проекта по введению маркировки товаров контрольными (идентификационными) знаками по товарной позиции «Предметы одежды, принадлежности к одежде и прочие изделия из натурального меха» заключено 8 сентября 2015 года в г. Гродно (Республика Беларусь). Следующим этапом создания эффективной системы прослеживаемости на пространстве ЕАЭС является расширение спектра товаров, подлежащих маркировке. В этих целях подписано Соглашение о маркировке товаров средствами идентификации в Евразийском экономическом союзе (2 февраля 2018 года, г. Алматы). В этом же году состоялся запуск нового пилотного проекта по цифровой маркировке табачных изделий в рамках ЕАЭС, в котором участвуют Российская Федерация и Казахстан. В рамках данного пилотного проекта в России внедряется маркировка табачной продукции. С марта 2019 года участники проекта подключились к системе маркировки табака. С 2019 года производители табачной продукции обязаны маркировать каждую пачку сигарет.

цифровой маркировке табачных изделий в рамках ЕАЭС, в которых участвуют Российская Федерация и Республика Казахстан.

На втором этапе реализации цифровой повестки ЕАЭС (до 2022 года) предусмотрено формирование институтов цифровой экономики и цифровых активов, а также развитие цифровых экосистем. В настоящее время осуществляется интеграция в следующие цифровые системы на основе цифровой платформы или комплексов цифровых платформ:

1) цифровая экосистема торговли в ЕАЭС;

2) экосистема цифровых транспортных коридоров ЕАЭС;

3) цифровая экосистема для обеспечения трудоустройства и занятости граждан государств – членов ЕАЭС.

Советом Евразийской экономической комиссии от 13 июля 2018 г. № 17 было издано распоряжение «О проработке инициативы по созданию экосистемы цифровых транспортных коридоров Евразийского экономического Союза» [1007]. Разработаны концепция создания экосистемы цифровых транспортных коридоров в ЕАЭС [1008], а также верхнеуровневый план мероприятий по реализации проекта «Экосистема цифровых транспортных коридоров ЕАЭС» [1009]. Важно упомянуть, что решению задач по объединению транспортно-логистических платформ в единую экосистему будет способствовать реализация пилотных проектов с последующими запусками во всех государствах – членах ЕАЭС по следующим направлениям:

а) бесшовная инфраструктура перемещения грузов;

б) бесшовное информационное сопровождение перевозки [1010].

Совместное исследование группы Всемирного банка и Евразийской экономической комиссии по внедрению цифровой повестки ЕАЭС до 2025 года [1011] показало целесообразность укрепления так называемых «аналоговых» основ трансформации. В этой связи важно достижение политического консенсуса и обеспечение руководством преобразований на высшем уровне, а также укрепление соответствующих институтов управления; создание гармонизированного законодательства и нормативной правовой базы для интеграции и осуществления цифровой трансформации. Требуется вовлечение в процесс различных организаций, в том числе органов государственной власти, частного сектора, исследовательских и образовательных учреждений, средств массовой информации, а также широких слоев населения. По их мнению, необходимо наличие

опытного управленческого и технического персонала, постоянно совершенствующего необходимые навыки, а также проведение последовательной политики по развитию навыков широких слоев населения и повышению осведомленности общества об ожидаемых дивидендах от цифрового развития. Цифровые дивиденды предполагают: ускорение экономического роста, создание новых рабочих мест; улучшение государственных услуг. Необходима технологическая совместимость, интероперабельность и масштабируемость цифровых инфраструктур, платформ и решений, обязательных для эффективной, инклюзивной и безопасной цифровой экономики.

Среди основных направлений создания цифрового пространства ЕАЭС целесообразно выделить следующие: обеспечение усиления процессов экономической интеграции и международного сотрудничества; создание благоприятной среды для внедрения региональных цифровых инициатив; создание общей цифровой инфраструктуры и цифровых платформ; цифровизация ведущих экономических отраслей экономики и рынков стран-участников. Кроме того, группой Всемирного банка и ЕЭК представлены механизмы осуществления преобразований в этих направлениях, в том числе создание общей благоприятной нормативной правовой базы, государственно-частных партнерств для реализации приоритетных инициатив, развитие диалога между всеми заинтересованными сторонами в цифровых экосистемах, продвижение лучших цифровых практик и решений.

Среди объективных рисков, связанных с отсутствием продвижения повестки формирования цифровой экономики эксперты выделяют «утечку мозгов» из региона, усиление влияния глобальных игроков на цифровом пространстве ЕАЭС, поступательная потеря конкурентоспособности товаров и услуг и угроза цифровому суверенитету региона.

На основании вышеуказанных фактов экспертами Всемирного банка были разработаны ключевые рекомендации развития Цифрового пространства и реализации цифровой повестки ЕАЭС до 2025 года, осуществление которых приведет к ускорению экономического роста, созданию новых рабочих мест, улучшению качества государственных услуг и росту конкурентоспособности стран ЕАЭС, включая:

а) создание институциональной и правовой основы Цифровой повестки, распределение ответственности и полномочий между органами управления на интеграционном и национальном уровнях;

б) предоставление финансовых ресурсов для реализации Цифровой повестки с учетом долгосрочного и комплексного характера преобразований;

в) обеспечение общедоступных образовательных программ развития цифровой грамотности населения, а также специальных программ, направленных на повышение уровня цифровых навыков среди широких слоев общества;

г) обеспечение широкополосного доступа в Интернет, поддержки разработки и внедрения безопасных и надежных трансграничных межсекторальных цифровых платформ и цифровых решений.

Важно отметить, что на страновом уровне государства ЕАЭС разрабатывают национальные концепции и программы цифровизации, целью которых является имплементация в национальных экономических системах лучших международных практик, направленная на повышение конкурентоспособности государств – членов Евразийского экономического союза.

Важным наднациональным институтом, определяющим актуальные направления цифровой трансформации экономики Республики Беларусь, формирование соответствующей экосреды, является Союзное государство. В данном контексте представляется целесообразным отметить согласование в 2021 году основных направлений реализации положений Договора о создании Союзного государства на 2021–2023 годы и 28 Союзных программ [1012], среди которых цифровую направленность имеют договоренности:

1) о гармонизации подходов к обеспечению информационной безопасности, созданию механизма взаимного признания результатов аудита в области информационной безопасности, применению средств трансграничного контроля целостности и подтверждения подлинности при обмене электронной информацией;

2) гармонизации законодательства Российской Федерации и Республики Беларусь в сфере ПОД/ФТ для финансового сектора и реализации совместных мероприятий в данной области;

3) интеграции платежных систем в области национальных систем платежных карт, систем передачи финансовых сообщений и расчетов, внедрения международного стандарта финансовых сообщений ISO 20022, системы быстрых платежей, развития финансовых технологий, гармонизированных подходов в области надзора и наблюдения за платежными системами;

4) гармонизации требований в области защиты прав потребителей финансовых услуг и инвесторов, а также предотвращения недобросовестных практик на финансовом рынке;

5) интеграции информационных систем государственных контролирующих органов по прослеживаемости товаров;

6) интеграции информационных систем по маркировке товаров;

7) интеграции информационных систем государственных контролирующих органов в части ветеринарного и карантинного фитосанитарного контроля;

8) интеграции информационных систем транспортного контроля государственных контролирующих органов;

9) формировании единых принципов функционирования единого рынка связи и информатизации, включая гармонизацию использования электронных документов и электронной подписи, а также предоставление государственных услуг в электронной форме.

Заключение

Таким образом, для ЕАЭС характерно формирование начальных уровней регулирования цифровой экономики, акцентированных на блоках выработки общей стратегии, внедрения и регулирования отдельных цифровых инноваций и концепций. В отличие от ЕС, практически отсутствуют общие институциональные блоки регулирования финансового рынка и защиты киберпространства. Кроме того, отсутствуют общие подходы к внедрению современных цифровых концепций, включая AI/ML, IoT, Big Data, Блокчейн и пр. Это может свидетельствовать о низком уровне наднационального взаимодействия и возможном отсутствии доверия между странами ЕАЭС в данных сегментах государственного регулирования.

Отдельные направления (например, в сфере информационной безопасности на уровне центральных банков стран ЕАЭС) находятся в ведении специализированных государственных институтов Российской Федерации. Таким образом, наднациональное регулирование цифровизации (уровня Евразийской экономической комиссии) замещается межведомственным (линейным) взаимодействием конкретных министерств и ведомств России. Данный факт может свидетельствовать о низком уровне регуляторной интеграции стран ЕАЭС.

На уровне Союзного государства взаимодействие по унификации и гармонизации отдельных цифровых направлений государственного регулирования, включая киберзащиту, финансовый сектор, информационные системы, в настоящее время также находится на начальной стадии.

Глава 4

АДАПТАЦИЯ БЕЛОРУССКОЙ ЭКОНОМИКИ К УГРОЗАМ И РИСКАМ, СВЯЗАННЫМ С ЦИФРОВОЙ ЭКОНОМИКОЙ

Для Республики Беларусь характерен малый открытый тип экономики, что предполагает влияние мировых тенденций цифровизации на ее экономическое развитие, конкурентоспособность как продукции, так и экономической модели в целом, проблематику обеспечения экономической безопасности, связанную с внедрением новых технологий в ключевые сферы жизнедеятельности государства. В данном контексте представляется жизненно важным для национальной экономики разработать модель ее цифровизации с учетом объективных и возможных рисков и угроз, связанных с внедрением цифровых технологий как в секторальном, так и макроэкономическом разрезе, а также международного опыта регулирования и наднациональных механизмов, формируемых в рамках ЕАЭС и Союзного государства.

4.1. Цифровая экономика и ее инфраструктура в Республике Беларусь: эволюция формирования, тенденции, механизмы-драйверы

С учетом открытого характера национальной экономики Республики Беларусь страна вынуждена адаптировать проводимую политику к современным цифровым тенденциям с целью сохранения конкурентоспособности производимой продукции на мировых рынках. Данная адаптация предполагает формирование современной цифровой инфраструктуры как базиса для цифровизации национальной экономики.

Следует выделить ряд этапов развития цифровой инфраструктуры и соответствующей трансформации экономики.

Базовый этап (2005–2015 годы). Отличительной характеристикой институциональной среды цифровой экономики Республики

Беларусь является наличие специального инновационного кластера, резиденты которого занимаются разработкой программных продуктов и предоставлением IT-услуг, – Парка высоких технологий (ПВТ), созданного в 2005 году[1]. Данный институт регуляторной среды представляет собой особую экономическую зону со специальным налогово-правовым режимом, способствующую благоприятному развитию IT-бизнеса. В рамках представленной модели ПВТ функционально является составным элементом как технологического, так и финансового блока, поскольку посредством кластера государство стимулирует как технологические, так и FinTech направления развития (табл. 4.1).

С учетом международного опыта формирования институциональной экосистемы (табл. 3.1, 3.2, 3.3, 3.5, 3.6), в разрезе полноты

[1] Декретом Президента Республики Беларусь № 12 от 22 сентября 2005 года «О Парке высоких технологий», направленным на создание благоприятных условий для повышения конкурентоспособности отраслей экономики Республики Беларусь, основанных на новых и высоких технологиях, дальнейшего совершенствования организационно-экономических и социальных условий для проведения разработок современных технологий и увеличения их экспорта, привлечения в эту сферу отечественных и иностранных инвестиций путем создания Парка высоких технологий (ПВТ). Основными направлениями деятельности Парка высоких технологий являются: экспорт информационно-коммуникационных технологий и иных новых и высоких технологий, исключительные права на результаты интеллектуальной деятельности в сфере новых и высоких технологий; содействие привлечению отечественных и иностранных инвестиций в развитие сферы новых и высоких технологий; разработка и внедрение информационно-коммуникационных и иных новых и высоких технологий в Республике Беларусь; содействие кадровому обеспечению инновационного развития национальной экономики, развитие образования в сфере информационно-коммуникационных технологий; формирование институциональной среды, стимулирующей инновационную деятельность, в том числе содействие развитию системы венчурного финансирования, развитие стартап-движения. С целью выполнения поставленных задач предусмотрены такие льготы и преференции резидентам ПВТ, как их освобождение от налога на прибыль, налога на добавленную стоимость по оборотам от реализации товаров (работ, услуг), оффшорного сбора в отношении объектов обложения оффшорным сбором при расчетах за рекламные, маркетинговые, посреднические услуги, а также при выплате (передаче) дивидендов их учредителям (участникам), части прибыли, начисленной собственнику их имущества. Кроме того, доходы физических лиц, полученные в течение календарного года от резидентов Парка высоких технологий по трудовым договорам (контрактам), а также доходы резидентов Парка высоких технологий – индивидуальных предпринимателей, являющихся плательщиками подоходного налога с физических лиц, доходы в виде дивидендов облагаются подоходным налогом с физических лиц по ставке 9%.

охвата, глубины детализации, комплексности и временного лага имплементации блоков стратегии (СЦ), механизмов внедрения и регулирования отдельных цифровых инноваций и концепций (ИБЦИ), регулирования финансового рынка (ИБФР) и защиты киберпространства (ИБЗК) представляется возможным провести следующий сравнительный анализ (рис. 4.1, с. 132).

Таблица 4.1

Институциональная матрица экосистемы цифровой экономики Республики Беларусь (разработано автором)

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2005–2015 годы)	СЦ	Стратегия развития информационного общества на период до 2015 года (Постановление Совета Министров Республики Беларусь от 9 августа 2010 года № 1074)	Прав	Формирование базового комплекса электронного правительства, включая общегосударственную автоматизированную информационную систему, систему межведомственного электронного документооборота, систему управления открытыми ключами проверки электронной цифровой подписи, единое расчетное информационное пространство
		Национальная программа ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы, отраслевые и региональные программы информатизации		
	ИБЦИ	Декрет «О Парке высоких технологий» (№ 12 от 22 сентября 2005 года)	ПР	Сектор ИКТ
		Закон «Об электронном документе и электронной цифровой подписи» (от 28 декабря 2009 года № 113-З)	Пар, Прав	Электронный документооборот
		СООО «Белорусские облачные технологии», 2012	Минсвязи, ОАЦ	Рынок облачных решений
	ИБФР	Указ «О развитии цифровых банковских технологий» (№ 478, декабрь 2015 года)	Нацбанк, ПР	Развитие системы безналичных платежей для физических и юридических лиц

Продолжение табл. 4.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2016–2020 годы)	СЦ	Стратегия развития информатизации в Республике Беларусь на 2016–2022 годы (Постановление Совета Министров 03.11.2015 № 26)	Прав	Внедрения передовых ИКТ во все сферы человеческой жизнедеятельности; создание, модернизация и внедрение специализированных автоматизированных информационных систем (АИС); развитие Интернет-платформ (краудфандинга)
		Государственная программа развития цифровой экономики и информационного общества на 2016 – 2020 годы		
	ИБЦИ	Совет по развитию цифровой экономики, Постановление Совета Министров Республики Беларусь от 28 февраля 2018 года № 167	Минсвязи, Прав	Координация деятельности по реализации государственной политики в сфере цифровой трансформации экономики
		Перевод некоторых административных процедур для юридических лиц и индивидуальных предпринимателей в разряд «цифровых» через единый портал электронных услуг (Распоряжение Совета Министров, апрель 2020 года)	Прав	Цифровое правительство
		Белорусская интегрированная сервисно-расчетная система (БИСРС), 2016	Минсвязи, Прав	
		Технический комитет по стандартизации ТК ВУ 38 «Цифровая трансформация», 2018	Прав, Госстандарт	Государственные стандарты в сфере цифровой трансформации промышленности
		Решение Правления ОАО «Небанковская кредитно-финансовая организация «ЕРИП» (протокол № 41) о предоставлении на платной основе данных о клиентах, их представителях с целью обновления (актуализации) данных (октябрь 2021 года)	ЕРИП	Формирование зачатков национального рынка Big Data
	ИБФР	Декрет «О развитии цифровой экономики» (№ 8 от декабря 2017 года)	ПР	Расширение разрешенных видов деятельности для резидентов ПВТ, Блокчейн и криптовалюты, ICO и смарт-контракты

Продолжение табл. 4.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2016–2020 годы)	ИБФР	Постановление Правления Национального банка Республики Беларусь № 108 «Об одобрении стратегии развития цифрового банкинга на 2016 – 2020 годы»	Нацбанк	Цифровой банкинг
		Небанковская кредитнофинансовая организация «Единое расчетное информационное пространство», 2016	Нацбанк	Расчетное обслуживание юридических и физических лиц
		Постановление Правления Национального банка Республики Беларусь № 497 «Об утверждении инструкции о порядке функционирования межбанковской системы идентификации» (МСИ), 2016	Нацбанк	Система удаленной идентификации клиентов без их личного присутствия и предоставления им услуг с помощью цифровых каналов обслуживания
		Постановление Правления Национального банка Республики Беларусь № 280 «О функционировании информационной сети, построенной с использованием технологии блокчейн» (июль 2017 года)	Нацбанк	Блокчейн
		Постановление Правления Национального банка Республики Беларусь № 12 «Об утверждении Инструкции о порядке формирования и ведения реестра банковских гарантий» (январь 2017 года)		
		Постановление Правления Национального банка Республики Беларусь № 540 «О некоторых вопросах функционирования системы мгновенных платежей и проведения мгновенных платежей» (ноябрь 2018 года)	Нацбанк	Создание системы мгновенных межбанковских расчетов Национального банка

Продолжение табл. 4.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2016–2020 годы)		Указ № 148 «О цифровых банковских технологиях», (апрель 2019 года)	Нацбанк, ПР	Расширение списка организаций, имеющих право использовать МСИ для идентификации своих клиентов; формирование нормативной базы для смарт-контрактов
		Постановление Правления Национального Банка Республики Беларусь № 379 «Об утверждении инструкции об использовании программно-аппаратных средств и технологий, проведении процедур удаленной идентификации, удаленного обновления (актуализации), 2019 год	Нацбанк	Регулирование отдельных аспектов удаленной идентификации клиентов
		Указ № 175 «О страховании» (май 2019 года)	ПР	Регламентация заключения договоров добровольного страхования в электронном виде (как на официальном сайте организации, так и уполномоченными организациями (банками)
		Постановление Правления Национального банка Республики Беларусь № 428 «О совершении и (или) исполнении юридически значимых действий посредством смарт-контрактов» (декабрь 2020 года)	Нацбанк	Смарт-контракты
Второй уровень (2021–н. в.)	СЦ	Государственная программа «Цифровое развитие Беларуси на 2021–2025 годы»	Прав	Реализация концептов «Умный город», «Промышленность 4.0», создание не менее семи государственных цифровых платформ
	ИБЦИ	Указ Президента № 107 «О биометрических документах» (март 2021 года)	ПР	Цифровое правительство

Окончание табл. 4.1

Период	Институциональный блок	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Второй уровень (2021–н.в гг.)	ИБЦИ	Агентство сервисизации и реинжиниринга, постановление Совета Министров № 646 «О снижении административной нагрузки и цифровизации административных процедур» (ноябрь 2021 года)	Прав	
	ИБФР	Указ № 196 «О сервисах онлайн-заимствования и лизинговой деятельности», 2021 год	Нацбанк, ПР	Сервисы онлайн-заимствования
		Постановление Правления Национального банка Республики Беларусь № 310 «О деятельности операторов сервисов онлайн-заимствования» (октябрь 2021 года)	Нацбанк	Требования к сервису онлайн-заимствования, которые касаются идентификации и аутентификации юридических и физических лиц
		Проект Закона Республики Беларусь «О платежных системах и платежных услугах», в стадии разработки	Нацбанк	Регулирование рынка цифровых платежных систем
		Стандарт ISO 20022 для платежной системы, в стадии разработки	Нацбанк	Международный стандарт обмена электронными сообщениями между организациями финансовой отрасли
		Стандарт по платежным API, в стадии разработки	Нацбанк	Развитие открытых банковских API
		Проект национальной CBDC, в стадии разработки	Нацбанк	Проект внедрения цифрового рубля

Примечание. Сокращения: СЦ – стратегия цифровизации; ИБЦИ – институциональный блок механизмов внедрения и регулирования отдельных цифровых инноваций и концепций; ИБФР – институциональный блок регулирования финансового рынка; ИБЗК – институциональный блок защиты киберпространства; ПР – Президент Республики Беларусь, Прав – Правительство Республики Беларусь, Пар – Парламент Республики Беларусь; СБ – Совет Безопасности Республики Беларусь; ОАЦ – Оперативно-аналитический центр; Минсвязи – Министерство связи и коммуникаций Республики Беларусь; Нацбанк – Национальный банк Республики Беларусь; Госстандарт – Государственный комитет по стандартизации Республики Беларусь.

