

## РОЛЬ ЦИФРОВОЙ ЭКОНОМИКИ В УКРЕПЛЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВА

*С.Л. Шатров, канд. экон. наук, доц.*

*М.А. Дорошкова, студентка*

*Белорусский государственный университет транспорта, Гомель*

*В статье рассматриваются актуальность цифрового развития государства и роль цифровой экономики в укреплении экономической безопасности страны. Представлены основные тенденции автоматизации и цифровизации, а также основные группы рисков, возникающих в результате внедрения цифровых технологий.*

**Ключевые слова:** *цифровизация, цифровая экономика, экономическая безопасность, устойчивое развитие, прогнозирование, риски и угрозы, информационные технологии, конкурентоспособность, финансовая система.*

В современном мире цифровизация экономической сферы рассматривается как ключевой элемент для экономического роста и обеспечения национальной безопасности государства. В условиях стремительного прогресса информационных технологий, переход к цифровой экономике становится обязательным условием для ускорения темпов роста и повышения конкурентных позиций страны.

Отличительные особенности процесса использования цифровых технологий и построения цифровой экономики заключаются в следующем:

Использование активов, не имеющих физической формы, для повышения экономической эффективности деятельности.

Уделение большого внимания данным и информационным сведениям, их хранения и обработка на облачных платформах, что обеспечивает доступ для разных групп пользователей, масштаб использования и скорость загрузки.

Совершенствование способов взаимодействия с партнерами: поставщиками и покупателями, инвесторами, налоговыми и статистическими органами, иными государственными структурами, региональными компаниями и конкурентами.

Повсеместное развитие сети Интернет, изменяющей виды и формы взаимодействия в современном обществе.

Глобализация информационного обмена, появление новых инструментов продаж, организации хозяйственных отношений, открывающих новые рынки сбыта.

Построение управленческой системы по принципу самоорганизации: внедрение более гибких и адаптивных бизнес-моделей, позволяющих повысить эффективную производственную деятельность хозяйственного субъекта и выйти на самофинансирование.

Одним из важнейших аспектов цифровизации экономики является ее влияние на экономическую безопасность страны.

Экономическая безопасность – это совокупность инструментов и мер, обеспечивающих стабильное и устойчивое экономическое развитие государства, способных противодействовать внутренним и внешним угрозам [1].

Ключевым фактором, определяющим обеспечение экономической безопасности государства, является устойчивый экономический рост ведущих производственных предприятий. Устойчивое развитие субъектов хозяйствования не только создает фундамент для привлечения инвестиций, построения развитой рыночной инфраструктуры, но и обеспечивает прочность финансово-экономической системы и оперативность управленческих решений.

В связи с этим, отметим, что влияние цифровизации экономики на экономическую безопасность государства различно. С одной стороны, цифровизация открывает новые возможности и способствует росту уровня экономической безопасности. К примеру, внедрение цифровых технологий в производственные процессы может привести к увеличению эффективности и конкурентоспособности компаний. Это, в свою очередь, может быть причиной нарастания производственных мощностей и роста объемов выпуска продукции, развития экспортно-импортных отношений и, как следствие, укрепления внешнеэкономических связей. Вместе с этим, цифровые технологии являются одним из инструментов, способствующих переходу хозяйственных субъектов на новый уровень путем повышения качества выпускаемой продукции и оказываемых услуг, а также снижения издержек. [2].

С другой стороны, внедрение технологий цифровой экономики порождает появление широкого перечня рисков и угроз для экономической безопасности. Прежде всего, отметим риски кибератак на информационные сервисы крупных компаний, финансовых и банковских учреждений, платформы государственных предприятий и важную инфраструктуру страны. Такие инциденты вызывают искажения информационных потоков и (или) полное прекращение поступления данных на протяжении неопределенных промежутков времени, что нарушает рыночную динамику, создает неблагоприятные условия для экономического развития, ведет к утечке конфиденциальной информации, сбоям в работе систем и утрате контроля над важнейшими объектами.

Основной задачей обеспечения экономической безопасности в условиях стремительных изменений современного глобального пространства является прогнозирование вызовов и угроз, связанных с повсеместной цифровизацией. Характерные черты развития цифровой экономики включают наличие интеллектуальных ресурсов, увеличение значимости данных, сетевую структуру ведения бизнеса, масштабное внедрение интернета и международный характер обмена информацией.

Появление цифровых финансовых активов (ЦФА) стало одним из основных аспектов цифровой трансформации как в глобальной, так и в национальной экономике. Исследуя перспективы синергии между цифровыми национальными валютами и ЦФА, можно заметить широкие горизонты для международного движения капитала.

Виртуальные активы и их различные применения приобрели популярность благодаря технологии, позволяющей осуществлять финансовые операции с минимальными затратами и без посредников. Отсутствие валютных и юридических препятствий облегчает перемещение токенов в интернете. Поскольку виртуальные активы действуют на глобальном уровне, локальные ограничения их обращения в отдельных странах не способны существенно ограничить их распространение по всему миру.

Многообразие виртуальных активов представлено следующими их основными группами [3]:

Криптовалюты – это цифровое представление стоимости, которое может быть продано или передано и может использоваться для платежных или инвестиционных целей;

Стейблкоины – токены, курс которых поддерживается алгоритмом, обеспечивается иными финансовыми активами, валютами, имуществом;

Токены, выпускаемые в процессе ICO, – токены, имеющие эмитента, обязанного перед инвесторами по правам, предоставляемым этими токенами, имеющие свойства и подобию известных ценных бумаг, акций и облигаций;

Невзаимозаменяемые токены (NFT);

Производные финансовые инструменты на виртуальные активы, торгуемые на криптобиржах.