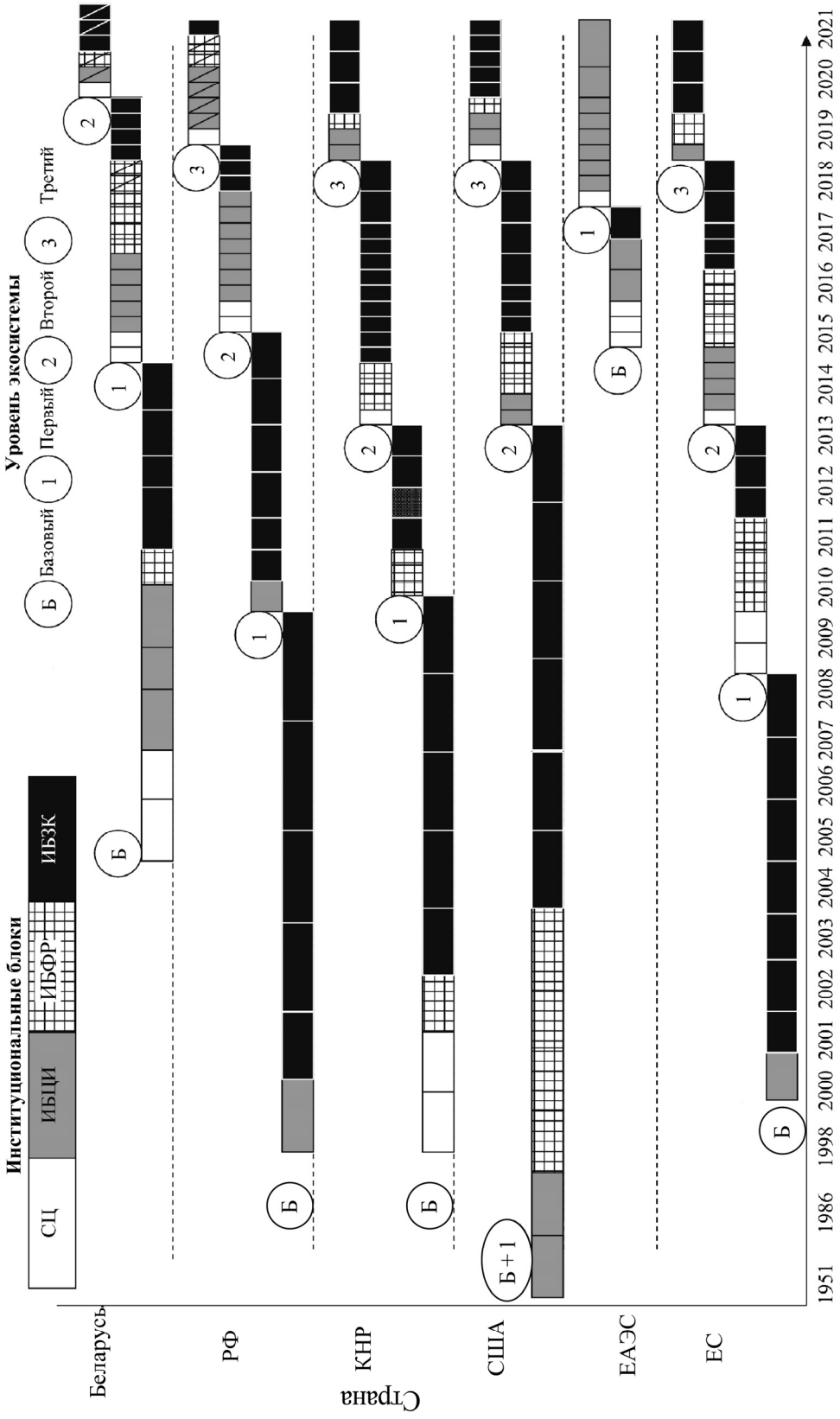


Рис. 4.1. **Графический анализ регуляторной институциональной экосистемы Республики Беларусь, США, Российской Федерации (РФ), КНР и ЕС** (разработано автором)

Эталонным образцом системного подхода к формированию институциональной экосистемы цифровой экономики является ЕС. Относительно данного интеграционного объединения отмечаем отставание как в комплексности принимаемых механизмов регулирования цифровой экосреды, так и интенсивности их внедрения. Республика Беларусь отстает в цифровизации не только от ведущих технологических государств и интеграционных объединений, но и Российской Федерации.

В 2009 году в Беларуси установлены правовые основы применения электронных документов, определены основные требования, предъявляемые к ним, а также правовые условия использования электронной цифровой подписи в электронных документах, при соблюдении которых электронная цифровая подпись в электронном документе является равнозначной собственноручной подписи в документе на бумажном носителе[2].

Развитие информатизации в Республике Беларусь в течение 2011–2015 годов осуществлялось в соответствии со Стратегией развития информационного общества до 2015 года[3]. В результате реализации данной стратегии создан базовый комплекс электронного правительства, включающий такие компоненты, как общегосударственная автоматизированная информационная система, система межведомственного электронного документооборота, Государственная система управления открытыми ключами проверки электронной цифровой подписи, единое расчетное информационное пространство и другие. В социально-трудовой сфере Республики Беларусь стал функционировать комплекс государственных информационных систем и государственных информационных ресурсов[4] [1013].

---

[2] В соответствии с Законом Республики Беларусь от 28 декабря 2009 года № 113-З «Об электронном документе и электронной цифровой подписи».

[3] Утверждена Постановлением Совета Министров Республики Беларусь от 9 августа 2010 г. № 1074 и разработанными для ее выполнения Национальной программой ускоренного развития услуг в сфере информационно-коммуникационных технологий на 2011–2015 годы, отраслевыми и региональными программами информатизации.

[4] Государственная информационная система социальной защиты, Информационно-вычислительная система государственной службы занятости, Автоматизированная система управления индивидуальным (персонифицированным) учетом в системе государственного социального страхования, Автоматизированная система управления профессиональным пенсионным страхованием, портал государственной службы занятости и корпоративный портал Фонда социальной защиты населения.

В 2012 году основано совместное общество с ограниченной ответственностью «Белорусские облачные технологии» (компания beCloud), представляющие интересы государства на рынке услуг облачных технологий и являющиеся одним из ведущих поставщиков облачных решений, IT-инфраструктуры и хостинга в Беларуси. Провайдер оказывает услуги на базе собственных телекоммуникационных сетей и дата-центра, используя, в том числе модели IaaS, SaaS, PaaS, DaaS[5]. На базе единой республиканской сети передачи данных и beCloud создана республиканская платформа, которая представляет собой программно-технический комплекс для распределенной обработки данных, реализующий технологии облачных вычислений и обеспечивающий взаимодействие с внешней средой. СООО «Белорусские облачные технологии» в качестве оператора республиканской платформы имеет право запрашивать у государственных органов и организаций информацию о текущем и перспективном состоянии оборудования для доступа к информационным услугам или информационным системам и ресурсам, определять и размещать в свободном доступе в Интернете формы и содержание технических условий на подключение к республиканской платформе, на перенос в республиканский центр обработки данных оборудования или информационных систем и ресурсов, утверждать стандартные формы договоров оказания услуг с использованием республиканской платформы, заключаемых с госорганами и организациями [1014].

С целью внедрения современных банковских технологий в декабре 2015 года принят Указ Президента «О развитии цифровых банковских технологий», направленный на развитие системы безналичных платежей для физических и юридических лиц, результатом чего стало создание Небанковской кредитно-финансовой организации «Единое расчетное информационное пространство» (ЕРИП).

Первым этапом (2016–2020 годы) данного процесса в Республике Беларусь можно считать принятие государственной программы развития цифровой экономики и информационного общества на 2016–2020 годы [1015]. Программа включает такие подпрограммы, как «Информационно-коммуникационная инфраструктура», «Инфраструктура информатизации» и «Цифровая трансформация».

[5] О компании beCloud. – Режим доступа: https://becloud.by/about-company/. – Дата доступа: 15.02.2022.

В рамках программы предусматривалось, в том числе, развитие Интернет-платформ (краудфандинга) в качестве инструмента взаимодействия потребителей и производителей товаров и услуг, инвесторов и соискателей инвестиций[6].

В декабре 2017 года подписан Декрет № 8 «О развитии цифровой экономики» [1016], цель которого – создание условий для привлечения мировых IT-компаний в Беларусь, открытия ими своих представительств, центров разработок и создания конкурентоспособного высокотехнологического цифрового продукта (услуги) с высокой добавленной стоимостью. Кроме того, задачами документа являлось обеспечение инвестиций в будущее (IT-кадры и образование) и внедрение новейших финансовых инструментов и технологий. Помимо работы Парка высоких технологий, Декрет № 8 также затрагивал новые направления развития цифровой сферы, такие как Блокчейн и криптовалюты[7]. Документ позволил заключать внешнеэкономические сделки в электронном виде с использованием Интернета, отменил ряд ограничений по операциям резидентов ПВТ с электронными деньгам, упразднил разрешительный порядок на открытие счетов в банках-нерезидентах, внедрил использование институтов английского права.

---

[6] Вследствие отсутствия специализированного законодательства, организация краудфандинга в Беларуси сталкивается со следующими юридическими проблемами: риск неверной идентификации, так как в основном площадкой для краудфандинга является Интернет, то есть риск столкнуться с виртуальными мошенниками, которые могут использовать информацию о третьих лицах, без уведомления последних; качество проверки бизнес-проекта – проверка качества документов, плана и реализации проектов осуществляется исключительно краудфандинговой площадкой. Инвесторы как таковые не вовлечены в данный процесс, соответственно, здесь могут возникнуть недопонимания и несоответствие ожиданиям инвесторов; отсутствие требований к контролю за инвестированием – законодательством либо иным способом не определены методы, которые смогут гарантировать передачу средств непосредственно в данный проект. Риск увеличивается, если краудфандинговая площадка работает с проектами различных направленностей.

[7] Декрет значительно расширил перечень разрешенных видов деятельности для резидентов ПВТ. В обновленном списке – разработки в сфере биотехнологий, медицины, авиационных и космических технологий, системы беспилотного управления транспортом, киберспорт, биржи криптовалют и др. При этом отсутствуют ограничения на объем выручки от дополнительных видов деятельности. Кроме того, данным правовым документом легализованы криптовалюты, ICO и смарт-контракты. В ПВТ начали функционировать криптобиржи и криптообменники, а у граждан и юридических лиц создана возможность майнить, покупать, дарить, обменивать криптовалюту, более того, до 2023 года деятельность по майнингу, приобретению и отчуждению токенов для физических лиц и резидентов ПВТ не облагается налогами.

С целью институционального развития цифровизации национальной экономики, осуществления общей координации данной деятельности, в 2018 году создан Совет по развитию цифровой экономики, цель которого – координация деятельности по реализации государственной политики в сфере цифровой трансформации экономики и развития информационно-коммуникационных технологий[8]. Основными задачами Совета являются:

1) определение целей и задач цифровой трансформации национальной экономики;

2) установление приоритетов внедрения цифровых технологий для производственных отраслей, сфер торговли и услуг, социальной сферы с учетом последних достижений в сфере информационно-коммуникационных технологий и развития глобального цифрового пространства;

3) формирование благоприятной правовой и регуляторной среды для развития национальной цифровой экономики;

4) стимулирование перехода к передовым цифровым технологиям в различных сферах экономики и общественных отношений;

5) формирование и развитие современной цифровой инфраструктуры и создание цифровых платформ различного назначения;

6) развитие национальной индустрии информационно-коммуникационных технологий;

7) вопросы эффективности работы республиканских органов государственного управления, иных государственных организаций, подчиненных Правительству Республики Беларусь, местных исполнительных и распорядительных органов, иных организаций в сфере развития цифровой экономики;

8) реализация инвестиционных проектов и проектов государственно-частного партнерства в области информационно-коммуникационных технологий;

9) международное сотрудничество в сфере цифровой экономики [1017]. Организационное и информационное обеспечение деятельности Совета осуществляется Министерством связи и информатизации.

В целях формирования условий, содействующих развитию информационного общества, разработан ряд новых образовательных

[8] Постановление Совета Министров Республики Беларусь от 28 февраля 2018 г. № 167.

стандартов, планов и программ подготовки специалистов в области ИКТ. Созданы информационная система электронного зачисления в учреждения высшего образования, информационные сервисы для обеспечения взаимодействия учреждений образования, органов управления и населения, а также комплекс мер по защите информации в отраслевых информационных системах Министерства образования Республики Беларусь [1018]. В учреждениях образования реализуется проект «Электронная школа» (участие в котором, по предварительным оценкам, в 2020 году принимают около 80% школ).

Активно внедряются информационные технологии в системе здравоохранения. Функционируют система «Telemedicine» по цифровой маммографии, единая «Telemedicine» система г. Минска по цифровой флюорографии. К системе электронных рецептов подключено уже более 600 учреждений. Ведется активная работа по формированию в стране централизованной системы электронного здравоохранения, в рамках которой планируется переход к использованию интегрированных электронных медицинских карт, содержащих всю медицинскую информацию о пациенте, начиная с его рождения. Осуществляется разработка центральной программной платформы единой электронной инфосистемы здравоохранения Беларуси[9], которая представляет собой интегрированную информационную систему, обеспечивающую хранение и обработку медицинской информации в области здравоохранения. В нее включены базы (банки) данных, реестры (регистры) в здравоохранении, единый электронный архив мединформации о пациентах, иные информационные ресурсы, государственной статистики здравоохранения. Предполагается разработка различных уровней доступа пользователей к информации. Основной элемент системы – электронная медицинская карта пациента [1019].

Введен в эксплуатацию единый реестр лицензий, с июля 2020 г. сведения из него предоставляются на едином портале электронных услуг. Выполнены работы по созданию, модернизации и внедрению специализированных автоматизированных информационных систем, направленных на цифровую трансформацию процессов управления: АИС «Расчет налогов», АИС «Персонифицированный учет», АИС

[9] Реализуется в рамках Соглашения о займе (проект «Модернизация системы здравоохранения Республики Беларусь») между Республикой Беларусь и Международным банком реконструкции и развития, ратифицированном Законом Республики Беларусь от 10 апреля 2017 года № 21-З.

«Контрольная деятельность», единая автоматизированная информационная система таможенных органов (в результате доля таможенных деклараций, поданных в электронном виде, достигла 99,99%), информационные системы охраны границы и пограничного контроля (за пять лет к использованию подключены 26 объектов органов пограничной службы) и др.

В целом в рамках утвержденной «Стратегии развития информатизации в Республике Беларусь на 2016–2022 годы»[10] реализованы проекты, направленные на развитие эффективной и прозрачной системы государственного управления посредством внедрения ИКТ; совершенствование системы управления процессами информатизации и правового их регулирования; создание и внедрение государственной системы идентификации субъектов информационных отношений; дальнейшее формирование единого информационного пространства для оказания электронных услуг на основе интеграции информационных систем. Общая сумма бюджетного финансирования составила 175,5 млн руб.

В июле 2017 года постановлением Правления Национального банка была принята Инструкция об общих принципах функционирования информационной сети, построенной с использованием технологии Блокчейн. С октября 2017 года в эксплуатацию введена технологическая платформа, построенная на основе технологии Блокчейн – «Реестр банковских гарантий». Назначение системы – сбор и раскрытие информации о выданных банковских гарантиях, обслуживание процессов их выдачи[11].

В апреле 2020 года Советом Министров принято распоряжение о переводе некоторых административных процедур для юридических лиц и индивидуальных предпринимателей в разряд «цифровых» через единый портал электронных услуг[12]. Создана

---

[10] Утверждена постановлением Совета Министров 03.11.2015 № 26.

[11] В ноябре 2018 года Приорбанк провел первую в Беларуси сделку (между Мозырским НПЗ и Райффайзенбанком) с использованием технологии Блокчейн. По поручению Мозырского НПЗ Приорбанк выпустил международную банковскую гарантию для российской компании на платформе R-chain. Для операции использовалось ПО Райффайзенбанка, в разработке которого участвовали специалисты белорусского банка (В Беларуси впервые провели международную сделку-гарантию на блокчейне. – Режим доступа: https://tech.onliner.by/2018/11/08/blockchain-13. – Дата доступа: 08.11.2018).

[12] Единый перечень административных процедур, осуществляемых государственными органами и иными организациями в отношении юридических лиц и индивидуальных предпринимателей, утвержден постановлением Совета Министров № 156 от 17 февраля 2012 года. Речь идет о 147 процедурах. Предполагается, что они станут электронными в 2020–2024 годах.

Белорусская интегрированная сервисно-расчетная система (БИСРС) – комплекс информационных систем и ресурсов, предназначенный для оказания пользователям (физическим и юридическим лицам) государственных услуг и административных процедур в электронной форме с применением идентификационных карт (ID-карт).

Функционирует автоматизированная система финансовых расчетов, которая предназначена для формирования, контроля, ведения учета и отчетности по исполнению бюджетов всех уровней. Создано единое расчетное и информационное пространство для осуществления платежей физическими и юридическими лицами. Функционирует автоматизированная система межбанковских расчетов, система безналичных расчетов по розничным платежам. Банки активно внедряют мобильные приложения, позволяющие держателям банковских платежных карточек осуществлять платежи с использованием мобильных устройств [1020].

Отмечаем начало использования технологий IoT в управлении городской инфраструктурой г. Минска[13], в транспорте (система электронного сбора платы за проезд BelToll) и, частично, – в промышленности («БелАЗ» оснащает свои изделия датчиками износа). В 2016 году РУП «Белтелеком» начато оказание услуги «Умный дом», абонентская база которой составила около 74 тыс. абонентов [1021]. В 2019 году разработана и утверждена типовая концепция развития «умных городов» в Республике Беларусь, которая в дальнейшем будет адаптирована и масштабирована на указанные одиннадцать городов (районов) страны. В качестве пилотного проекта разработаны концепция «Умный город» (адаптация типового решения) для города Орши и Оршанского района и план («дорожная карта») ее реализации в соответствии с подпрограммой «Умный город» Программы развития Оршанского района на период до 2023 года[14], утвержденной Указом Президента Республики Беларусь от 31 декабря 2018 г. № 506 [1020].

В 2016–2017 годах реализован пилотный проект на основе технологий Smart Grid электрических сетей (РЭС) в Бобруйском

[13] В рамках интеллектуальной транспортной системы г. Минска функционирует ряд элементов: автоматизированная система управления дорожным движением, система фото- и видеофиксации нарушений правил дорожного движения, система управления общественным транспортом и иные [1020].

[14] Утверждена Указом Президента Республики Беларусь от 31 декабря 2018 года № 506.

сельском районе филиала «Бобруйские электрические сети» РУП «Могилевэнерго» [1020]. По состоянию на 2020 год, 99% от общего количества подстанций напряжением 35–110 кВт оснащены удаленной сигнализацией и 88% – удаленным управлением. При этом все указанные подстанции оснащены средствами телемеханики. Продолжается создание полномасштабной автоматизированной системы контроля и учета электрической энергии, которая предназначена для сбора, обработки, хранения и визуализации информации о производстве, импорте, экспорте, передаче (распределении) и продаже (сбыту) электрической энергии (мощности).

На уровне цифровизации банковского сектора Национальным банком стратегически определены шесть укрупненных приоритетных направлений развития, включая развитие платежного пространства; внедрение удаленной идентификации; внедрение открытых API; расширение использования технологий распределенных реестров; Big Data, AI/ML; кибербезопасность [1022].

В 2018 году создан технический комитет по стандартизации ТК BY 38 «Цифровая трансформация», разрабатывающий государственные стандарты Республики Беларусь в сфере цифровой трансформации промышленности (в частности, СТБ IEC PAS 63088 «Умное производство. Модель эталонной архитектуры Индустрии 4.0 (RAMI 4.0)») [454]. В 2019 году начаты работы по интероперабельности в Беларуси, одним из ключевых стандартов определен ISO/IEC 33001 (оценка процесса. Концепции и терминология)[15]. В План государственной стандартизации 2019 года включены два стандарта: ISO 8000-2-2019 «Качество данных. Словарь» и «Цифровая трансформация. Термины и определения».[16] Дорожная карта разработки цифровых стандартов включает такие направления, как бизнес-процессы, данные, разработка приложений, управление технологиями в организации и проектами. С 2021 года действуют разработанные в рамках ТК BY 38 государственные стандарты на

[15] Предоставляет хранилище для ключевой терминологии, относящейся к оценке процесса. Он дает общую информацию о существующих концепциях оценки процесса, ее применении для оценки достижения характеристик качества процесса и его управления.

[16] Стандарты относятся к терминологии. Первый является международным, и его требуется кастомизировать в стране, второй необходим для установления процессных терминов, характеризующих цифровую трансформацию в Республике Беларусь. Его задачей является обеспечение принимаемых в настоящее время решений основными понятиями, словарными определениями.

термины и определения и качество данных в области цифровой трансформации.

На уровне коммерческих компаний важно отметить получение в 2017 году компанией А1 разрешения на запуск узкополосной сети NV-IoT, основными характеристиками которой являются большая емкость сети, высокое проникновение сигнала, широкая область применения (от внедрения интеллектуальных городских систем до управления домашними устройствами), экономичность, энергоэффективность. Кроме того, планируется запустить единую платформу, в которую будут поступать данные от каждого смарт-устройства, а также приложение, позволяющее дистанционного управлять приборами.

В масштабах страны в данный период (с 2016 по 2020 год) обеспечена инфраструктура подключения по технологии пассивных оптических сетей (GPON) всех квартир городской многоэтажной жилой застройки Беларуси, количество абонентов, подключенных по технологии GPON, достигло 2,15 млн человек, а общее количество абонентов увеличилось до 2,74 млн [1021]. Численность абонентов, подключенных к широкополосному доступу в сеть Интернет, составило 3,26 млн человек (на конец 2020 года). Широкополосным доступом в сеть Интернет обеспечены все учреждения образования в Республике Беларусь.

Обеспечен охват 92,0% населения услугами сотовой подвижной электросвязи стандарта LTE (4G). Пользователями услуг электросвязи по технологии LTE (4G) являются около 5 млн абонентов [1023].

Количество Интернет-пользователей в Республике Беларусь составило 83,1 единицы на 100 жителей. Доля домохозяйств, имеющих доступ к сети Интернет, равна 82%.

Вторым этапом (2021 год – н. в.) процесса цифровизации в Республике Беларусь можно считать принятие Советом Министров Республики Беларусь в феврале 2021 года государственной программы «Цифровое развитие Беларуси» на 2021–2025 годы, направленной на внедрение передовых информационных технологий в отрасли национальной экономики и сферы жизнедеятельности общества. Программой предусматривается выполнение мероприятий по созданию (развитию) современной информационно-коммуникационной инфраструктуры, внедрению цифровых инноваций в

отрасли экономики и технологий Smart City (умных городов)[17]. Программа должна к 2025 году охватить 17 городов и регионов, количество подключенных датчиков достигнет 3,7 млн единиц [1021].

Ожидается, что в результате реализации указанной программы будет создано не менее 7 государственных цифровых платформ, которые могут выступить в качестве типовых[18]. В процессе реализации Государственной программы предполагается проведение следующих мероприятий:

1) оцифровка данных – создание отсутствующих (недостающих) государственных информационных ресурсов;

2) разработка унифицированных протоколов обмена данными в едином формате, протоколов межведомственного (межплатформенного) взаимодействия;

3) развитие функционирующих и создание новых государственных информационных систем как сервисов государственной цифровой платформы – полноценный переход к микросервисной архитектуре[19];

4) формирование государственной цифровой информационной экосистемы, построенной на базе государственных цифровых платформ, взаимодействующих между собой в автоматизированном режиме [1021].

Министерством промышленности в рамках реализации отраслевой политики в качестве головной организации, отвечающей за

[17] С 2019 года проводится точечная практическая работа по внедрению цифровых технологий в регионах республики – начиная с одиннадцати городов (районов) страны с численностью более 80 тыс. человек населения, определенных потенциальными центрами экономического роста (г. Орша, Барановичи Пинск, Новополоцк, Полоцк, Мозырь, Лида, Борисов Солигорск, Молодечно, Бобруйск) [1024].

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

[19] Микросервисная архитектура – разновидность сервис-ориентированной архитектуры, предусматривающей модульный подход к разработке программного обеспечения, основанный на использовании распределенных заменяемых компонентов (микросервисов), оснащенных интерфейсами взаимодействия по стандартизированным протоколам. Основным преимуществом такой архитектуры является возможность по мере необходимости обновлять микросервисы (приложения, сервисы) изолированно, что востребовано при гибкой динамике задач и функций, появлении новых участников и ролей пользователей.

цифровую трансформацию промышленных предприятий, определено ОАО «ЦНИИТУ». На базе данного предприятия организуется центр компетенций цифровой трансформации промышленности Республики Беларусь, который будет формировать политику и основные направления развития предприятий республики на этапах внедрения концепции Индустрия 4.0 [1020].

В рамках мероприятий, направленных на цифровую трансформацию производственных процессов и управление ими, предусматривается выполнение реинжиниринга и оптимизации бизнес-процессов отечественных предприятий с использованием передовых производственных технологий, соответствующих концепции I4.0, включая:

а) создание «цифровых двойников» технологических и бизнес-процессов, выпускаемой (планируемой к производству) продукции;

б) внедрение платформенных решений для управления производством, активами предприятий, обеспечения накопления и обработки данных в режиме реального времени, использования систем поддержки принятия решений, инструментов предсказательной и отчетной аналитики;

в) развитие современных инструментов работы с заказчиками и поставщиками, каналов продвижения продукции и взаимодействия с клиентами.

В рамках программы предусматривается разработка комплекса программно-инструментальных средств для управления жизненным циклом изделий производственных предприятий, который будет включать такие решения, как «цифровой двойник изделия», «цифровой двойник производства», «цифровой двойник обслуживания продукта», программный комплекс интеллектуальной обработки сенсорных данных, получаемых от технологического оборудования, задействованного в производственном процессе. Предполагается, что реализация данных направлений цифровизации производства позволит повысить качество управления производственным процессом, производительность труда, сократить производственные издержки.

Кроме того, предполагается разработать типовое решение для производственного предприятия в целях предоставления его впоследствии как услуги другим белорусским предприятиям (с учетом предварительной адаптации решения под определенное производство). В качестве пилотных площадок определены такие

предприятия, как «МТЗ-холдинг», Управляющая компания холдинга «Минский моторный завод», управляющая компания холдинга «БелОМО», «Полесье». Стоимость Государственной программы составляет 3,72 млрд рублей, из которых 86,5% – собственные средства исполнителей мероприятий [1021].

Вместе с тем следует отметить снижение объема среднетехнологического производства (95,8% к уровню 2019 года) в стране в 2020 году и определенный рост высокотехнологической продукции (106,4% к уровню 2019 года) главным образом за счет фармацевтики на фоне пандемии в общем объеме производства Республики Беларусь. Также отмечается снижение в 2020 году доли среднетехнологичного производства в общем объеме производства (48,2% по сравнению с 52% в 2019 году), незначительный рост доли высокотехнологичного производства (3,3% по сравнению с 2,8% в 2019 году) и значительный рост доли низкотехнологичного производства (37% по сравнению с 33,9% в 2019 году).

В сельском хозяйстве создана и функционирует информационная система идентификации, регистрации, прослеживаемости животных и продукции животного происхождения (AITS), предназначенная для государственного регулирования и управления [1020]. Ведутся работы по исследованию процесса дифференцированного внесения минеральных удобрений (элемент концепции «Precision agriculture» (PA)).

В мае 2020 года компания A1 в тестовом режиме запустила в эксплуатацию сеть 5G SA (Standalone), которая является первой в Беларуси полноценной 5G-сетью, построенной на основе автономной архитектуры[20]. Но данный проект охватывает небольшое количество районов только в г. Минске. В январе 2021 года первая тестовая локация компании Huawei развернута в индустриальном парке «Великий Камень», где сеть работает в диапазоне частот 3,6 ГГц. Вторая опытная зона расположена в Копыльском районе Минской области, где впервые в СНГ белорусское республиканское унитарное предприятие электросвязи «Белтелеком» осуществило тестирование сети пятого поколения в диапазоне 700 МГц. Кроме того, в мае 2020 года инфраструктурный оператор beCloud в тестовом режиме запустил самую большую в Беларуси сеть 5G в

[20] Проект по развертыванию тестовой 5G-сети осуществлен в партнерстве с компанией ZTE.

Минске в диапазонах 3500 МГц и 2600 МГц, состоящую из двадцати базовых станций[21].

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

Ведется работа по созданию централизованной системы электронного здравоохранения, предусматривающей переход к использованию электронных медицинских карт, содержащих медицинскую информацию о пациенте и посредством которых будет обеспечен постоянный дистанционный доступ к медицинским данным, а также переход к сопровождению процессов оказания медицинской помощи преимущественно в электронной форме (ведение документов различного назначения, организация работы скорой медицинской помощи, учет обеспечения лекарственными средствами и изделиями медицинского назначения, санитарно-эпидемиологический мониторинг, лабораторная диагностика и т. п.) [1020]. С 2021 года в системе здравоохранения функционирует единая электронная инфосистема. Электронная база получила название централизованной информационной системы здравоохранения (ЦИСЗ). В этой системе будут собираться, накапливаться и храниться данные о состоянии здоровья граждан страны. Фактически речь идет о цифровом архиве на основе аккумулирования электронных медкарт пациентов. Пользователи ЦИСЗ получат цифровой доступ к услугам в области здравоохранения с использованием личного электронного кабинета пациента[22]. Точкой входа в личный кабинет пациента станет единый портал электронных услуг (https://nces.by/category/portal-gov-by/).

---

[21] beCloud запустил тестовую зону 5G с максимальной для Беларуси скоростью. – Режим доступа: https://becloud.by/media-center/news/becloud-zapustil-testovuyu-zonu-5g-s-maksimalnoy-dlya-belarusi-skorostyu/. – Дата доступа: 28.05.2020.

[22] Порядок работы и использования ЦИСЗ регулируется постановлением Совета Министров № 267 от 13 мая 2021 года.

Следует отметить интеграционные составляющие программы цифровизации. Разработан программно-аппаратный комплекс «Национальный сегмент Интегрированной информационной системы Евразийского экономического союза», в который включены интеграционный шлюз и программный комплекс «Доверенной третьей стороны». Комплекс предназначен для взаимодействия информационных систем государственных органов Республики Беларусь и информационных систем государств – членов Евразийского экономического союза и Евразийской экономической комиссии в рамках общих процессов. В настоящее время Республика Беларусь осуществляет информационный обмен с ЕЭК в рамках 15 общих процессов (ведутся работы по присоединению еще к 15 общим процессам)[23] [1020].

Важно отметить, что на поддержку программы цифровых реформ в Беларуси была направлена Инициатива Европейского Союза EU4Digital (eTrade/eLogistics), предполагавшая принятие ряда мер по продвижению ключевых областей цифровой экономики и общества в соответствии с нормами и практикой ЕС[24] [1025].

---

[23] Осуществляются следующие проекты. 1. Создан механизм «единого окна» в системе регулирования внешнеэкономической деятельности: Совет ЕЭК принял детализированный план на 2020 год по реализации основных направлений развития механизма «единого окна» в системе регулирования внешнеэкономической деятельности. Данный документ служит одним из инструментов управления проектом по развитию и внедрению механизма «единого окна» в государствах – членах ЕАЭС. Министерством иностранных дел формируются профильные экспертные группы для реализации пунктов указанного плана. 2. Разработана «“Дорожная карта” по созданию благоприятных условий для развития цифровой экосистемы торговли в Евразийском экономическом союзе». На Коллегии ЕЭК в 2020 году утверждена рабочая группа высокого уровня. 3. Разработаны подходы к формированию экосистемы и План мероприятий по формированию экосистемы цифровых транспортных коридоров ЕАЭС. На базе НИРУП «Институт прикладных программных систем» с привлечением представителей заинтересованных государственных органов и организаций создана экспертная группа для управления реализацией проекта со стороны Республики Беларусь. 4. Разрабатывается общая «Евразийская сеть промышленной кооперации, субконтрактации и трансфера технологий» [1020].

[24] Планируется, что в ходе реализации пилотного проекта компании из Беларуси и Молдовы будут обмениваться электронными счетами с использованием решения e-Delivery, а государственные таможенные и налоговые органы обоих государств получат доступ к передаваемым данным. Со стороны Европейского союза ответственным по указанному пилотному проекту выступает компания Earns&Young Baltic [1020]. Инициатива EU4Digital поддерживает страны-партнеры на Востоке для обеспечения бесперебойной электронной торговли с ЕС и предлагает гармонизацию трех областей электронной коммерции: 1) законодательство (например, защита прав потребителей, доставка посылок); 2) стандарты (например, совместимость, предварительные цифровые таможенные декларации); 3) экосистема электронной коммерции (например, налогообложение, платежи).

Международная оценка цифровизации Республики Беларусь свидетельствует о динамичном развитии данного процесса в стране. Так, Беларусь занимает 2-е место в мире по технологическим навыкам в рейтинге «Global Skills Index» [1026]. В отчете Международного союза электросвязи «Измерение информационного общества», опубликованном в 2017 году, Республика Беларусь заняла итоговое 32-е место в рейтинге по индексу развития информационно-коммуникационных технологий из 176 стран мира[25]. В обзоре ООН по электронному правительству в 2020 году Республика Беларусь заняла 40-е место по индексу готовности к электронному правительству в рейтинге, сохранив свои позиции как страны с высоким уровнем его значения[26], а также очень высокий уровень электронного участия (EPI)[27] (57-е место в рейтинге). Более того, Беларусь вошла в 13 стран с очень высоким уровнем развития

[25] За всю историю существования данного рейтинга Республика Беларусь поднялась с 53 места в 2007 году до 32 места в 2017 году (в 2018–2019 годах индекс не публиковался). За это время Республика Беларусь неоднократно входила в десятку стран с наиболее динамичным развитием ИКТ (в 2012, 2013 и 2015 годах) [1020].

[26] По сравнению с 2018 годом индекс готовности к электронному правительству Беларуси вырос на 5,8% в 2020 году. В 2018 году значение индекса готовности к электронному правительству Республики Беларусь соответствовало 38-му месту в данном рейтинге, в 2016 – 49-му. Среди государств – участников ЕАЭС лидирующие позиции в рейтинге по индексу электронного правительства заняли Казахстан (29-е место), Россия (36-е место), далее расположились Беларусь (40-е место), Армения (68-е место) и Киргизия (83-е место). К 2020 году, согласно обзору ООН, наша страна сохранила лидерство в регионе Восточной Европы по уровню развития информационно-коммуникационной инфраструктуры. Субиндекс телекоммуникационной инфраструктуры за два года вырос на 20,3%. В обзоре отмечен очень высокий уровень развития человеческого капитала в Беларуси. Прирост значения соответствующего субиндекса Республики Беларусь относительно 2018 года составил 2,6%. В соответствии с оценкой ООН, уровень развития электронных услуг в Республике Беларусь не претерпел значительных изменений по сравнению с 2018 годом (субиндекс веб-услуг соответствует значению 0,7). Отмечено, что Республика Беларусь по итогам 2018–2019 годов получила высокое значение по индексу развития открытых государственных данных (значение индекса соответствует 0,96). Такие результаты достигнуты за счет создания в 2018 году Национального портала открытых данных (data.gov.by). В настоящее время ведутся работы по созданию нормативных правовых условий для его активной эксплуатации заинтересованными. По уровню электронного участия (e-participation) Беларусь, согласно обзору ООН, вошла в подгруппу стран с очень высоким уровнем значения индекса развития электронного участия (0,7–1,0), заняв итоговое 57-е место в рейтинге по данному параметру совместно с Филиппинами, Парагваем, ЮАР и Индонезией. Первенство поделили Эстония, Республика Корея и США.

[27] Использование правительствами электронных решений для обмена информацией, взаимодействия с заинтересованными сторонами или электронного принятия решений [1027].

человеческого капитала и хорошо развитой цифровой инфраструктурой [1027]. В 2021 в Глобальном индексе инновационности (WIPO) страна заняла 62-е место (в 2020 году – 64-е место) [1028, 1029], при этом, как показал анализ, значительное падение показателей политической стабильности, ИКТ, инвестиций компенсировано ростом рейтинга в сфере высшего образования, общей инфраструктуры, торговле, конкуренции и масштабе рынка, влиянии и распространении знаний.

Важнейшей институциональной составляющей цифровой экономики Беларуси, субъектом цифровизации являются действующие в стране IT-компании. По итогам 2020 года в Парке работало около 70 тыс. специалистов. Резидентами ПВТ является 1021 компания.

В 2020 году объем экспорта резидентов ПВТ составил 2,735 млрд долларов [1030]. По сравнению с 2019 годом экспорт вырос на 25%, при этом отмечаем стабильно позитивную динамику роста экспорта за весь период функционирования ПВТ (2007–2020 годы). За январь – май 2021 года экспорт услуг ИКТ составил 1,23 млрд долларов (рост 17,8%). Общий объем производства составил 7,4 млрд рублей с темпом роста 143%. Доля ПВТ в ВВП Беларуси по итогам 2020 года превысила 4% (при величине занятых в ПВТ около 1,5% от всех занятых в экономике страны).

Основные потребители IT-продуктов и услуг резидентов ПВТ – США и страны ЕС – на их долю приходится около 90% всего экспорта. В первую пятерку стран-партнеров ПВТ входят США, Кипр, Великобритания, Ирландия и Россия [1030]. Белорусские разработчики оказывают IT-услуги крупнейшим корпорациям и организациям мира (Samsung, HTC, Лондонской фондовой бирже, Всемирному банку, Microsoft, Coca-Cola, Toyota, Google, British Petroleum и др.). Шесть компаний-резидентов ПВТ вошли в список лучших провайдеров услуг аутсорсинга (рейтинг 2017 Global Outsourcing 100): Bell Integrator, Ciklum, EPAM, IBA Group, Intetics и Itransition.

Ключевыми объектами экспорта в 2020 году являются телекоммуникационные услуги (доля в экспорте 27,7%) и программное обеспечение (25,6%). При этом важно отметить отрицательную динамику роста доли услуг ИКТ и положительную динамику роста экспорта программного обеспечения в динамике по сравнению с 2018 годом.

В 2020 году резиденты ПВТ более чем на 30% нарастили налоговые отчисления в бюджет, которые составил 418 млн рублей.

По данным Министерства по налогам и сборам Республики Беларусь, за 2020 год один резидент ПВТ принес в бюджет в среднем 434,5 тыс. рублей (для сравнения в 2019 году налоговые поступления составили 422,8 тыс. рублей). Резиденты ПВТ обеспечили 1,54% общего объема налоговых поступлений (в 2019 году – 1,13%) [1030].

Выручка компаний сектора «Информация и связь» в 2020 году составила 10,3 млрд рублей, по сравнению с 2019 годом рост составил 16% [1031]. По чистой прибыли IT-компании вместе с предприятиями связи – на втором месте среди всех видов деятельности. Суммарная чистая прибыль в секторе превысила 1,8 млрд рублей, она увеличилась по сравнению с 2019 годом на 36%[28].

Лидером по объему полученной выручки в 2020 году стала израильская компания Playtika (с офисом разработки в г. Минске) [1032], размер которой превысил 1 млрд долларов (рост 17% по сравнению с 2019 годом). Из белорусских компаний самую большую выручку за 2020 год получил Vizor – более 175 млн долларов (на 78% больше, чем в 2019 году). Следом по данному показателю идут Apalon и Belka Games. Выручка Belka Games выросла за 2020 год в 2,2 раза и достигла 90 млн долларов.

Одной из крупнейших белорусских IT-компаний является EPAM, которая стала одной из четырех технологических компаний, входящих в список Forbes «25 самых быстрорастущих публичных технологических компаний», а также признана лидером в индустрии IT-сервисов в списке Fortune «100 самых быстрорастущих компаний» в 2019 и в 2020 годах. Выручка EPAM в 2020 году составила 2,66 млрд долларов, что на 15,9% превышает показатель 2019 года. Численность персонала EPAM на конец 2020 года составила около 41,2 тыс. сотрудников [1033]. В 2021 году было объявлено о намерении включить компанию в американский индекс S&P 500.

Согласно рейтингу самых дорогих компаний в игровой индустрии[29], белорусская компания Wargaming занимает 16-е место с оценкой 1,5 млрд долларов[30]. В 2021 году компания с белорусскими

[28] Данные официальной статистики не отражают полностью финансовое положение в секторе «Информация и связь», в том числе в IT-компаниях. В расчетах Белстата учтены показатели только части крупных компаний ПВТ. Суммарная чистая прибыль IT-компаний за 2019 год составила 571 млн рублей.

[29] Разработан консалтинговой компанией Games One.

[30] Game Unicorn Index. – Режим доступа: https://gamesone.co/unicorn-index/. – Дата доступа: 15.04.2021.

корнями PandaDoc – разработчик платформы электронных документов повысила свою капитализацию до 1 млрд долларов.

В 2020 году приток прямых иностранных инвестиций в ПВТ вырос на 26% и составил 331,7 млн долларов. В 2020 году в ПВТ созданы 23 центра разработки зарубежных корпораций, общее их количество составило 107 [1030]. Объем венчурных инвестиций[31] в Республику Беларусь в 2020 году сократился[32] на 21,8% [1034]. 85% венчурных инвестиций было привлечено IT-компаниями, что обусловлено устойчивостью данного сектора к влиянию пандемии COVID-19, а также ростом спроса на IT-решения в 2020 году. В марте 2020 года состоялась первая в Беларуси на 100% дистанционная венчурная сделка, в рамках которой белорусский стартап StringersHub привлек 500 тыс. долларов[33]. При этом основным направлением венчурного инвестирования в 2020 году стали ИТ (доля в общем объеме – 85%), что значительно выше показателей 2019 года (на ИТ сферу приходилось 23%).

В начале 2021 года компания Playtika Holding Corp. (с офисом разработки в г.Минске[34]) провела IPO (на Nasdaq Global Select Market), в результате чего удалось реализовать около 70 млн акций и привлечь 1,88 млрд долларов [1032]. В конце 2020 года израильская компания-разработчик Moon Active объявила о покупке белорусской студии Melsoft[35] [1035]. Среди других сделок с приобретением белорусских IT-активов в 2020 году самым активным инвестором стал игровой бренд MY.GAMES (входит в Mail.ru Group)[36].

---

[31] Нормативно-правовые акты, регулирующие сферу венчурного финансирования: Положение о порядке создания субъектов инновационной инфраструктуры, утвержденное Указом Президента Республики Беларусь от 3 января 2007 года № 1; Закон Республики Беларусь от 10 июля 2012 года «О государственной инновационной политике и инновационной деятельности в Республике Беларусь»; Закон Республики Беларусь от 12 июля 2013 года «Об инвестициях» № 53-З; Государственная программа инновационного развития Республики Беларусь на 2016–2020 годы, утвержденная указом Президента Республики Беларусь от 31 января 2017 года № 31.

[32] Большинство инвесторов заключили на 30–60% меньше сделок по сравнению с 2019 годом. Исключение составляют лишь бизнес-ангелы, которые в 2020 году заключили сделок на 36 млн долларов (в 2019 году – 45,6 млн долларов).

[33] В качестве инвесторов выступили белорусская сеть бизнес-ангелов Angels Band, венчурная группа Starta Vetures и фонд Insta Ventures.

[34] В компании работают 3700 человек, 600 из них в минском офисе.

[35] Сумма сделки не называется, но по оценкам она могла составить 500 млн долларов. Именно столько мог получить бывший владелец студии – компания Wargaming.

[36] Компания инвестировала в белорусскую Mamboo Games, белорусские мобильные студии Appyfurious и Purple Games.

В 2021 году отмечается рост сферы E-Commerce. Так, по состоянию на 1 сентября количество зарегистрированных в Торговом реестре Интернет-магазинов составило 27,2 тыс., что на 6,8% больше, чем на 1 января 2021 года[37] За 2021 год онлайн-продажи в белорусских интернет-магазинах выросли на 25% – до 3,4 млрд руб. Доля интернет-продаж в розничном товарообороте страны составила 5,8%[38].

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

1) политический кризис в стране;

2) COVID-19;

3) сложная макроэкономическая ситуация;

4) ужесточение государственного регулирования сектора ИТ;

5) санкционная политика со стороны ЕС, США, Великобритании не только в отношении Беларуси, но и Российской Федерации.

Это формирует ряд тенденций цифровизации экономики Республики Беларусь и развития сектора ИТ в среднесрочной перспективе (в течение 2–3 лет).

1. Наблюдаются негативные изменения в налоговой политике в отношении сектора ИКТ. В новой редакции Налогового кодекса повышен подоходный налог (с 9% до 13%) для резидентов ПВТ и индустриального парка «Великий камень»[39]. Вместе с тем для резидентов ПВТ сохраняются льготы по налоговым отчислениям в Фонд социальной защиты населения[40]. Налог на прибыль для мобильных операторов с 1 января 2021 года повышен с 18% до 30% [1036]. Прогнозируется, что с 2022 года возможен массовый исход IT-компаний из Беларуси в юрисдикции стран-соседей членов ЕС (Литвы, Латвии, Польши, Эстонии), а также Украины, по причинам положительной динамики увеличения фискальной нагрузки, страновых санкционных ограничений, отсутствия доступа к венчурным

[37] Количество интернет-магазинов в Беларуси за 8 месяцев увеличилось на 6,8%. – Режим доступа: https://belretail.by/news/kolichestvo-internet-magazinov-v-belarusi-za-mesyatsev-uvelichilos-na. – Дата доступа: 20.09.2021.

[38] Итоги года: на долю локальных онлайн-ритейлеров в Беларуси приходится 5,8%. – Режим доступа: https://belretail.by/news/itogi-goda-na-dolyu-lokalnyih-onlayn-riteylerov-v-belarusi-prihoditsya. – Дата доступа: 29.12.2021.

[39] Действовать нынешняя ставка налога для резидентов IT- и индустриального парка будет до 2023 года.

[40] Отчисления в ФСЗН в Беларуси составляют 35% дохода, но сотрудники компаний-резидентов ПВТ платят его в привязке к средней зарплате по стране.

финансовым ресурсам на национальном уровне. Сравнительный анализ размеров фискальных выплат показывает сохраняющуюся привлекательность условий белорусской юрисдикции по основным составляющим: ставке подоходного налога (13% по сравнению с 20–25% в странах-соседях), социальным взносам работников (1% по сравнению с 11% в Латвии, 13,7% в Польше, 19,5% в Литве), налоге на прибыль (1% от выручки по сравнению с 18% в Украине, 19% в Польше, 20% в Латвии). Вместе с тем фактор увеличения фискальной нагрузки из трех приведенных является наименее определяющим для принятия решения о смене белорусской юрисдикции [1037].

2. Политическая нестабильность в стране снижает интерес инвесторов к белорусским стартапам и вызывает отток квалифицированных кадров из страны, что наносит существенный ущерб инвестиционному климату в Беларуси. Согласно докладу консалтинговой компании CIVITTA и инвестиционного фонда Bulba Ventures [1038], в 2020 году Беларусь резко потеряла инновационную привлекательность. Так, 69% компаний не готовы позиционировать себя как белорусские. 11 из 12 стартапов утверждают, что политическая напряженность пагубно сказывается на инновационной экосистеме в стране[41]. Большинство белорусских стартапов предпочитают регистрировать штаб-квартиру за границей или как минимум иметь зарубежный филиал либо представительство. 60% стартапов не рассматривают страну как важный рынок. Среди наиболее частых последствий политического кризиса стартапы, которые уже ощутили его влияние, отмечают изменение планов и дополнительные расходы (45%), ухудшение доступа к внешнему финансированию (32%), угрозы развитию бизнеса (28,5%), снижение эффективности работы команды (27%) [1039].

3. Усиливаются миграционные настроения в среде IT-специалистов. Так, 50% респондентов [1038] сообщили, что планируют полный или частичный переезд или уже его совершили. На конец 2020 года 25% респондентов активно интересовались перспективами трудовой миграции (почти двукратный рост по сравнению с 2019 годом), около 10% уже отвечали из-за границы (близко к

[41] Среди основных проблем экосистемы стартапов были названы: проблемы с привлечением финансирования (78%), низкий интерес правительства к развитию экосистемы (73%), недостаточный уровень взаимодействия между бизнесом и правительством (73%), законодательные ограничения или регулирование (61%).

трехкратному росту)[42] [1040]. Данные о направлениях релокейта свидетельствуют о переводе ключевыми игроками сектора ИТ части сотрудников, главным образом, в такие страны как Литва, Польша и Украина. Согласно данным исследования IMAGURU [1039], 58% белорусских стартапов покинули Республику Беларусь[43].

4. В секторе ИТ традиционный аутсорсинг утвердился на уровне более 40% занятых, более 20% специалистов заняты в компаниях смешанного типа [1040].

5. На фоне кризисных явлений в стране осуществляется концентрация доли IT-рынка в компаниях с количеством сотрудников более 500 человек, что обусловлено их конкурентным преимуществом обеспечить стабильный доход и возможности перемещать сотрудников как между проектами, так и между офисами. При этом продолжает снижаться число занятых в компаниях с количеством сотрудников менее 50 человек. Новым трендом является рост занятых в компаниях вне белорусской юрисдикции (около 5,5% респондентов).

6. Пандемия COVID привела к резкому росту сегмента E-commerce, который в 2020 году вырос на 40% и достиг 2,3 млрд рублей. По статистике самой быстрорастущей категорией стали медицинские товары – их продажи выросли на 692% [1041]. Доля Интернет-продаж в розничном товарообороте страны составила 4,5%[44] [1042]. Данные показатели обусловлены увеличением онлайн-покупок белорусов во время самоизоляции и их стремлением избавиться от рублевых накоплений вследствие девальвации национальной валюты (более чем на 20% за год) [1023].

7. С ростом удаленного доступа к рабочим местам и увеличением объема онлайн платежей усиливается всеобщее внимание к проблематике кибербезопасности [1036].

---

[42] Среди направлений потенциальной миграции на первое место вырвалась Польша, визовая программа PBH привлекает более 43% разработчиков. Литва и Украина, которые были во втором эшелоне направлений, сразу прибавили, привлекают 25% и 20% соответственно. Традиционные лидеры: США, Германия или Канада несколько утратили позиции. Это может означать, что многие думают скорее о временном релокейте в ожидании развития ситуации.

[43] По данным организации, более 20 тысяч IT-специалистов уехали из Беларуси в 2020 году (14 октября 2021 года онлайн-дискуссия «Диалог о будущем», организованная Белорусским институтом стратегических исследований (BISS) и Belarus in Focus).

[44] В 2019 году, по оценкам Белстата, на интернет-торговлю приходилось 4,1% [1023].

8. По оценке ActiveCloud, облачный рынок Беларуси вырос на 20–25% в национальной валюте по сравнению с 2019 годом. В дальнейшем, по прогнозам [1036], МСП будет использовать стратегию Cloud-only, фокусируясь на моделях PaaS (Platform as a Service) и SaaS (Software as a service). Средний и крупный бизнесы будут следовать стратегии Cloud-first с элементами мультиоблачности. В этом сегменте усилится тренд на сближение и стирание границ между собственными (приватными) и облачными (публичными) инфраструктурами клиентов.

9. Отмечается рост сегментов HealthTech/MedTech, а также FinTech (включая ERP и InsurTech). В Беларуси IT-проекты имеют аутсорсинговую природу, так как продуктовые решения сильно завязаны на особенностях регуляции рынков [1043].

Важно отметить, что сектор FinTech поступательно развивается в Республике Беларусь. В 2019 году создана первая криптобиржа Currency.com, которая привлекла инвестиции VP Capital и Larnabel Ventures и в 2020 году вошла в топ-20 мирового рейтинга [1044]. В этом же году заработали регулируемые криптобиржи – iExchange (учредитель – компания «Криптотрейд»[45]) и Free2ex[46] (ООО «Пиксель Интернет»). С 2021 года в Беларуси начала работать криптобиржа BYNEX.BY. Разработчиком платформы выступила компания-резидент ПВТ ООО «ЕРПБЕЛ» [1045]. Следует отметить, что интенсивное развитие криптоинфраструктуры в Республике Беларусь способствует формированию национального крипторынка. Так, по данным Currency.com, за 2019–2020 годы количество зарегистрированных аккаунтов на площадке увеличилось в 5 раз (с 50 тыс. до 250 тыс.), в декабре 2020 года объем торгов на криптобирже составил 2,6 млрд долларов (рост за период в 30 раз), максимальный объем торгов за день приблизился к отметке в 120 млн долларов [1045]. По оценкам платежной платформы Triple A, в Беларуси более 350 тыс. человек являются владельцами криптовалют (19-е место в мировом крипторейтинге)[47].

---

[45] В данный момент сервис не работает по причине смены юрисдикции.

[46] Белорусам теперь доступен новый вид заработка и инвестиций. – Режим доступа: https://myfin.by/stati/view/belorusam-teper-dostupen-novyj-vid-zarabotka-i-investicij-rasskazyvaem-podrobnee. – Дата доступа: 23.09.2021.

[47] Triple A: Беларусь занимает 19-е место в мировом крипторейтинге. – Режим доступа: https://dev.by/news/triple-a-belarus-kripta. – Дата доступа: 20.10.2021.

Следует отметить участие белорусских банков в развитии FinTech в стране. Согласно исследованию [1046], четыре белорусских банка (ОАО «Белагропромбанк», ОАО «Белинвестбанк», ОАО «Банк БелВЭБ» и ОАО «СберБанк») находятся в процессе создания банковской экосистемы, еще как минимум восемь банков намерены продвигать небанковские сервисы, а ОАО «Банк Дабрабыт» планирует внедрить модель BaaS, предполагающую развитие финансовых сервисов опосредованно через своих партнеров. Кроме того, в 2018 году АСБ «Беларусбанк» стал платежным партнером криптообменника White Bird и криптобиржи Bynex[48]. В 2019 году создана инвестплатформа Банка БелВЭБ – Finstore.by. За год функционирования платформа позволила путем продажи токенов белорусских компаний привлечь финансовые ресурсы на сумму 9,3 млн долларов (механизм ICO) [1044]. На конец мая 2021 года на Finstore.by более 4 тыс. человек инвестировали в токены[49] порядка 28 млн долларов. На платформе предлагаются цифровые долговые обязательства белорусских компаний разного профиля (производственных, торговых, финансовых). Всего зарегистрировано 108 выпусков токенов. В 2021 году на рынок цифровых токенизированных активов вышла БЖД с объемом эмиссии токенов – 5 млн долларов. В настоящее время БелВЭБ – единственное уполномоченное Нацбанком Беларуси банковское учреждение, получившее разрешение на проведение такого рода транзакций. Вместе с тем в белорусской банковской системе разрабатываются[50] законодательные основы, которые позволят 12 банкам в стране приобретать, отчуждать и хранить собственные токены, а также токены других банков и юрлиц. Сделки с токенами банки смогут совершать через резидентов ПВТ-операторов криптоплатформ.

[48] В Беларуси заработал первый легальный сервис по обмену криптовалют. – Режим доступа: https://belarusbank.by/ru/33139/press/bank_news/36990. – Дата доступа: 16.11.2020.

[49] Среди долговых инструментов, доступных на белорусском рынке, токены обладают следующими преимуществами: 1) отсутствие транзакционных расходов. Finstore.by не взимает комиссию за сделки с токенами в рамках своей площадки; 2) отсутствие потерь по причине курсовых разниц: если инвестор приобрел за доллары США токены, то доход по процентам, а также основной долг выплачиваются в валюте покупки, а затем конвертируются 1 : 1 в доллары США; 3) высокий уровень доходности. По некоторым токенам доходность превышает 10% годовых; 4) возможность отозвать средства. Практически все эмитенты предлагают возможность досрочно вернуть свои инвестиции; 5) доступность широкому кругу лиц. Стоимость токенов начинается от 20 USD; 6) дистанционное управление портфелем; 7) доходы по токенам не облагаются налогами вплоть до 1 января 2023 года [1049].

[50] Нацбанк подготовил проект указа, который разрешит с января 2022 года совершать операции с токенами белорусским банкам.

Эксперимент планируется провести в течение трех лет – с 1 января 2022 года по 1 января 2025 года [1047]. За время осуществления эксперимента планируется оценить условия и возможности привлечения банками денежных средств через проведение ICO; риски при проведении операций с токенами; влияние таких операций на финансовую стабильность и эффективность мер денежно-кредитной политики.

Важно отметить активное развитие в стране цифровых платежных систем. Так, в 2021 году Альфа-Банк предоставил клиентам осуществление денежных переводов по номеру телефона между картами Mastercard и Visa любых белорусских банков[51]. В основу нового сервиса легла цифровая платформа для совершения переводов по номеру мобильного телефона Mastercard Transfers Hub [1034]. В 2021 году инициировано подключение Беларуси к платежным возможностям Google Pay[52] [1048], Mastercard запускает сервис мгновенных денежных переводов в мессенджере Viber[53] [1050]. Кроме банковских институтов, систему цифровых платежей развивают белорусские мобильные операторы. Так, компания A1 предложила своим пользователям приложения A1 banking в рамках сервиса «A1 кошелек» проведение расчетов за любые товары, работы и услуги с помощью электронных денег – без процентов в пределах лимита до 150 рублей и на условиях отсрочки оплаты[54]. Согласно данным исследования сервиса электронных платежей – ЮMoney (входит в экосистему СберБанка), число бесконтактных платежей смартфонами[55] в Беларуси выросло за август 2020 года – июль 2021 года (по сравнению с

[51] Комиссия за перевод составит 1% до 31 марта 2021 года и 1,5% после этой даты.

[52] Компании в Беларуси начали принимать оплату через платежную платформу Google Pay (web-решение) в расчетах за товары или услуги.

[53] Для осуществления перевода отправителю не нужно знать номер карты получателя, достаточно иметь получателя в своей адресной книге Viber или знать номер его телефона. Новая услуга доступна для держателей карт любого белорусского банка, чей аккаунт Viber привязан к белорусскому номеру мобильного телефона. Технологическим партнером проекта является МТБанк, который предоставляет функционал сервиса карточных переводов. Сервис объединяет технологию Mastercard Send и платформу Mastercard Transfers HUB, на которой могут быть добавлены платежные карты различных белорусских банков и платежных систем.

[54] Кроме того, A1 предлагает развлекательные услуги, а также подключение «умных устройств» в рамках приложения «Умный дом». МТС со своей стороны предоставляет частным клиентам финансовые, развлекательные, образовательные, медицинские услуги и услуги трекинга – определения местоположения.

[55] Рассматривались платежи с помощью Apple Pay, Google Pay, Samsung Pay, Garmin Pay, Mi Band, Koshelek, технологии HCE через мобильное приложение сервиса, а также оплата виртуальными и пластиковыми картами ЮMoney.

данными с августа 2019 по июль 2020 года) на 29%, оборот увеличился в 1,7 раза, средний чек – в 1,3 раза, до 20 рублей [1051].

Кроме того, в 2021 году подписан указ № 196 «О сервисах онлайн-заимствования и лизинговой деятельности», которым предусмотрено развитие альтернативных банковским механизмов привлечения и предоставления денежных средств физическим и юридическим лицам с помощью сервисов онлайн-заимствования[56] [1052]. Целью принятия данного документа является развитие финансового рынка Республики Беларусь, деловой инициативы и предпринимательства, повышение доступности финансовых услуг для населения, а также обеспечение сохранения защиты интересов потребителей финансовых услуг [1053]. Национальный банк Республики Беларусь планирует в 2022 году внедрить систему мгновенных платежей для физических лиц, ведутся работы по развитию открытых банковских API, направленные на реализацию концепции открытого банкинга в стране, обеспечения удобного и безопасного способа обмена информацией между банками, их клиентами и технологическими компаниями, повышения прозрачности предоставляемых финансовыми организациями услуг. Введен в действие стандарт проведения расчетов, определяющий регламент взаимодействия поставщиков и пользователей API, определены требования к открытым информационным API, одобрена Концепция по развитию открытых банковских API [1022].

Исследование, проведенное совместно VISA и CIVITTA в отношении рынка FinTech-услуг Республики Беларусь, выявило 98 FinTech-компаний в стране, занятых, главным образом, в сфере платежных сервисов, переводов (22%), Блокчейн (15%), инвестирования (12%), автоматизации банков (10%), бухгалтерского учета (9%)[57]. При этом лишь 14% компаний производят уникальный продукт, создающий нишу на рынке, 65% игроков нацелены на рынки стран ЕС и Великобританию [1026].

С учетом отмеченной динамики цифровизации экономики Республики Беларусь в секторальном разрезе, как показывает рис. 4.2, можно утверждать об относительно равномерном поступательном внедрении IT-технологий. За расчет приняты данные межотраслевого

[56] Указом определены требования для заключения договоров займа посредством сервисов онлайн-заимствования, установлен порядок предоставления займов и утверждено Положение о деятельности операторов сервиса онлайн-заимствования и договорах, заключаемых посредством данного сервиса.

[57] Остальные FinTech компании заняты в более узких нишах: скоринговые системы (6%), онлайн кредитование (6%), краудфандинг (6%), маркетплейсы (6%), P2P кредитование (1%), PerTex (регистрация компаний онлайн) (1%), другое (4%).

баланса за 2016–2019 годы, где выведены расчетные показатели доли «Услуг в области компьютерного программирования, консультационных и аналогичных услуг» и «Услуг в области информационного обслуживания» относительно всей совокупности производственных факторов в использовании в секторальном разрезе в основных ценах, формирующих, таким образом «расчетный показатель цифровизации»[58].

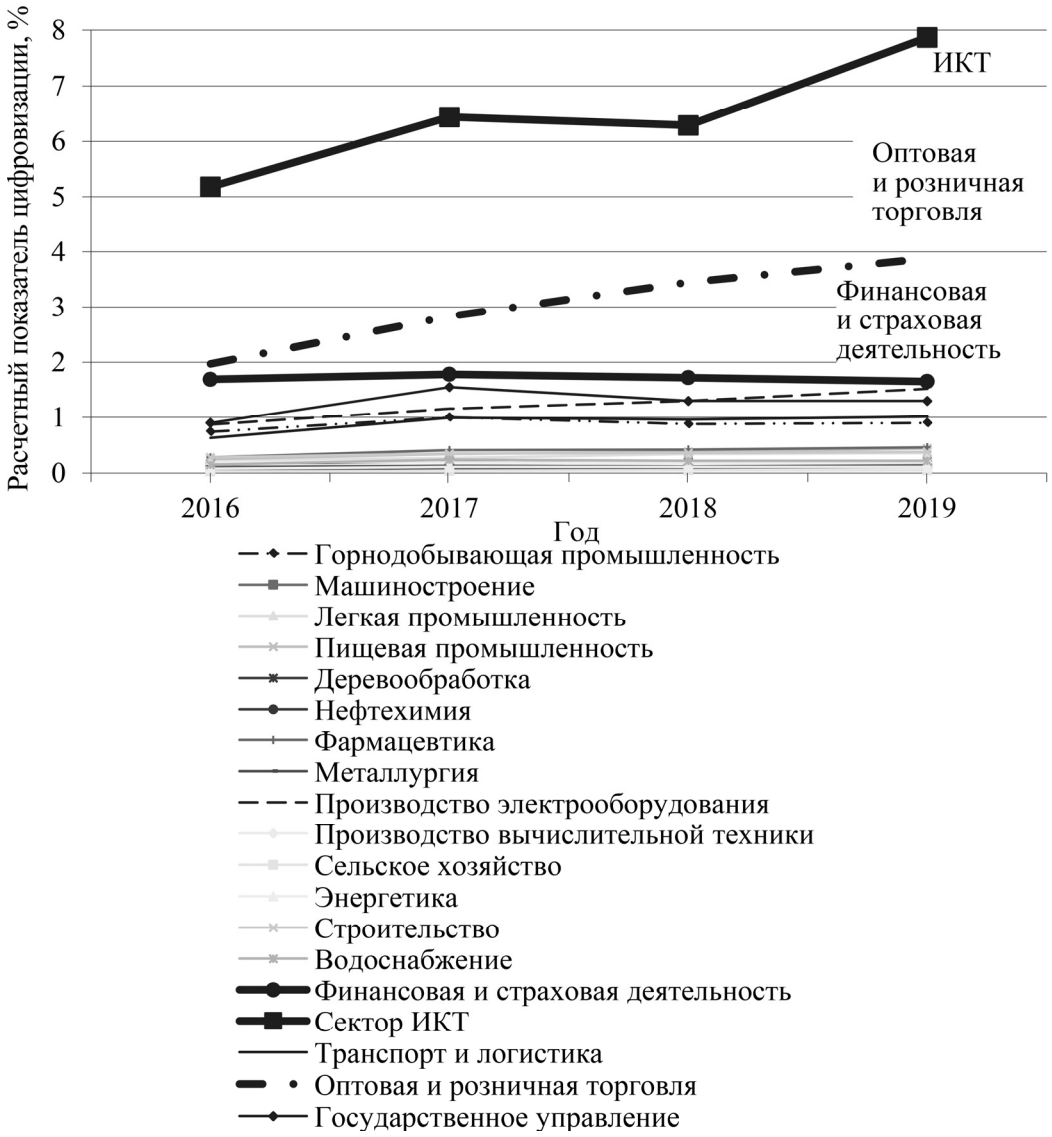


Рис. 4.2. **Динамика цифровизации в отраслевом разрезе** (разработано автором на основе данных межотраслевого баланса)

[58] Система таблиц "Затраты-Выпуск". – Режим доступа: https://www.belstat.gov.by/ofitsialnaya-statistika/realny-sector-ekonomiki/natsionalnye-scheta/sistema-tablits-zatraty-vypusk/index.php?sphrase_id=1636679. – Дата доступа: 20.12.2021.

Как показано на графике, наибольший уровень внедрения цифровых технологий отмечается в таких отраслях, как сектор ИКТ, оптовая и розничная торговля и финансовая деятельность.

Важно отметить, что с учетом методологии оценки цифровизации экономики, разработанной компанией McKinsey [1054], ключевыми критериями прогресса цифровизации является наличие устойчивой экономики, сильного кадрового резерва, высококачественной цифровой инфраструктуры и динамичной технологической экосистемы. Республика Беларусь имеет как сильные, так и слабые стороны.

1. Макроэкономическая ситуация в Беларуси в 2021 году усложняется. Санкционные и антисанкционные мероприятия в отношении страны, политическая и правовая неопределенность препятствуют обеспечению стабильного экономического роста, повышению конкурентоспособности экономики страны.

2. Преимуществом является наличие квалифицированной рабочей силы в Беларуси, обусловленное высоким уровнем специального высшего образования по соответствующим специальностям. Именно высокая квалификация IT-специалистов делает Беларусь привлекательной для иностранных инвесторов и приход в ПВТ крупных иностранных IT-компаний, включая IDT (США), IAC/InterActiveCorp (США), Appstud SAS (Франция), BSL (Россия), Вебби ГмбХ (Германия), VIAcode (США), Globant (Бразилия), Дельтатрэ Груп Лимитед (Великобритания) и пр.

3. Вместе с тем требуется дальнейшее внедрение цифровых технологий в систему среднего образования, увеличение подготовки IT-кадров в системе высшего образования, поскольку страна сталкивается с необходимостью системной цифровизации ключевых секторов и отраслей производства. По данным статистики, в 2020 году по специальностям «Техника и технологии» в стране обучалось на 29,3% студентов меньше по сравнению 2013 годом, хотя относительно общего количества студентов по всем специальностям доля обучающихся техническим специальностям выросла с 19,7% до 21,6%.

4. Развитая цифровая инфраструктура в стране, льготный режим функционирования ПВТ сохраняют при прочих равных условиях привлекательный характер для осуществления определенных IT-операций в Беларуси (услуги аутсорсинга, тестирования и пр.). Именно продуктовая бизнес-модель в секторе ИТ обеспечивает технологическое развитие страны. Вместе с тем продуктовая

направленность IT-компаний, ввиду складывающейся внутренней и внешней конъюнктуры, будет сокращаться.

5. Ключевым фактором в данной связи является резкое снижение инвестиционной привлекательности страны. Внутренние инвестиционные (венчурные) ресурсы носят чрезвычайно ограниченный характер и представлены, главным образом, на уровне таких организаций и компаний, как [1055] Белинфонд[59], инвестиционная компания Bulba Ventures[60], инвестиционная организация Haxus[61]. В этой связи дополнительное сокращение возможностей для привлечения внешнего финансирования на внутреннем рынке будет способствовать регистрации управляющих компаний (офисов) за пределами Республики Беларусь, что приведет к поступательному исходу перспективных IT-проектов из страны.

С учетом отмеченных критериев прогресса цифровизации экономики Республики Беларусь и выделенных тенденций в качестве комплекса мероприятий, направленных на создание условий развития и внедрения цифровых технологий, представляется целесообразной реализация четырех блоков институциональных изменений:

1) на уровне надгосударственного регулирования (ЕАЭС и Союзного государства):

а) создание Совета ЕАЭС по цифровым технологиям с учетом опыта интеграции цифровых систем ЕС и стран Центральной и Восточной Европы (EU4Digital);

б) формирование гармонизированной цифровой деловой среды в ЕАЭС;

в) стимулирование интеграции передового опыта внедрения цифровых технологий (в первую очередь с Российской Федерацией, как с наиболее продвинутым государством ЕАЭС в сфере цифровизации);

2) на национальном уровне:

а) ускорение оцифровки государственных услуг;

---

[59] Создан в 1998 году, является некоммерческой организацией, находящейся в подчинении Государственного комитета по науке и технологиям Республики Беларусь. Средства для финансирования проектов выделяются Белинфонду из бюджета. Объектами финансирования являются преимущественно инновационные проекты крупных организаций, а не стартапы.

[60] Создана в марте 2018 года. Основная концепция – вкладывать усилия и время в ограниченное количество проектов.

[61] Зарегистрирована на Кипре, но большая часть команды – белорусы. Проинвестировано три успешных проекта: AIMATTER, MSQRD, maps.me.

б) поступательное формирование интегрированной цифровой платформы в рамках концепции E-Government с использованием успешного опыта Эстонии;

в) формирование технологических и правовых условий для развития рынка деперсонализированных цифровых данных (рынка Big Data) (с учетом практики ЕРИП[62]);

г) трехуровневое развитие ИКТ в секторе национального образования: на уровне среднего образования – реализация государственных проектов внедрения обучающих программ знакомства с цифровыми технологиями; в системе высшего образования – увеличение набора студентов по специальностям, актуальным требованиям сектора ИКТ; на уровне послевузовского образования – реализация программ переобучения и повышения квалификации;

д) развитие IT-сегмента рынка труда в том числе путем стимулирования трудовой IT-миграции в страну (упрощение миграционных процедур, проведение рекламных компаний за рубежом и пр.);

3) на уровне бизнес-среды:

а) формирование (развитие) цифровой экосистемы как для сектора ИКТ, так и традиционных отраслей;

б) повышение операционной эффективности традиционных отраслей (внедрение цифровых приложений и каналов распространения, использование Big Data Analytics и AI, реализация улучшенной IT-архитектуры);

в) повышение финансовой доступности для стартапов, в том числе с использованием механизмов государственно-частного партнерства[63];

г) формирование нормативно-правовой среды и разработка соответствующей программы поддержки создания технологических кластеров с целью ускорения внедрения цифровых технологий.

---

[62] С 1 октября 2021 года ЕРИП на платной основе предоставляет данные о клиентах, их представителях с целью обновления (актуализации) данных (Обновлен сборник вознаграждений за операции, осуществляемые ОАО «Небанковская кредитно-финансовая организация «ЕРИП». – Режим доступа: https://www.raschet.by/o-sisteme/novosti/2712/. – Дата доступа: 29.09.2021).

[63] Например, в октябре 2021 года подписано Соглашение о сотрудничестве и взаимодействии по развитию и поддержке стартап-движения и малого инновационного предпринимательства между ОАО «Белагропромбанк», Министерством экономики и Государственным комитетом по науке и технологиям Беларуси. Основная цель подписания соглашения – объединение усилий Минэкономики, ГКНТ и Белагропромбанка по созданию благоприятной среды для развития стартап-движения и малого инновационного предпринимательства в стране.

Заключение

Таким образом, как показал приведенный анализ, по уровню комплексности и системности принимаемых управленческих решений по построению современной экосистемы цифровой экономики Республика Беларусь значительно отстает от образцовых международных практик. Наша страна осуществляет стратегическое планирование развития данной сферы посредством разработки и реализации цифровых программ. Вместе с тем финансовые ограничения не позволяют проводить широкомасштабное внедрение цифровых технологий на государственном уровне наравне со странами-соседями. Институциональный технологический и финансовые блоки являются плохо проработанными и имеют скорее рамочную, неспециальную форму в отношении современных цифровых инноваций (таких, например, как AI / ML, IoT, Cloud Computing, Блокчейн, FinTech и пр.).

Выделены факторы развития цифровой экономики страны, связанные с продолжающимся политическим кризисом, последствиями COVID-19 для внутреннего рынка, сложной макроэкономической ситуацией, санкционной политикой ЕС, США и Великобритании, ужесточением государственного регулирования сектора ИТ, ростом миграции ИКТ-бизнеса.

Возможными механизмами преодоления негативных факторов со стороны государства является принятие комплекса мероприятий по четырем составляющим, включая наднациональное регулирование на уровне ЕАЭС и Союзного государства; на национальном уровне реализация концепции E-Government и проведение образовательной политики, направленной на рост цифровых навыков населения; на уровне бизнес-среды – стимулирование развития отраслевых цифровых экосистем, внедрение технологий Big Data Analytics и AI, реализация улучшенной IT-архитектуры, формирование условий для создания национальных технологических кластеров и цифровых стартапов.

4.2. Кибербезопасность в системе национальной безопасности Республики Беларусь

В условиях цифровизации экономики страны на первый план угроз национальной безопасности выходят соответствующие риски, связанные с внутренней и внешней цифровой безопасностью.

Проблема кибербезопасности, включая безопасность данных, их целостность является чрезвычайно актуальной в современной экономике. С учетом интегрированности белорусской экономики и цифровой экосистемы в международную среду данная проблема имеет потенциальный рост влияния на экономику Беларуси. Кроме того, обеспечение цифровой безопасности требует от государства проведения комплексной политики, охватывающей одновременно управление рисками цифровой безопасности, конфиденциальность данных и защиту потребителей как на внутреннем, так и внешнем контурах [1056].

Национальная безопасность представляет собой, согласно белорусскому законодательству[64], состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз. Составляющими элементами национальной безопасности являются политическая безопасность; военная безопасность, социальная безопасность, демографическая безопасность; а также экономическая безопасность – состояние экономики, при котором гарантированно обеспечивается защищенность национальных интересов Республики Беларусь от внутренних и внешних угроз; научно-технологическая безопасность – состояние отечественного научно-технологического и образовательного потенциала, обеспечивающее возможность реализации национальных интересов Республики Беларусь в научно-технологической сфере; информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Кибербезопасность – состояние защищенности информационной инфраструктуры и содержащейся в ней информации от внешних и внутренних угроз [1057]. Соответственно, угроза национальной безопасности – потенциальная или реально существующая возможность нанесения ущерба национальным интересам Республики Беларусь.

Базовым законодательным актом регулирования вопросов информационной безопасности в Республике Беларусь стало принятие в 2008 году закона «Об информации, информатизации и защите информации»[65]. Данный законодательный акт устанавли-

[64] Концепция национальной безопасности Республики Беларусь: утв. Указом Президента Республики Беларусь от 9 ноября 2010 года № 575.

[65] Закон Республики Беларусь от 10 ноября 2008 года № 455-З.

вает основы политики государственного регулирования в области информации, информатизации и защиты информации, которые включают:

1) обеспечение условий для реализации и защиты прав государственных органов, физических и юридических лиц;

2) создание системы информационной поддержки решения задач социально-экономического и научно-технического развития Республики Беларусь;

3) создание условий для развития и использования информационных технологий, информационных систем и информационных сетей на основе единых принципов технического нормирования и стандартизации, оценки соответствия требованиям технических нормативных правовых актов в области технического нормирования и стандартизации;

4) формирование и осуществление единой научной, научно-технической, промышленной и инновационной политики в области информации, информатизации и защиты информации с учетом имеющегося научно-производственного потенциала и современного мирового уровня развития информационных технологий;

5) создание и совершенствование системы привлечения инвестиций и механизма стимулирования разработки и реализации проектов в области информации, информатизации и защиты информации;

6) содействие развитию рынка информационных технологий и информационных услуг, обеспечение условий для формирования и развития всех видов информационных ресурсов, информационных систем и информационных сетей;

7) обеспечение условий для участия Республики Беларусь, административно-территориальных единиц Республики Беларусь, государственных органов, физических и юридических лиц в международном сотрудничестве, включая взаимодействие с международными организациями, обеспечение выполнения обязательств по международным договорам Республики Беларусь;

8) разработку и обеспечение реализации целевых программ создания информационных систем, применения информационных технологий;

9) совершенствование законодательства Республики Беларусь об информации, информатизации и защите информации (табл. 4.2).

Таблица 4.2

Институциональная матрица защиты киберпространства Республики Беларусь (разработано автором)

Период	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Базовый уровень (2005–2015 годы)	Закон Республики Беларусь «Об информации, информатизации и защите информации» (от 10 ноября 2008 года № 455-З)	Пар	Области информации, информатизации и защиты информации
	Оперативно-аналитический центр при Президенте Республики Беларусь (Указ Президента от 1 апреля 2008 года)	ПР	Обеспечение защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь
	Концепция национальной безопасности Республики Беларусь (Указ Президента от 9 ноября 2010 года № 575)	ПР	Научно-технологическая и информационная безопасность
	Положение о технической и криптографической защите информации, утверждено Указом от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации»	ПР	Криптографическая защита информации
Первый уровень (2016–2020 годы)	Центр мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере FinCERT.by (создан в 2018 году)	Нацбанк	Кибератаки и мошенничество с использованием электронных платежных инструментов и средств платежа
	Концепция информационной безопасности Республики Беларусь, утверждена постановлением Совета Безопасности Республики Беларусь (от 18 марта 2019 года № 1)	ПР, СБ	Цифровые угрозы в промышленности, на транспорте, в энергетике, электросвязи, здравоохранении и системах жизнеобеспечения
	Концепция обеспечения кибербезопасности в банковской сфере (постановление Правления Национального банка Республики Беларусь от 20.11.2019 № 466)	Нацбанк	Киберриски в банковской деятельности

Окончание табл. 4.2

Период	Название документа (организации), год принятия (создания)	Институт регулирования	Основной объект регулирования в сфере цифровизации
Первый уровень (2016–2020 годы)	Указ «О совершенствовании государственного регулирования в области защиты информации» Президента Республики Беларусь (от 09.12.2019 № 449)	ПР	Криптографическая защита информации
	Введены в действие следующие государственные стандарты Республики Беларусь: СТБ 34.101.73-2017, СТБ 34.101.74-2017, СТБ 34.101.75-2017, СТБ 34.101.76-2017, СТБ 2518-2017, СТБ 34.101.14-2017, СТБ 34.101.30-2017, СТБ 34.101.37-2017	ОАЦ	Защита информации
Второй уровень (2021 – н. в)	Подпрограммы «Информационная безопасность» и «Цифровое доверие» в рамках Государственной программы «Цифровое развитие Беларуси» на 2021–2025 годы»	ОАЦ	Программные и программно-аппаратные средства защиты информационных ресурсов, информационных и телекоммуникационных систем
	Концепция безопасного функционирования объектов банков, небанковских кредитно-финансовых организаций, открытого акционерного общества «Банк развития Республики Беларусь» и безопасности оказания банковских услуг (постановление Правления Национального банка Республики Беларусь 23.03.2021 № 69)	Нацбанк	Защита цифровой инфраструктуры и информации
	Закон «О защите персональных данных» (от 07.05.2021 № 99-З)	Пар, ОАЦ	Цифровые персональные данные
	Национальный центр защиты персональных данных, в соответствии с Указом № 422 от 28 октября 2021 года «О мерах по совершенствованию защиты персональных данных»	ПР, ОАЦ	
	Указ Президента «О кибербезопасности» (в стадии разработки, план на июнь 2022 года)	ПР, ОАЦ	Обеспечение кибербезопасности

Примечание. Сокращения: ПР – Президент Республики Беларусь; Прав – Правительство Республики Беларусь; Пар – Парламент Республики Беларусь; СБ – Совет Безопасности Республики Беларусь; ОАЦ – Оперативно-аналитический центр; Минсвязи – Министерство связи и коммуникаций Республики Беларусь; Нацбанк – Национальный банк Республики Беларусь; Госстандарт – Государственный комитет по стандартизации Республики Беларусь.

В рамках утвержденной в 2019 году Концепции информационной безопасности Республики Беларусь [1057] предложены такие определения в сфере цифровых угроз, как кибератака, кибербезопасность, киберинцидент, кибертерроризм, киберустойчивость. В документе отмечено, что цифровая трансформация экономики является важнейшей составляющей формирования информационного общества и одним из главных направлений развития Республики Беларусь, в результате которого в ближайшие десятилетия все отрасли, рынки, сферы жизнедеятельности государства должны быть переориентированы на новые цифровые экономические модели. Вместе с тем политическая и социально-экономическая сферы, общественная и военная безопасность становятся все более уязвимыми перед преднамеренными или случайными технологическими воздействиями. Повсеместное функционирование объектов промышленности, транспорта, энергетики, электросвязи, здравоохранения и систем жизнеобеспечения с автоматизированными системами управления ставит в прямую зависимость жизнь и здоровье населения, экологическую и социальную безопасность от их надежности и защищенности. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными. Отдельно отмечены угрозы и риски незаконного и необоснованного вмешательства в частную жизнь граждан, похищение персональных данных, компрометация реквизитов доступа и избыточное профилирование.

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

В рамках Государственной программы «Цифровое развитие Беларуси на 2021–2025 годы» [1021] утверждены подпрограммы «Информационная безопасность» и «Цифровое доверие», в соответствии с которыми одним из важнейших условий успешного развития государства названо укрепление доверия и безопасности к техническим решениям на основе ИТ, а также к государственным

электронным сервисам, включая государственные информационные системы (цифровые платформы). Предполагается реализация таких мероприятий, как:

1) разработка и внедрение программных и программно-аппаратных средств защиты информационных ресурсов, информационных и телекоммуникационных систем;

2) формирование и совершенствование технических условий для надежной идентификации и удостоверения данных в рамках оказания государственных услуг и осуществления административных процедур в электронной форме.

В результате реализации указанных мероприятий, как предполагается разработчиками программы, будут обеспечены повышение уровня информационной безопасности данных и технологий в рамках созданной цифровой информационной экосистемы, конкурентоспособность отечественных разработок и технологий информационной безопасности, выстроена эффективная система защиты прав и законных интересов граждан, бизнеса и государства от угроз информационной безопасности [1020].

В 2019 году Национальным банком Республики Беларусь утверждена Концепция обеспечения кибербезопасности в банковской сфере, направленная на гарантирование кибербезопасности банков, небанковских кредитно-финансовых организаций, ОАО «Банк развития Республики Беларусь». Данный документ вводит понятие «киберриск» в отношении банковской деятельности и обозначает «потенциальную возможность (вероятность) для банка, Национального банка понести потери (убытки), иные дополнительные затраты, не получить запланированные доходы вследствие противоправных действий лица либо группы лиц, совершенных посредством использования информационных технологий, в целях несанкционированного доступа к объектам информационной инфраструктуры банка, Национального банка и направленных на нарушение конфиденциальности, целостности, доступности, подлинности и сохранности защищаемой информации» [1058]. Среди основных отраслевых киберугроз выделяются: воздействие через аппаратные уязвимости, компьютерный шпионаж, целенаправленные кибератаки, клиент-ориентированные кибератаки.

В соответствии с мировыми тенденциями государственной защиты цифровых персональных данных, в мае 2021 года в Беларуси

принят новый закон «О защите персональных данных»[66], в котором с ноября 2021 года введены следующие требования к операторам:

1) обеспечивать соразмерность обработки персональных данных заявленным целям их обработки;

2) принимать меры по обеспечению достоверности обрабатываемых персональных данных, при необходимости обновлять их (а также корректировать по запросам субъектов данных);

3) хранить персональные данные не дольше, чем это требуют заявленные цели обработки;

4) предоставлять субъекту данных информацию обо всех условиях обработки персональных данных;

5) получать согласие на обработку персональных данных от субъектов данных[67];

6) обеспечивать защиту персональных данных;

7) при обработке специальных персональных данных принимать комплекс мер, направленных на предупреждение рисков, которые могут возникнуть при этом, для прав и свобод субъектов персональных данных;

8) соблюдать процедуры и условия трансграничной передачи данных и пр. [1059].

Аналогично европейскому регулированию сферы защиты персональных данных (GDPR), белорусское законодательство вводит новые требования к обработке цифровых персональных данных, включая:

а) назначение лица или отдела, ответственного за защиту данных;

б) разработку политики компании в отношении обработки данных и предоставление доступа к ней для неограниченного круга лиц;

в) обучение работников работе с персональными данными и др. [1060].

В соответствии с Указом № 422 от 28 октября 2021 года в Беларуси создан Национальный центр защиты персональных данных, который наделен правом проводить проверки соблюдения законодательства о персональных данных, выносить предписания об устранении выявленных нарушений, требовать прекращения обработки персональных данных.

Защита персональных данных коснется и цифровизации медицины в стране. В рамках единой электронной инфосистемы

[66] Закон от 07.05.2021 № 99-З «О защите персональных данных». Режим доступа: https//etalonline.by. – Дата доступа: 19.09.2021

[67] Согласие должно быть информированным, свободным, однозначным выражением воли, пользователю должна быть предоставлена определенная информация перед тем, как он даст согласие (наименование оператора, цели обработки, перечень данных, срок и т. д.), разъяснены последствия дачи и отказа от дачи согласия.

здравоохранения Беларуси для обеспечения сохранности данных предполагается обезличивание информации путем введения идентификаторов, замены состава и декомпозиции[68] [1019].

Государственное институциональное регулирование и управление в области информации, информатизации и защиты информации осуществляются Президентом Республики Беларусь, Советом Министров Республики Беларусь, Национальной академией наук Беларуси, Оперативно-аналитическим центром при Президенте Республики Беларусь, Министерством связи и информатизации Республики Беларусь, иными государственными органами в пределах их компетенции [1058].

Уполномоченным органом по управлению сетью электросвязи общего пользования в Республике Беларусь является оперативно-аналитический центр (ОАЦ) при Президенте Республики Беларусь [1061]. ОАЦ осуществляет регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь, или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

Кроме того, данное государственное учреждение осуществляет ряд функций в рамках защиты критической инфраструктуры[69] Республики Беларусь, включая:

1) определение порядка технической и криптографической защиты информации, обрабатываемой на критически важных объектах

---

[68] Осуществлять обезличивание персональных данных будет оператор централизованной информационной системы здравоохранения после ввода ее в промышленную эксплуатацию. Ввод системы намечен на май 2023 года.

[69] Вопросы безопасности критических инфраструктур в Республике Беларусь регулируются Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации»), утверждено Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации. Указом определено понятие «критически важный объект информатизации» следующим образом: «критически важный объект информатизации – объект информатизации, который на основании критериев отнесения объектов информатизации к критически важным объектам информатизации и показателей уровня вероятного ущерба национальным интересам Республики Беларусь в политической, экономической, социальной, информационной, экологической и иных сферах включен в Государственный реестр критически важных объектов информатизации». Защита критически важных объектов и их совокупности, которую принято называть критически важной инфраструктурой или критической инфраструктурой, представляет собой одну из наиболее важных задач обеспечения национальной безопасности. Защита критически важных объектов включает проведение мероприятий, которые должны обеспечить их сохранение в случае различных воздействий природного или техногенного характера.

информатизации, в том числе порядка проведения аудита систем информационной безопасности критически важных объектов информатизации;

2) ведение Государственного реестра критически важных объектов информатизации, а также предоставление сведений из него;

3) выдача письменных предписаний об устранении организациями выявленных нарушений[70] и (или) приостановление (прекращение) функционирования критически важного объекта информатизации;

4) разработка проектов актов законодательства, в том числе обязательных для соблюдения технических нормативных правовых актов, и принятие таких актов по вопросам технической и криптографической защиты информации[71];

5) иные полномочия[72] в сфере технической и криптографической защиты информации[73].

---

[70] На основе Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации»), и иных нормативных правовых актов в сфере технической и криптографической защиты информации.

[71] ОАЦ по результатам выполнения ГНТП «Защита информации – 3» разработаны и введены в действие следующие государственные стандарты Республики Беларусь: СТБ 34.101.73-2017 «Информационные технологии. Методы и средства безопасности. Межсетевые экраны. Общие требования»; СТБ 34.101.74-2017 «Информационные технологии. Системы сбора и обработки данных событий информационной безопасности. Общие требования»; СТБ 34.101.75-2017 «Информационные технологии. Системы обнаружения и предотвращения вторжений. Общие требования»; СТБ 34.101.76-2017 «Информационные технологии. Методы и средства безопасности. Системы обнаружения и предотвращения утечек информации из информационных систем. Общие требования»; СТБ 2518-2017 «Специальные компьютерные системы, используемые при проведении электронных лотерей и электронных интерактивных игр. Технические требования»; СТБ 34.101.14-2017 «Информационные технологии и безопасность. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования»; СТБ 34.101.30-2017 «Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация»; СТБ 34.101.37-2017 «Информационные технологии и безопасность. Методы и средства безопасности. Системы управления сайта. Общие требования» (Научно-техническая деятельность. – Режим доступа: https://oac.gov.by/activity/technical-and-cryptographic-information-protection/scientific-and-technical-activities. – Дата доступа: 13.02.2022).

[72] В соответствии с Положением о технической и криптографической защите информации, утвержденным Указом Президента Республики Беларусь от 16.04.2013 № 196 «О некоторых мерах по совершенствованию защиты информации» (в редакции Указа Президента Республики Беларусь от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации»), и иными законодательными актами.

При оценке рисков в сфере информационной безопасности ОАЦ руководствуется методологией, основанной на отдельных критических показателях уровня вероятного ущерба по пяти основным сферам: политической, экономической, социальной, информационной и экологической [1062]. В экономической плоскости в качестве критериев оценки информационного объекта выделен потенциальный ущерб более 100 тыс. базовых величин, для расчетных банковских систем и энергосистем – прекращение или нарушение функционирования более двух часов.

Для противодействия киберпреступности в Беларуси внедрены около 2 тыс. разработок и программных комплексов по защите информации, которые позволяют обнаруживать вредоносное ПО, его блокировать и пресекать другие преступные действия.

Разработку цифровых технических средств защиты информации в Республике Беларусь осуществляет учреждение ОАЦ – Научно-производственное республиканское унитарное предприятие научно-исследовательский Институт технической защиты информации (НИИ ТЗИ). Данная организация проводит аттестацию объектов информатизации[74], сертификацию и государственную экспертизу[75], аудит информационной безопасности[76].

Уполномоченным правоохранительным органом по борьбе с киберпреступностью является Главное управление МВД по противодействию киберпреступности («Управление К»). По данным этого учреждения, в 2020 году в Беларуси зарегистрировано свыше 25,5 тыс. киберпреступлений с нарастающей динамикой (рис. 4.3), к уголовной ответственности привлечены 1592 человека [1063]. Пострадавшими от данного вида преступлений в Беларуси в 2020 году стали около 100 тыс. человек[77].

---

[73] Общие сведения. – Режим доступа: https://oac.gov.by/activity/critical-information-objects/technical-and-cryptographic-information-protection/general-information-kvoi. – Дата доступа: 08.02.2022.

[74] Выполнение комплекса организационно-технических мероприятий и работ, осуществляемых до ввода в эксплуатацию объекта информатизации, в результате которых документально подтверждается соответствие объекта информатизации требованиям нормативных правовых актов по технической защите государственных секретов.

[75] Испытания продукции (средств защиты информации) на соответствие техническим нормативным правовым актам (ТНПА), а также заявленным показателям (характеристикам) в области технической защиты информации.

[76] Аудит информационной безопасности – это системный процесс получения объективных качественных и количественных оценок текущего состояния корпоративной информационной системы в соответствии с определенными критериями информационной безопасности.

[77] Необходима надежная защита от киберпреступности. – Режим доступа: https://www.sb.by/articles/informatsiya-bez-opasnosti3445.html. – Дата доступа: 27.05.2021.

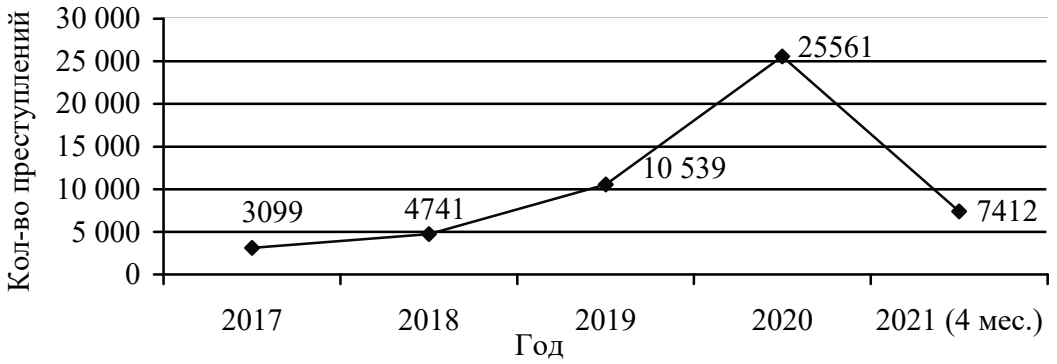


Рис. 4.3. **Количество киберпреступлений в Республике Беларусь за период 2017–2021 годы** [1064]

В 2018–2020 годах предприятиям причинен ущерб на сумму более 2 млн рублей, при этом за четыре месяца 2021 года сумма причиненного киберпреступниками ущерба – более 290 тыс. рублей[78].

Вместе с тем, по данным исследования компании McAfee [832], сумма потенциальных потерь от киберпреступлений составляет для развитых в сфере ИТ стран от 0,7 до 0,9% ВВП в год (что при экстраполяции относительно Республики Беларусь дает расчетный показатель в размере около 1 млрд рублей в год[79]).

Причинами роста в Беларуси киберпреступлений называют [1022] ускорение цифровизации финансового сектора и увеличение доли безналичных расчетов. Основными видами киберпреступлений, по данным правоохранительных органов[80], являлись шифрование коммерческой информации, подмена реквизитов при переводе средств, социальная инженерия: «вишинг»[81] и «фишинг»[82].

---

[78] Как защититься от киберпреступников. – Режим доступа: https://www.sb.by/articles/zaslon-dlya-kiberataki3.html. – Дата доступа: 03.06.2021.

[79] В зависимости от уровня продвинутости стран – от 0,7–0,9% ВВП для Европы, США, Японии; Азии и Л. Америки – от 0,25–0,55%; Африки и Ближнего Востока – от 0,06–0,18. По оценкам ЕС, более 12% всех европейских компаний подверглись атакам киберпреступников [238].

[80] Главное управление по противодействию киберпреступности КМ МВД РБ предупреждает. – Режим доступа: https://www.mrik.gov.by/glavnoe-upravlenie-po-protivodejstviyu-kiberprestupnosti-km-mvd-rb-preduprezhdaet. – Дата доступа: 13.02.2022.

[81] Вишинг – метод кибермошенничества, предполагающий телефонную коммуникацию жертвы с преступниками, выдающими себя за сотрудников банка, покупателей и т. д. и выманивающих у держателя платежной карты конфиденциальную информацию.

[82] Фишинг – метод кибермошенничества, предполагающий рассылку электронных писем от имени популярных брендов, банков или внутри социальных сетей, в которых содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом.

В данном контексте важно отметить низкий рейтинг Республики Беларусь (89-е место) в Глобальном индексе кибербезопасности ITU[83], который оценивает способность стран противостоять угрозам кибербезопасности [1065]. Страна получила крайне низкие оценки по таким показателям, как обучение в сфере кибербезопасности, разработка национальных стратегий в сфере кибербезопасности, технические возможности национальных и отраслевых регуляторов; и средние оценки по показателям: нормативное регулирование в отношении кибербезопасности и противодействия киберпреступности, сотрудничество между агентствами, компаниями и государствами.

Для обеспечения специализированной защиты финансового сектора экономики Национальным банком Беларуси в 2018 году создан центр мониторинга и противодействия компьютерным атакам в кредитно-финансовой сфере (FinCERT.by) [1066]. Основными задачами FinCERTby являются:

1) организация, координация и осуществление оперативного взаимодействия Национального банка с банками и иными организациями по вопросам противодействия кибератакам и мошенничеству с использованием электронных платежных инструментов и средств платежа;

2) сбор и анализ данных о кибератаках, киберугрозах, уязвимостях информационной инфраструктуры банков, а также о мошенничестве с использованием электронных платежных инструментов и средств платежа, подготовка аналитических материалов;

3) установление требований к обеспечению защиты объектов информационной инфраструктуры банков, совершенствование методологии, направленной на противодействие киберугрозам и мошенничеству с использованием электронных платежных инструментов и средств платежа [1058].

С целью укрепления международного взаимодействия данной организацией заключены соглашения о взаимодействии с Центральным банком России и Национальным банком Казахстана.

---

[83] Республика Беларусь в Глобальном индексе кибербезопасности (ITU) получила достаточно низкий рейтинг (89-е место из 194 стран). Низкие оценки страна получила по таким показателям, как обучение в сфере кибербезопасности, разработка национальных стратегий в сфере кибербезопасности, технические возможности национальных и отраслевых регуляторов. Средние оценки выставлены по следующим показателям: нормативное регулирование в отношении кибербезопасности и противодействия киберпреступности, сотрудничество между агентствами, компаниями и государствами.

В рамках рекомендаций FATF[84], с целью контроля за деятельностью криптоплатформ в Республике Беларусь, администрация Парка высоких технологий в 2021 году назначена специальным уполномоченным государственным органом. Она получила дополнительные полномочия по контролю за деятельностью резидентов ПВТ, осуществляющих финансовые операции, направленные на пресечение незаконных финансовых операций в сфере высоких технологий.

Заключение

Таким образом, в Республике Беларусь созданы основы нормативной базы для регулирования сферы цифровой безопасности, определены элементы государственного институционального регулирования и управления в области информации, информатизации и защиты информации. Основные направления развития национальной политики, регулирующей кибербезопасность, определены в Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы» в подпрограммах «Информационная безопасность» и «Цифровое доверие». Важным элементом адаптации национальной регуляторной среды к угрозам и вызовам цифровизации стало принятие Закона «О защите персональных данных» и создание соответствующего национального центра.

Вместе с тем специальное законодательство в области кибербезопасности в Беларуси в настоящее время отсутствует[85], кроме того, страна не ратифицировала Будапештскую конвенцию о киберпреступности, которая направлена на содействие международному сотрудничеству в данной сфере. В условиях трансграничного характера цифровых преступлений отсутствие международных соглашений объективно препятствует их эффективному противодействию.

Институциональный блок, связанный с киберзащитой, нуждается в серьезной трансформации с учетом нарастающего объема цифровых угроз и низкой подготовленностью, как показало международное исследование, национальной инфраструктуры к такого рода вызовам.

---

[84] Важно также отметить, что криптовалюты не облагаются налогами, как и доходы от операций с ними. Для проведения операций нужно подтвердить свою личность, и при необходимости проведения транзакций на сумму более 10 тыс. долларов США в эквиваленте в месяц следует подтверждать источники доходов.

[85] В 2022 году планируется к принятию Указ Президента о кибербезопасности.

В этой связи представляется целесообразным расширение взаимодействия Республики Беларусь со странами ЕАЭС по направлениям создания института, аналогичного Европейской организации кибербезопасности, с целью агрегирования международного опыта и лучших практик противодействия киберугрозам и формирования Союза безопасности в рамках данного интеграционного объединения. С учетом межотраслевого характера киберугроз представляется возможным создание также ассоциированного с организацией кибербезопасности – широкопрофильного центра компетенций в области промышленной, технологической и исследовательской цифровой безопасности и сети национальных координационных центров. Задачами данного института могут стать исследование текущих и будущих цифровых угроз, разработка соответствующих практик противодействия, подготовка специалистов для работы по соответствующим направлениям киберзащиты в органах государственного управления, объектах критической инфраструктуры и пр.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

880. Фридмен, М. Капитализм и свобода / М. Фридмен. – М.: Новое изд-во, 2006. – 240 с. – Режим доступа: http://pavroz.ru/files/friedmancap.pdf (дата обращения: 03.01.2020).

881. Клименко, А. В. Государственное регулирование экономики: вопросы теории и лучшая практика / А. В. Клименко, О. С. Минченко // Вопросы государственного и муниципального управления. – 2016. – № 3. – С. 7–30. – Режим доступа: https://vgmu.hse.ru/data/2016/10/06/1122683343/%D0%9A%D0%BB%D0%B8%D0%BC%D0%B5%D0%BD%D0%BA%D0%BE,%20%D0%9C%D0%B8%D0%BD%D1%87%D0%B5%D0%BD%D0%BA%D0%BE%203-2016.pdf (дата обращения: 04.12.2019).

882. Ashby, W. R. An Introduction to Cybernetics / W. R. Ashby. – London: Chapman & Hall, 1956. – URL: http://pespmc1.vub.ac.be/books/IntroCyb.pdf (date of access: 22.10.2021).

883. Ходжсон, Д. Экономическая теория и институты / Д. Ходжсон. – М.: Дело, 2003. – 464 с.

884. Новикова, И. В. Глобализация, государство и рынок: ретроспектива и перспектива взаимодействия / И. В. Новикова. – Минск: Акад. упр. при Президенте Респ. Беларусь, 2009. – 218 с.

885. Воробьева, И. П. Государственное регулирование национальной экономики: учеб. пособие / И. П. Воробьева. – Томск: Изд. дом ТГУ, 2014. – 292 с. – Режим достапа: https://core.ac.uk/download/pdf/287483131.pdf (дата обращения: 15.10.2020).

886. Хавина, С. А. Государственное регулирование экономики / С. А. Хавина // Большая российская энциклопедия. – Режим достапа: https://bigenc.ru/economics/text/2373038 (дата обращения: 24.05.2021).

887. The Committee for Economic Development of the Conference Board (CED): A Policy Statement by the Committee for Economic Development of the Conference Board. – 2017. – URL: https://www.ced.org/reports/regulation-and-the-economy (date of access: 25.02.2019).

888. Вебер, М. История хозяйства: очерки всеобщей социальной истории / М. Вебер. – Пг.: Наука и школа, 1923. – 244 с.

889. Cowhey, P. Transforming Global Information and Communication Markets: The Political Economy of Innovation Cambridge /

P. Cowhey, J. Aronson, D. Abelson. – Cambridge: The MIT Press, 2009. – 341 p. – URL: http://klangable.com/uploads/books/book.pdf (date of access: 30.03.2022).

890. Verbruggen, P. Does Co-Regulation Strengthen EU Legitimacy? / P. Verbruggen // European Law Journal. – 2009. – Vol. 15 (4). – P. 425–441.

891. OECD, Regulatory Policy and Governance: Supporting Economic Growth and Serving the Public Interest. – Paris: OECD Publishing, 2011. – 98 p.

892. Li, K.-W. Role of Government. Redefining Capitalism in Global Economic Development / K.-W. Li // Academic Press. – 2017. – P. 31–43.

893. Thelen, K. How Institutions Evolve: The Political Economy of Skills in Germany, Britain, the United States, and Japan / K. Thelen. – Cambridge: University Press, 2004. – 16 p. – URL: https://assets.cambridge.org/97805218/37682/sample/9780521837682ws.pdf (date of access: 24.04.2020).

894. The impact of technology-push and demand-pull policies on technical change – Does the locus of policies matter? / M. Peters [et al.] // Research Policy. – 2012. – Vol. 41. – P. 1296–1308.

895. Ding J. Deciphering China's AI dream: the context, components, capabilities, and consequences of China's strategy to lead the world in AI / J. Ding. – Oxford: Future of Humanity Institute, University Oxford, 2018. – P. 1–44.

896. Agile Regulation for the Fourth Industrial Revolution: A Toolkit for Regulators / World Economic Forum. – 2020. – 56 p. – URL: https://www.weforum.org/pages/agile-regulation-for-the-fourth-industrial-revolution-a-toolkit-for-regulators (date of access: 11.03.2021).

897. Виноградова, О. Три закона о цифре, приложение для экономии в дождливый день и роботы-кредиторы: обзор Bloomchain / О. Виноградова. – 2020. – Режим работы: https://bloomchain.ru/detailed/tri-zakona-o-tsifre-prilojenie-dlja-jekonomii-v-dojdlivyi-den-i-roboty-kreditory-obzor-bloomchain (дата обращения: 14.12.2020).

898. Ríos, M. Technological Neutrality and Conceptual Singularity / M. Ríos. – 2013. – 4 p. – DOI: 10.2139/ssrn.2198887.

899. Путин заявил о необходимости цифровой трансформации России. – 2020. – URL: https://tass.ru/ekonomika/10172635 (дата обращения: 05.01.2021).

900. Investigating of Competiotion in Digital Markets: Subcomittee on Antitrust, Commercial and Administrative Law of the Committee on

the Judiciary US House of Represantatives // Majority Staff Report and Recommendations. – 2020. – 450 p. – URL: https://judiciary.house.gov/uploadedfiles/competition_in_digital_markets.pdf (date of access: 20.09.2021).

901. Raskin, M. Digital Currencies, Decentralized Ledgers, and the Future of Central Banking: Working Paper 22238 / M. Raskin, D. Yermack; National Bureau of Economic Research. – 2016. – 18 p. – URL: http://www.nber.org/papers/w22238 (date of access: 20.06.2019).

902. China bans financial, payment institutions from cryptocurrency business: Financial Post. – 2021. – URL: https://financialpost.com/pmn/business-pmn/china-bans-financial-payment-institutions-from-cryptocurrency-business-2 (date of access: 20.05.2021).

903. Малин, Р. Гиперконтроль властей КНР: зачем он нужен и что ждет китайские компании / Р. Малин. – 2021. – Режим работы: https://quote.rbc.ru/news/article/612900359a79479925db5688 (дата обращения: 11.10.2021).

904. Шамардина, Л. Пекин опубликовал новый проект правил для китайских интернет-платформ / Л. Шамардина. – 2021. – Режим работы: https://thebell.io/pekin-opublikoval-novyj-proekt-pravil-dlya-kitajskih-internet-platform (дата обращения: 21.08.2021).

905. Tracy, R. U.S. Launches Task Force to Study Opening Government Data for AI Research / R. Tracy // Washington Street Journal. – 2021. – URL: https://www.wsj.com/articles/u-s-launches-task-force-to-open-government-data-for-ai-research-11623344400?mod=djemalertNEWS (date of access: 15.06.2021).

906. С 1 сентября Китай национализирует большие данные, собираемые всеми техгигантами в мире. – 2021. – Режим работы: https://www.secuteck.ru/news/s-1-sentyabrya-kitaj-nacionaliziruet-bolshie-dannye-sobiraemye-vsemi-tekhgigantami-v-mire (дата обращения: 20.06.2021).

907. Муравьева, А. Как закон о защите данных в Китае сработал против технологических компаний / А. Муравьева. – 2021. – Режим работы: https://www.forbes.ru/biznes/439513-kak-zakon-o-zasite-dannyh-v-kitae-srabotal-protiv-tehnologiceskih-kompanij (дата обращения: 15.09.2021).

908. Schechner, S. Amazon Faces Possible $425 Million EU Privacy Fine / S. Schechner // Washington Street Journal. – 2021. – URL: https://www.wsj.com/articles/amazon-faces-possible-425-million-eu-privacy-fine-11623332987?mod=djemalertNEWS (date of access: 13.06.2021).

909. Sahni, R. FinTech Landscape USA / R. Sahni. – 2021. – URL: https://iclg.com/practice-areas/fintech-laws-and-regulations/usa (date of access: 18.10.2021).

910. Castro D. Everything the U.S. government is doing to help the private sector build the Internet of Things / D. Castro, J. New. – 2016. – 18 p. – URL: http://www2.datainnovation.org/2016-federal-support-iot.pdf (date of access: 24.03.2021).

911. Consumer Attitudes Towards IoT Security: British Government, DCMS // Government response to the Secure by Design informal consultation / J. Stannard [et al.]. – London, 2020. – 33 p.

912. NITI Aayog: National strategy for artificial intelligence: AIFORALL Discussion Paper. – 2018. – 115 p. – URL: https://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf (date of access: 20.06.2019).

913. Hon, W. Banking in the cloud: Part 1 – Part 2 – regulation of cloud as 'outsourcing' / W. Hon, C. Millard // Computer law & security review. – 2018. – Vol. 34. – P. 337–357. – DOI: 10.1016/j.clsr.2017.11.006.

914. Michaels, L. Regulation and Supervision in a Digital and Inclusive World. Handbook ofBlockchain / L. Michaels, M. Homer // Digital Finance, and Inclusion. – 2018. – Vol. 1. – P. 330–346. – DOI: 10.1016/B978-0-12-810441-5.00014-2.

915. Groot M. Information as the Fuel for Financial Services' Business Processes: A Primer in Financial Data Management / M. Groot. – 2017. – P. 65–106. – DOI:10.1016/B978-0-12-809776-2.00003-X.

916. Oduor, J. Financial Sector Regulation AND Governance in Africa / J. Oduor, J. Kebba // Extending Financial Inclusion in Africa. – Cambridge: Elsevier, 2019. – P. 137–163. – DOI:10.1016/B978-0-12-814164-9.00007-4.

917. Godwin AIntroduction to special issue – The twin peaks model of financial regulation and reform in South Africa // Law and Financial Markets Review. – 2017. – Vol. 11 (4). – P. 151–153.

918. Kathrin, H. China shift on online payment services / H. Kathrin // Financial Times. – 2010. – URL: https://www.ft.com/content/5986061a-7d65-11df-a0f5-00144feabdc0 (date of access: 25.06.2019).

919. FSC Introduces New Penalty Standards on Virtual Asset Service Providers. – 2021. – URL: https://www.fsc.go.kr/eng/pr010101/75536 (date of access: 15.03.2021).

920. Degerli, K. Regulatory Challenges and Solutions for Fintech in Turkey / K. Degerli // Procedia Computer Science. – 2019. – Vol. 158. – P. 929–937. – DOI: 10.1016/j.procs.2019.09.133.

921. Malinova, K. Do retail traders suffer from high frequency traders? / K. Malinova, A. Park, R. Riordan. – 2018. – 52 p. – URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID3100220_code1159860.pdf?abstractid=2183806&mirid=1 (date of access: 15.01.2018).

922. Haferkorn, M. The German high-frequency trading act: Implications for market quality / M. Haferkorn, K. Zimmermann. – 2014. – 34 p. – URL: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2603196_code1685487.pdf?abstractid=2514334.&mirid=1 (date of access: 30.07.2020).

923. Mas, I. Bitcoin-Like Protocols and Innovations / I. Mas, D. Lee, K. Chuen // Handbook of Digital Currency. – Amsterdam: Elsevier, 2015. – P. 419–451.

924. Cryptocurrency. Enforcement Taskforce: U.S. Department of Justice: Report of the attorney general's cyber digital task force. – 2020. – 83 p.

925. SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering: Press Release № 2020–338 U.S. Securities and Exchange Commission. – 2020. – URL: https://www.sec.gov/news/press-release/2020-338 (date of access: 07.01.2021).

926. Report on Srablecoins / US President's Working Group on Financial Markets, Federal Deposit Insurance Corporation, Office of Comptroller of the Currence. – 2021. – 26 p. – URL: https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf (date of access: 02.02.2022).

927. U.S. regulators speak on stablecoin and crypto regulation. – 2021. – URL: https://www.davispolk.com/insights/client-update/us-regulators-speak-stablecoin-and-crypto-regulation (date of access: 13.12.2021).

928. Charfeddine, L. Investigating the dynamic relationship between cryptocurrencies and conventional assets: Implications for financial investors / L. Charfeddine, N. Benlagha, Y. Maouchi // Economic Modelling. – 2020. – Vol. 85. – P. 198–217. – DOI: 10.1016/j.econmod.2019.05.016.

929. Bitcoin: Safe haven, hedge or diversifier? Perception of bitcoin q in the context of a country's economic situation – A stochastic volatility approach / A. Kliber [et al.] // Physica A: Statistical Mechanics and its Applications. – 2019. – Vol. 524 (C). – P. 246–257. – DOI: 10.1016/j.physa.2019.04.145.

930. FCA warns consumers of the risks of investments advertising high returns based on cryptoassets. – 2021. – URL: https://www.fca.org.uk/news/news-stories/fca-warns-consumers-risks-investments-advertising-high-returns-based-cryptoassets (date of access: 13.01.2021).

931. Toksabay, E. Bitcoin tumbles after Turkey bans crypto payments citing risks / E. Toksabay. – 2021. – URL: https://www.reuters.com/technology/turkey-bans-use-cryptocurrencies-payments-sends-bitcoin-down-2021-04-16/ (date of access: 18.04.2021).

932. Crawley, J. Argentina's Tax Authority Orders Crypto Exchanges to File Information on Transactions: Report / J. Crawley. – 2021. – URL: https://finance.yahoo.com/news/argentina-tax-authority-orders-crypto-111253107.html (date of access: 24.05.2021).

933. Wang, S. Integrated framework for information security investment and cyber insurance / S. Wang // Pacific-Basin Finance Journal. – 2019. – Vol. 57. – 12 p. – DOI: 10.1016/j.pacfin.2019.101173.

934. Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments / Department of the Treasury. – 2021. – URL: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf (date of access: 30.09.2021).

935. National Cyber-security Strategy 2016 to 2021 / Cabinet Office, HM Government. – 2016. – URL: www.gov.uk/government/ publications/national-cyber-security- strategy-2016-to-2021 (date of access: 02.08.2018).

936. Weber, R. Rose is a rose is a rose is a rose – what about code and law? / R. Weber // Computer Law & Security Review. – 2018. – Vol. 34 (4). – P. 701–706. – DOI: 10.1016/j.clsr.2018.05.005.

937. Zhang, H. A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services / H. Zhang, Z. Tang, K. Jayakar // Telecommunications Policy. – 2018. – Vol. 42 (5). – P. 409–420. – DOI: 10.1016/j.telpol.2018.02.004.

938. Qi, A. Assessing China's Cybersecurity Law / A. Qi, G. Shao, W. Zheng // Computer Law & Security Review. – 2018. – Vol. 34 (6). – P. 1342–1354. – DOI: 10.1016/j.clsr.2018.08.007.

939. Носов, С. Система кибербезопасности в Китае / С. Носов // Зарубежное военное обозрение. – 2021. – № 2. – С. 17–24 – Режим доступа: http://factmil.com/publ/strana/kitaj/sistema_kiberbezopasnosti_v_kitae_2021/59-1-0-1833 (дата обращения: 03.03.2022).

940. Cary D. China's National Cybersecurity Center CSET Issue Brief / D. Cary. – 2021. – 71 p. – URL: https://cset.georgetown.edu/

wp-content/uploads/CSET-Chinas-National-Cybersecurity-Center.pdf (date of access: 11.11.2021).

941. Ларина, Е. Китай готовится стать кибердержавой. Совет по внешней и оборонной политике / Е. Ларина, В. Овчинский. – 2021. – Режим доступа: http://svop.ru/main/38449/ (дата обращения: 07.08.2021).

942. Guidelines for determining critical information infrastructure (for Trial Implementation) / Cyberspace Administration of China [CAC]. – 2016. – URL: http://www.shasm.gov.cn/detail.asp?id=18438 (date of access: 16.12.2019).

943. Скрынникова, А. Group-IB предложила создать центр по борьбе с утечкой данных россиян / А. Скрынникова. – 2020. – Режим доступа: https://www.rbc.ru/technology_and_media/01/09/2020/5f48def79a794775a632fa73?from=from_main_1 (дата обращения: 16.09.2020).

944. Бурмистрова, С. Шохин оценил в 1 трлн. долларов затраты бизнеса из-за перехода на российский софт / С. Бурмистрова. – 2021. – Режим доступа: https://www.rbc.ru/business/15/04/2021/6076cad69a794766eaf20606 (дата обращения: 20.04.2021).

945. Степанова, Ю. Госсектор скинулся на защиту / Ю. Степанова, Н. Королев // Коммерсантъ. – 2021. – № 130. – С. 7. – Режим доступа: https://www.kommersant.ru/doc/4918309?tg (дата обращения: 30.07.2021).

946. Ruan, K. Case Study: Insuring the Future of Everything / K. Ruan // Digital Asset Valuation and Cyber Risk Management. – 2019. – Chapter 10. – P. 159–167. DOI: 10.1016/b978-0-12-812158-0.00010-7.

947. Understanding Cyber Insurance – A Structured Dialogue with Insurance Companies: EIOPA Report. – 2018. – 33 p. – URL: https://www.eiopa.europa.eu/sites/default/files/publications/reports/eiopa_understanding_cyber_insurance.pdf (date of access: 16.12.2019).

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

949. Цели в области устойчивого развития / ООН. – Режим доступа: https://www.un.org/sustainabledevelopment/ru/sustainable-development-goals/ (дата обращения: 22.02.2022).

950. Tobias, A. Global Crypto Regulation Should be Comprehensive, Consistent, and Coordinated / A. Tobias, H. Dong, N. Aditya. –

2021. – URL: https://blogs.imf.org/2021/12/09/global-crypto-regulation-should-be-comprehensive-consistent-and-coordinated/?utm_medium=email&utm_source=govdelivery (date of access: 13.12.2021).

951. Agile Nations Charter. – 2020. – 4 p. – URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942312/Agile_Nations_Charter.pdf (date of access: 13.01.2021).

952. May, A. Public Engagement: Nations Sign First Agreement to Unlock Potential of Emerging Tech / A. May // World Economic Forum. – 2020. – URL: https://www.weforum.org/press/2020/12/nations-sign-first-agreement-to-unlock-potential-of-emerging-tech (date of access: 13.12.2020).

953. G20 Global Smart Cities Alliance on Technology Governance. – URL: https://globalsmartcitiesalliance.org/?page_id=107 (date of access: 16.10.2020).

954. FATF хочет помочь криптобиржам в выявлении подозрительных сделок. – 2020. – URL: https://whattonews.ru/fatf-hochet-pomoch-kriptobirzham-v-vyjavlenii-podozritelnyh-sdelok/ (date of access: 27.09.2020).

955. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing: FATF Report. – 2020. – 24 p. – URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf (date of access: 19.09.2020).

956. Демидова, А. FATF сформулировала признаки подозрительной активности пользователей криптовалют / А. Демидова. – 2020. – Режим доступа: https://bits.media/fatf-sformulirovala-priznaki-podozritelnoy-aktivnosti-polzovateley-kriptovalyut (дата обращения: 28.09.2020).

957. Groot, M. Challenges and Trends in the Financial Data Management Agenda: A Primer in Financial Data Management / M. Groot. – 2017. – Chapter 4. – P. 107–126. – DOI: 10.1016/B978-0-12-809776-2.00004-1.

958. Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers: FATF Report. – 2021. – 46 p. – URL: https://www.fatf-gafi.org/media/fatf/documents/recommendations/Second-12-Month-Review-Revised-FATF-Standards-Virtual-Assets-VASPS.pdf (date of access: 04.08.2021).

959. Readout from a Treasury Spokesperson on Secretary Mnuchin's Discussion with G7 Finance Ministers and Central Bank Governors / U.S. Department of the Treasury. – 2020. – URL: https://home.treasury.gov/news/press-releases/sm1203 (date of access: 24.12.2020).

960. G20 Rome Leaders' Declaration. – 2021. – URL: https://www.consilium.europa.eu/media/52732/final-final-g20-rome-declaration.pdf (date of access: 11.11.2021).

961. The rise of digital money – a strategic plan to continue delivering on the IMF's mandate: IMF Staff Report. – 2021. – URL: https://www.imf.org/-/media/Files/Publications/PP/2021/English/PPEA2021054.ashx (date of access: 22.02.2022).

962. Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy / N. Kshetri // Telecommunications Policy. – 2017. – Vol. 41 (10). – P. 1027–1038. – DOI:10.1016/j.telpol.2017.09.003.

963. Директива 2000/31/ЕС Европейского парламента и Совета Европейского Союза «О некоторых правовых аспектах информационных услуг на внутреннем рынке, в частности, об электронной коммерции» (Директива об электронной коммерции) от 08.06.2000. – 37 с. – Режим доступа: http://www.eurasiancommission.org/ru/act/texnreg/depsanmer/consumer_rights/Documents/%D0%94%D0%B8%D1%80%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%B0%202000%2031%20%D0%95%D0%A1%20%D0%9E%D0%B1%20%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D1%82%D1%82%D0%BE%D1%80%D0%B3%D0%BE%D0%B2%D0%BB%D0%B5.pdf (дата обращения: 08.06.2020).

964. The European Commission Cloud Strategy: European Commission. – 2019. – 28 p. – URL: https://ec.europa.eu/info/sites/default/files/ec_cloud_strategy.pdf (date of access: 26.05.2019).

965. Online Platforms and the Digital Single Market Opportunities and Challenges for Europe. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2016) 288/2 – 2016. – 15 p. – URL: https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-288-EN-F1-1.pdf (date of access: 04.02.2022).

966. Benjamin M. What the draft European Union AI regulations mean for business: McKinsey Analytics / M. Benjamin [et al.]. – 2021. – 7 p. – URL: https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20analytics/our%20insights/what%20the%20draft%20european%20union%20ai%20regulations%20mean%20for%20business/what-the-draft-european-union-ai-regulations-mean-for-business.pdf?shouldIndex=false (date of access: 15.11.2021).

967. A Digital Single Market Strategy for Europe / European Commission. COM (2015)192. – 2015. – 20 p. – DOI: 10.1017/CBO9781107415324.004.

968. Stefanoski, D. Are platforms trading crypto-assets subject to MiFID II/MiFIR? / D. Stefanoski, O. Sahin. – 2019. – URL: https://www.newrealityblog.com/2019/01/22/are-platforms-trading-crypto-assets-subject-to-mifid-ii-mifir/ (date of access: 24.01.2019).

969. Colangelo, G. From fragile to smart consumers: Shifting paradigm for the digital era / G. Colangelo, M. Maggiolino // Computer Law & Security Review. –2019. – Vol. 35 (2). – P. 173–181. – DOI: 10.1016/j.clsr.2018.12.004.

970. Final draft amending Regulatory Technical Standards and Implementing Technical Standards EBA/RTS/2020/06. – 2020. – 41 p. – URL: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Draft%20Technical%20Standards/2020/RTS/885780/EBA%20RTS-ITS%20passport%20notification.pdf (date of access: 28.06.2020).

971. TARGET Services / European Central Bank. Eurosystem. – URL: https://www.ecb.europa.eu/paym/target/html/index.en.html (date of access: 28.07.2021).

972. Bitcoin and the GDPR: Allocating responsibility in distributed networks / T. Buocz [et al.] // Computer Law & Security Review. – 2019. – Vol. 35 (2). – P. 182–198. – DOI: 10.1016/j.clsr.2018.12.003.

973. Context information sharing for the Internet of Things: A survey / E. de Matos [et al.] // Computer Networks. – 2020. – Vol. 166. – 19 p. – DOI: 10.1016/jxomnet.2019.106988.

974. Convention on Cybercrime: European Treaty Series. – Budapest, 2001. – No. 185. – 22 p. – URL: https://rm.coe.int/1680081561, https://www.coe.int/en/web/cybercrime/parties-observers (date of access: 14.10.2020).

975. Convention on Cybercrime: Council of Europe. ETS. – Budapest, 2001. – No. 185. – URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 (date of access: 14.10.2020).

976. Proactive Risk Management through Improved Cyber Situational Awareness. European Comission: Horizon 2020. – 2016. – URL: https://cordis.europa.eu/project/rcn/202674_en.html (date of access: 15.11.2021).

977. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised

Crime 2021–2025 COM(2021) 170 final. – 2021. – 31 p. – URL: https://ec.europa.eu/home-affairs/sites/default/files/pdf/14042021_eu_strategy_to_tackle_organised_crime_2021-2025_com-2021-170-1_en.pdf (date of access: 22.04.2022).

978. Resource efficiency, privacy and security by design: A first experience on enterprise servers and data storage products triggered by a policy process / D. Polverini [et al.] // Computers & security. – 2018. – Vol. 76. – P. 295–310. – DOI: 10.1016/j.cose.2017.12.001.

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

980. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU / European Commission: Joint Communication to the European Parliament and the Council. JOIN (2017). – 2017. – URL: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52017JC0450 (date of access: 07.01.2020).

981. Криштаносов, В. Б. Формирование институциональной экосистемы цифровой экономики в ЕС и ЕАЭС: сравнительный анализ / В. Б. Криштаносов // Социальные новации и социальные науки. – 2022. – № 2. – С. 140–154.

982. Lewis, J. Aux armes, citoyens: Cyber security and regulation in the United States / J. Lewis // Telecommunications Policy. – 2005. – Vol. 29. – P. 821–830.

983. Cybersecurity Policies / European Comission. – 2020. – URL: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies (date of access: 15.11.2021).

984. On the identification and designation of European critical infrastructures and the assessment of the need to improve their protection / European Council. Council Directive 2008/114/EC of 8.12.2008. – 2008. – URL: https://eur-lex.europa.eu/eli/dir/2008/114/oj (date of access: 20.12.2020).

985. European Security Union / Europen Comission. – URL: https://ec.europa.eu/info/strategy/priorities-2019-2024/promoting-our-european-way-life/european-security-union_en (date of access: 10.02.2022).

986. Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU

Security Union Strategy. COM/2020/605 final. – 2020. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605 (date of access: 15.11.2021).

987. ARIES: Evaluation of a reliable and privacy-preserving European identity management framework / J. Bernabe [et al.] // Future Generation Computer Systems. – 2020. – Vol. 102. – P. 409–425. – DOI: 10.1016/j.future.2019.08.017.

988. Council Implementing Regulation (EU) 2020/1125 of 30 July 2020 implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States ST/9568/2020/INIT. – 2020. – URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2020.246.01.0004.01.ENG&toc=OJ:L:2020:246:TOC (date of access: 20.08.2021).

989. Cerulus, L. EU, US launch initiative against ransomware / L. Cerulus, C. Goujard. – 2021. – URL: https://www.politico.eu/article/eu-us-launch-ransomware-cooperation-group/ (date of access: 28.06.2021).

990. Imposing Costs for Harmful Foreign Activities by the Russian Government: White House Administration / Statements and Releases. – 2021. – URL: https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/ (date of access: 25.04.2021).

991. Черненко, Е. Двоичный кодекс / Е. Черненко // Коммерсант. – 2021. – № 189/П. – С. 1. – Режим доступа: https://www.kommersant.ru/doc/5038983?tg (дата обращения: 26.10.2021).

992. Phijaisanit, E. AEC and the Changing Economic Landscape: Issues, Prospects, and Potentials / E. Phijaisanit // Internationalization and Managing Networks in the Asia. – 2017. – Chapter 2. – P. 7–28. – DOI: 10.1016/B978-0-08-100813-3.00002-X.

993. We're Stronger When We're Connected. ASEAN ICT Masterplan 2015. – Jakarta: Association of Southeast Asian Nations, 2011. – 28 p. – URL: https://www.asean.org/wp-content/uploads/images/2012/Economic/TELMIN/ASEAN%20ICT%20Masterplan%202015.pdf (date of access: 01.04.2019).

994. Schwab, K. The Global Competitiveness Report: World Economic Forum / K. Schwab. – 2019. – 666 p. – URL: http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf (date of access: 05.01.2022).

995. Global ICT Regulatory Outlook. – Switzerland, 2020. – 86 p. – URL: https://www.itu.int/dms_pub/itu-d/opb/pref/D-PREF-BB.REG_OUT01-2020-PDF-E.pdf (date of access: 23.06.2021).

996. E-Government Survey 2020: Digital Government in the Decade of Action for Sustainable Development / United Nations. – 2020. – 364 p. – URL: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Full%20Report).pdf (date of access: 26.11.2021).

997. Стратегические направления развития евразийской экономической интеграции до 2025 года. – 2021. – Режим доступа: http://www.eurasiancommission.org/ru/nae/news/Pages/14-01-2021-1.aspx (дата обращения: 01.04.2021).

998. О стратегии развития евразийской интеграции. – 2020. – Режим доступа: https://www.belta.by/economics/view/strategija-razvitija-evrazijskoj-integratsii-pozvolit-po-novomu-reshat-mnogie-voprosy-mjasnikovich-419794-2020/ (дата обращения: 01.04.2021).

999. О Концепции создания условий для цифровой трансформации промышленного сотрудничества в рамках Евразийского экономического союза и цифровой трансформации промышленности государств – членов Союза. – 2018. – Режим доступа: https://pravo.by/document/?guid=3871&p0=F01800405 (дата обращения: 03.04.2021).

1000. Конференция Организации Объединенных Наций по торговле и развитию. – 2019. – 31 р. – Режим доступа: https://unctad.org/system/files/official-document/der2019_overview_ru.pdf (дата обращения: 02.04.2021).

1001. Совместный цифровой проект стран ЕАЭС «Работа без границ» стартует 1 июля / Министерство экономического развития Российской Федерации – 2021. – Режим доступа: https://www.economy.gov.ru/material/news/sovmestnyy_cifrovoy_proekt_stran_eaes_rabota_bez_granic_startuet_1_iyulya.html (дата обращения: 26.05.2021).

1002. Будущее Евразийского экономического Союза: цифровая трансформация и молодежь // Реалистическое моделирование: материалы научного семинара. – М., 2020. – 78 с. – Режим доступа: http://council.gov.ru/media/files/ZbX6cOYEoyToLLFtVxHA4pFRGtckkjdT.pdf (дата обращения: 03.04.2021).

1003. Заявление о цифровой повестке Евразийского экономического союза. – 2016. – 3 с. – Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Documents/%D0%9F%D1%80%D0%BE%D0%B5%D0%BA%D1%82%20%D0%97%D0%B0%D1%8F%D0%B2%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%BD%D0%B0%20%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D0%B0%D0%BD%D0%B8%D0%B8.pdf (дата обращения: 05.04.2021).

1004. Обзор совместного исследования Всемирного банка и Евразийской экономической комиссии. – 2018. – 30 с. – Режим доступа: http://www.eurasiancommission.org/rau/act/dmi/SiteAssets/%D0%9E%D0%B1%D0%B7%D0%BE%D1%80%20%D0%92%D0%91.pdf (дата обращения: 05.04.2021).

1005. Международный опыт применения песочниц. – 2018. – 33 с. – Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/workgroup/materials/Documents/%D0%9C%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D1%8B%D0%B9%20%D0%BE%D0%BF%D1%8B%D1%82%20%D0%BF%D1%80%D0%B8%D0%BC%D0%B5%D0%BD%D0%B5%D0%BD%D0%B8%D1%8F%20%D0%BF%D0%B5%D1%81%D0%BE%D1%87%D0%BD%D0%B8%D1%86.pdf (дата обращения: 05.04.2021).

1006. Страны ЕАЭС протестируют новую передовую технологию таможенного оформления товаров электронной торговли. – 2021. – Режим доступа: https://primepress.by/news/ekonomika/strany_eaes_protestiruyut_novuyu_peredovuyu_tekhnologiyu_tamozhennogo_oformleniya_tovarov_elektronno-33857/ (дата обращения: 08.06.2021).

1007. О проработке инициативы по созданию экосистемы цифровых транспортных коридоров Евразийского экономического союза: распоряжение Совета Евразийской экономической комиссии № 17 от 13 июля 2018 г. – Режим доступа: https://pravo.by/document/?guid=3871&p0=F41800233 (дата обращения: 29.03.2021).

1008. ЕАЭС запускает создание экосистемы цифровых транспортных коридоров и приглашает к партнерству всех заинтересованных лиц. – 2019. – Режим доступа: http://www.eurasiancommission.org/ru/nae/news/Pages/19-06-2019-2.aspx (дата обращения: 08.04.2021).

1009. Перечень сервисов для формирования экосистемы цифровых транспортных коридоров ЕАЭС. – 2020. – Режим доступа: http://www.eurasiancommission.org/ru/nae/news/Pages/24_11_2020-1.aspx. (дата обращения: 25.03.2021).

1010. Криштаносов, В. Б. Проблематика регулирования цифровой экономики: международный и наднациональный аспекты / В. Б. Криштаносов // Цифровизация: экономика и управление производством: материалы 86-й науч.-техн. конф. проф.-преподават. состава, научных сотрудников и аспирантов (с междунар. участием), Минск, 31 января – 12 февраля 2022 г. / отв. за издание И. В. Войтов. – Минск: БГТУ, 2022. – С. 11–14.

1011. Цифровая повестка ЕАЭС 2025. – 2018. – 2 с. – Режим доступа: http://www.eurasiancommission.org/ru/act/dmi/SiteAssets/%D0%92%D1%81%D0%B5%D0%BC%D0%B8%D1%80%D0%BD%D1%8B%D0%B9%20%D0%B1%D0%B0%D0%BD%D0%BA%20%D0%9F%D0%B5%D1%80%D1%81%D0%BF%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D1%8B%20%D0%B8%20%D0%A0%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D0%B8%D0%B8.pdf (дата обращения: 02.04.2021).

1012. Совместное заявление Председателя Правительства Российской Федерации и Премьер-министра Республики Беларусь о текущем развитии и дальнейших шагах по углублению интеграционных процессов в рамках Союзного государства. – Минск, Республика Беларусь, 2021. – Режим доступа: http://government.ru/news/43234/ (дата обращения: 13.10.2021).

1013. Шакель, Н. Юридические аспекты использования облачных технологий / Н. Шакель // Журнал международного права и международных отношений. – 2014. – № 4. – С. 3–8.

1014. Внесены изменения в концепцию перехода госорганов на использование облачных технологий. – 2019. – Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2019/december/43864/ (дата обращения: 27.12.2019).

1015. Об утверждении Государственной программы развития цифровой экономики и информационного общества на 2016–2020 годы: постановление Совета Министров Республики Беларусь № 235 от 23 марта 2016. – 2016. – Режим доступа: https://www.pravo.by/document/?guid=12551&p0=C21600235&p1=1 (дата обращения: 22.04.2021).

1016. О развитии цифровой экономики: Декрет Президента Республики Беларусь № 8 от 21 декабря 2017. – 2017. – Режим доступа: https://pravo.by/document/?guid=12551&p0=Pd1700008&p1=1&p5=0 (дата обращения: 23.04.2021).

1017. Создан Совет по развитию цифровой экономики (по информации Национального центра правовой информации Республики Беларусь). – 2018. Режим доступа: https://pravo.by/novosti/novosti-pravo-by/2018/march/28019/ (дата обращения: 17.03.2019).

1018. Формируя цифровое пространство: годовой отчет ЕЭК за 2017 год. – 2018. – 172 с. – Режим доступа: http://www.eurasiancommission.org/ru/Documents/%d0%93%d0%be%d0%b4%d0%be%d0%b2%d0%be%d0%b9%20%d0%be%d1%82%d1%87%d0%b5%d1%82%202017.pdf (дата обращения: 18.04.2021).

1019. Инструкция о порядке обезличивания персональных данных лиц, которым оказывается медпомощь: комментарий к Постановлению Минздрава от 28.05.2021 № 64. – 2021. – Режим доступа: http://minzdrav.gov.by/ru/novoe-na-sayte/kommentariy-k-postanovleniyu-minzdrava-ot-28-maya-2021-goda-64-/ (дата обращения: 05.06.2021).

1020. Проект Концепции Государственной программы «Цифровое развитие Беларуси на 2021–2025 гг. – 2020. – 49 с. – Режим доступа: https://www.mpt.gov.by/sites/default/files/proekt_koncepcii_gosudarstvennoy_programmy.pdf (дата обращения: 21.03.2022).

1021. Государственная программа «Цифровое развитие Беларуси» на 2021–2025 годы. – 2020. – Режим доступа: https://www.mpt.gov.by/ru/news/04-02-2021-6992 (дата обращения: 16.04.2021).

1022. Калечиц, Д. Л. Приоритетные направления цифрового развития и новации платежного рынка / Д. Л. Калечиц // Банкаўскі веснік. – 2021. – № 10. – С. 3–4.

1023. Услуги электросвязи на территории республики оказывают 188 операторов. – 2021. – Режим доступа: https://www.mpt.gov.by/ru/news/04-05-2021-7166 (дата обращения: 14.05.2021).

1024. Шорр, Е. Проект «умные города» Беларуси. Нормативные и организационные составляющие / Е. Шорр // Презентация Минсвязи Республки Беларусь на Форуме ITU. – 2021. – 20 с. – Режим доступа: https://www.itu.int/en/ITU-D/Regional-Presence/CIS/Documents/Events/2021/Minsk-SSC/ITU%20Forum%2016%20Mar%202021%20-%20Elena%20Shorr.pdf (дата обращения: 26.05.2021).

1025. EU4Digital: Поддержка цифровой экономики. – 2016. – Режим доступа: https://eufordigital.eu/ru/countries/belarus (дата обращения: 22.04.2021).

1026. Белорусская Финтех-экосистема / VISA, CIVITTA. – 2021. – 76 с. – Режим доступа: https://ru.calameo.com/read/005151365071c8e895680?view=book&page=1 (дата обращения: 25.10.2021).

1027. Электронное правительство 2020. Цифровое правительство в десятилетии действий по достижению устойчивого развития. С дополнением по реагированию на COVID-19 / Департамент по экономическим и социальным вопросам ООН. – Нью-Йорк, 2020. – 324 с. – Режим доступа: https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20-%20Russian.pdf (дата обращения: 23.12.2021).

1028. Global Innovation Index 2020 / Cornell University, INSEAD, and the World Intellectual Property Organization (WIPO). – Geneva,

Switzerland, 2020. – 448 p. – URL:https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2020.pdf (date of access: 21.03.2022).

1029. Global Innovation Index (GII) 2021 / Cornell University, INSEAD, and the World Intellectual Property Organization (WIPO). – Geneva, Switzerland, 2021. – 226 p. – URL: https://www.wipo.int/edocs/pubdocs/en/wipo_pub_gii_2021.pdf (date of access: 21.03.2022).

1030. Абсолютный рекорд за всю историю парка. Экспорт ПВТ в 2020 году превысил 2,7 млрд. долларов. – 2021. – Режим доступа: https://park.by/press/news/absolyutnyy_rekord_za_vsyu_istoriyu_parka_eksport_pvt_v_2020_godu_prevysil_2_7_mlrd_dollarov/ (дата обращения: 15.03.2021).

1031. Убыточных компаний в ИТ и связи стало в 2 раза больше. Убытков – в 4. – 2021. – Режим доступа: https://dev.by/news/belstat-poschital-pribyl-i-ubytki-kompanii-v-it-i-svyazi (дата обращения: 28.02.2021).

1032. Резиденты ПВТ обновили рекорд по экспорту – $3,2 млрд за 2021 год – 2022. – Режим доступа: https://devby.io/news/pvt-obnovil-rekord-po-eksportu (дата обращения: 05.04.2022).

1033. EPAM объявила результаты деятельности за 4-й квартал и весь 2020 год. – 2021. – Режим доступа: https://careers.epam.by/newsroom/news/2021/epam-reports-results-for-fourth-quarter-and-full-year-2020 (дата обращения: 28.02.2021).

1034. Альфа-Банк и Mastercard запустили сервис перевода денег по номеру телефона для владельцев карт других банков. – 2021. – Режим доступа: https://belretail.by/news/alfa-bank-i-mastercard-zapustili-servis-perevoda-deneg-po-nomeru-telefona-dlya-vladeltsev-kart-drugi (дата обращения: 27.01.2021).

1035. Wargaming продала геймдев-студию Melsoft. По оценке СМИ, за сотни миллионов. – 2020. – Режим доступа: https://dev.by/news/wargaming-melsoft-coin-master (дата обращения: 28.12.2020).

1036. Что ждет рынок хостинга в Беларуси? Итоги года и ближайшие перспективы. – 2021. – Режим доступа: https://belretail.by/article/chto-jdet-ryinok-hostinga-v-belarusi-itogi-goda-i-blijayshie-perspektivyi (дата обращения: 24.01.2021).

1037. Янчис, В. Белорусский IT-бизнес открывает Вильнюс: учредители компании Cortlex рассказали о начале работы в Литве / В. Янчис, Д. Кишиневский. – 2021. – Режим доступа: https://www.delfi.lt/ru/news/economy/belorusskij-it-biznes-otkryvaet-vilnyus-uchrediteli-kompanii-cortlex-rasskazali-o-nachale-raboty-v-litve.d?id=86482615 (дата обращения: 24.02.2021).

1038. Сафронова, В. 60% стартапов из Беларуси отказались рассматривать страну как важный рынок / В. Сафронова. – 2021. – Режим доступа: https://rb.ru/news/belarus-startup-ecosystem/ (дата обращения: 20.06.2021).

1039. Сложный год // IMAGURU: стартапы Беларуси. – 2021. – 68 с. – Режим доступа: https://bel.biz/wp-content/uploads/2021/09/StartupBelarusReport2021-1.pdf (дата обращения: 21.03.2022).

1040. Эйчары загрустили. Остальные пока на позитиве // ИТ в Беларуси – 2020. – Ч. 3. – 2021. – Режим доступа: https://dev.by/news/it-v-belarusi-2020-3 (дата обращения: 18.06.2021).

1041. Объем рынка E-commerce в Беларуси вырос до 2,3 млрд рублей в 2020 году. – 2021. – Режим доступа: https://officelife.media/news/23242-obem-rynka-e-commerce-v-belarusi-vyros-do-2-3-mlrd-rubley-v-2020-godu/ (дата обращения: 25.01.2021).

1042. В этом году онлайн-продажи показали самые высокие темпы роста за последние несколько лет. – 2020. – Режим доступа: https://belretail.by/news/v-etom-godu-onlayn-prodaji-pokazali-samyie-vyisokie-tempyi-rosta-za-poslednie-neskolko-let (дата обращения: 03.01.2021).

1043. JavaScript тормозит. React растёт. «Ковидные» проекты не взлетели // ИТ в Беларуси – 2020. – Ч. 2. – 2021. – Режим доступа: https://dev.by/news/it-v-belarusi-2020-2 (дата обращения: 29.05.2021).

1044. Администрация ПВТ будет контролировать криптобиржи и крипту. – 2021. – Режим доступа: https://dev.by/news/administratsiya-pvt-budet-kontrolirovat-kriptobirzhi (дата обращения: 18.03.2021).

1045. Где легально купить биткоин в Беларуси и как быть с налогами? – 2021. – Режим доступа: https://finance.tut.by/news717525.html?c (дата обращения: 24.02.2021).

1046. Голикова, А. Экосистема финтеха Республики Беларусь: основные участники и особенности развития / А. Голикова // Банкаўскі веснік. – 2021. – № 10. – С. 61–72. – Режим доступа: https://www.nbrb.by/bv/arch/699.pdf (дата обращения: 18.12.2021).

1047. Белорусские банки будут продавать и покупать токены – эксперимент. – 2021. – Режим доступа: https://dev.by/news/eksperiment-tokeny-banki (дата обращения: 10.06.2021).

1048. В Беларуси появился Google Pay, но полноценный запуск планируется к лету. – 2021. – Режим доступа: https://belretail.by/news/v-belarusi-poyavilsya-google-pay-no-polnotsennyiy-zapusk-planiruetsya-k-letu (дата обращения: 25.02.2021).

1049. Токены – современный финансовый инструмент для инвестиций // Экономическая газета. – 2021. – Режим доступа: https://neg.by/novosti/otkrytj/investicii-v-belarusi-tokeny (дата обращения: 29.10.2021).

1050. В Беларуси заработали денежные переводы через Viber. Достаточно знать номер телефона получателя. – 2021. – Режим доступа: https://dev.by/news/belorusskie-polzovateli-mogut-perevodit-dengi-v-viber (дата обращения: 14.03.2021).

1051. Количество бесконтактных платежей в Беларуси за год выросло на 29% : исследование ЮMoney. – 2021. – Режим доступа: https://belretail.by/news/kolichestvo-beskontaktnyih-platejey-v-belarusi (дата обращения: 27.08.2021).

1052. Сервисы онлайн-заимствования появятся в Беларуси. – 2021. – Режим доступа: https://primepress.by/news/ekonomika/servisy_onlayn_zaimstvovaniya_poyavyatsya_v_belarusi_ukaz-33516/ (дата обращения: 05.06.2021).

1053. Указ Президента Республики Беларусь № 196 от 25 мая 2021 // Национальный правовой Интернет-портал Республики Беларусь. – 2021. – Режим доступа: https://pravo.by/document/?guid=12551&p0=P32100196&p1=1 (дата обращения: 05.06.2021).

1054. Digital Challengers in the next normal / McKinsey & Company. – 2020. – 72 p. – Режим доступа: https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-challengers-in-the-next-normal-in-central-and-eastern-europe (дата обращения: 05.05.2021).

1055. Марахина, И. Инвестиционная инфраструктура белорусской стартап-экосистемы: субъекты, проблемы и направления развития / И. Марахина // Банкаускі веснік. – 2020. – № 7. – С. 49–58.

1056. Beyond COVID-19 Advancing Digital Business Transformation in the Eastern Partner Countries / Organisation for Economic Co-operation 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).

1057. Концепция информационной безопасности Республики Беларусь: постановление Совета Безопасности Респ. Беларусь № 1 от 18 марта 2019. – 2019. – Режим доступа: https://pravo.by/upload/docs/op/P219s0001_1553029200.pdf (дата обращения: 25.05.2021).

1058. Концепция обеспечения кибербезопасности в банковской сфере: постановление Правления Нац. банка Респ. Беларусь № 466

от 20 ноября 2019. – 2019. – Режим доступа: https://www.nbrb.by/legislation/documents/koncepciya-kiberbezopasnosti.pdf (дата обращения: 25.03.2020).

1059. Шакель, Н. Новые подходы к защите персональных данных с 15 ноября 2021 года: комментарий к Закону № 99-З от 07.05.2021 «О защите персональных данных» / Н. Шакель. – 2021. – Режим доступа: https://bii.by/tx.dll?d=456664 (дата обращения: 20.06.2021).

1060. E-commerce в условиях нового Закона «О персональных данных»: чек-лист для ритейлеров. – 2021. – Режим доступа: https://belretail.by/news/e-commerce-v-usloviyah-novogo-zakona-o-personalnyih-dannyih (дата обращения: 05.07.2021).

1061. Лукашенко утвердил изменения в Закон «Об электросвязи» – новации касаются и угроз нацбезопасности. – 2021. – Режим доступа: https://www.belta.by/president/view/lukashenko-utverdil-izmenenija-v-zakon-ob-elektrosvjazi-novatsii-kasajutsja-i-ugroz-natsbezopasnosti-442675-2021/ (дата обращения: 13.06.2021).

1062. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь № 65 от 20 февраля 2020 «О показателях уровня вероятного ущерба национальным интересам Республики Беларусь». – 2020. – Режим доступа: https://oac.gov.by/public/content/files/files/law/prikaz-oac/2020%20-%2065.pdf (дата обращения: 17.04.2020).

1063. Киберпреступность в Беларуси / Белорусское телеграфное агентство. – 2021. – Режим доступа: https://www.belta.by/infographica/view/kiberprestupnost-v-belarusi-24963/ (дата обращения: 15.11.2021).

1064. Декада кибербезопасности / Департамент охраны МВД Республики Беларусь. – 2021. – Режим доступа: https://minsk.ohrana.gov.by/2021/05/12/%D0%B4%D0%B5%D0%BA%D0%B0%D0%B4%D0%B0-%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8/ (дата обращения: 03.06.2021).

1065. Global Cybersecurity Index 2020 // International Telecommunication Union (ITU). – Geneva: ITU, 2021. – 172 p. – URL: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf (date of access: 13.11.2021).

1066. Центр реагирования на компьютерные атаки в кредитно-финансовой сфере создан в Беларуси. – 2018. – Режим доступа: https://tvnews.by/comm/13541-centr-reagirovanija-na-kompjuternye-ataki-v-kreditno-finansovoj-sfere-sozdan-v-belarusi.html (дата обращения: 24.12.2019).

Научное издание

Криштаносов Виталий Брониславович

ЦИФРОВИЗАЦИЯ ЭКОНОМИКИ РУСПУБЛИКИ БЕЛАРУСЬ И НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ: СОВРЕМЕННЫЕ КОНЦЕПТУАЛЬНО-АНАЛИТИЧЕСКИЕ ПОДХОДЫ

Монография

В 2-х томах

Том 2

Редактор *Р. М. Рябая*
Компьютерная верстка *В. А. Маркушевская*
Дизайн обложки *П. П. Падалец*
Корректор *Р. М. Рябая*

Подписано в печать 25.01.2023. Формат $60\times84^{1}/_{16}$.
Бумага офсетная. Гарнитура Таймс. Печать ризографическая.
Усл. печ. л. 11,5. Уч.-изд. л. 12,0.
Тираж 100 экз. Заказ .

Издатель и полиграфическое исполнение:
УО «Белорусский государственный технологический университет».
Свидетельство о государственной регистрации издателя,
изготовителя, распространителя печатных изданий
№ 1/227 от 20.03.2014.
Ул. Свердлова, 13а, 220006, г. Минск.