Криптовалюты представляют собой особый тип цифровых финансовых активов: согласно данным платформы Coinmarketcap, рыночная капитализация криптовалютного рынка превышает 1 триллион долларов США, а суточный объем торгов составляет около 50 миллиардов долларов. Анализ рейтингов показывает, что наибольшей инвесторской привлекательностью обладают такие криптовалюты, как Bitcoin, Ethereum, Polygon, Ripple и Polkadot [4].

Среди главных рисков, связанных с сектором виртуальных активов, можно выделить обширные нерегулируемые перемещения капитала из развивающихся стран через блокчейн-основные виртуальные платежные системы, уклонение от уплаты налогов, финансирование незаконной или криминальной деятельности, а также возможный отток капиталов из банков в сторону виртуальных активов, что может негативно сказаться на эффективности денежно-кредитной политики.

Виртуальные активы наиболее удобно применяются для переводов денежных средств, однако недостаточное регулирование и контроль таких операций, широкое распространение несистемных приложений для обмена криптовалют является одним из наиболее распространенных причин утечки капитала из государства в оффшорные юрисдикции.

Несмотря на то, что активное использование цифровых технологий является первоочередной причиной возникновения угроз в отношении экономической безопасности, именно цифровизация выступает надежным инструментом обеспечения защиты и сохранности информации. Современные технологии позволяют модернизировать производства, внедрять системы, эффективно распределяющие имеющиеся ресурсы, осуществлять поиск резервов и совершенствовать управленческие подходы к росту производительности работников и эффективности осуществления деятельности по реализационной политике. Покупатели, в свою очередь, получают доступ к представленному в наглядной форме ассортименту выпускаемой продукции, могут легко сопоставлять характеристики товаров, их качество, цену и дополнительные предложения продавца, что существенно экономит время и сокращает затраты.

Среди ключевых технологических направлений в области цифровизации промышленности можно выделить следующие:

- широкое использование умных (квантовых) сенсоров в оборудовании и производственных системах (технологии индустриального Интернета вещей);
- переход к автоматизированному производству и активное внедрение роботов;
- перенос хранения данных и вычислений с локальных серверов на распределенные платформы (облачные технологии);
- полная автоматизация и интеграция производственных и управленческих процессов в единую информационную архитектуру (от оборудования до высших эшелонов власти);

- установка обязательной цифровой технической документации и внедрение электронного документооборота (безбумажные технологии);
- цифровое проектирование и моделирование технологических процессов, продуктов и объектов на протяжении всего их жизненного цикла (использование инженерного ПО);
- внедрение аддитивных технологий вместо традиционного резания материалов (3D-печать);
- использование мобильных технологий для мониторинга и управления процессами как в быту, так и на производстве;
- развитие промышленных аналитических технологий;
- реализация промышленных товаров через Интернет.

Новая цифровая эпоха характеризуется повышенной ролью автоматизации всех производственных и технических процессов. Данные изменения сопровождаются высвобождением производственных ресурсов, что является положительным фактором для бизнеса, т.к. приводит к снижению расходов и повышению производительности.

Однако, такая тенденция ведет к несоответствию между уже сложившейся процессной работой и новыми задачами и потребностями, большую роль играет недостаточное нормативно-правовое регулирование и необходимость в повышении квалификационных навыков задействованного персонала.

Внедряя технологии цифровизации бизнес-процессов, субъект хозяйствования может столкнуться со следующими группами рисков:

Интернет-вещей – риски данной категории связаны с организацией недостаточной защиты в случае несанкционированного доступа и кибератак, а также применение технологий способом, противоречащим законодательству конкретного государства.

Искусственный интеллект – риски, связанные с использованием данной технологии в корыстных целях, дестабилизация экономической системы, социальная напряженность, вызванная заменой большой доли рабочих мест технологиями роботизации и автоматизированием производственных процессов. К данной группе рисков также относятся незаконное слежение за гражданами и утечка их конфиденциальной информации.

Блокчейн – риски, относящиеся к данной группе, заключаются в угрозах безопасности информационной системы и инфраструктуры, построенной на ее основе, а также в необратимости информации в сети (невозможность исправления ошибок, некорректной информации), использованием токенов для отмывания денег и финансирования террористической деятельности.

Импортная микроэлектроника – риски, связанные с применением импортного программного обеспечения, баз данных, а также компьютерной техники, используемых в разных странах. В данном случае существует угроза содержания скрытых чипов для незаконных действий.

Облачные ресурсы – риски, зависящие от надежности работы телекоммуникационной инфраструктуры, а также понижение уровня контроля из-за распределения ответственности между пользователями.

Риски, связанные со стабильностью каналов передачи данных и их надежностью (в т.ч. сети Интернет) [5].

Учитывая вышеизложенное, следует подчеркнуть, что цифровая трансформация всех аспектов общества требует усиленных мер по обеспечению кибербезопасности и защиты

личной информации. Поддержка со стороны государства позволит максимизировать положительное воздействие цифровых технологий. Ключевыми направлениями такой поддержки выступают способы повсеместного информирования населения о потенциальных угрозах, взаимодействие с гражданами на постоянной основе, проведение консультационных встреч по вопросам использования информационных систем, гарантирующих безопасность их данных.

Ключевыми аспектами политики государства по укреплению экономической безопасности выступают следующие положения:

- разработка и совершенствование нормативно-правовой базы для цифрового развития экономики;
- разработка и внедрение собственного программного обеспечения на уровне государства;
- расширение цифровой инфраструктуры;
- совершенствование образовательных программ и повышении квалификационных навыков персонала [6];
- поддержка внедрения инновационных технологий;
- привлечение инвестиционных потоков в цифровые решения;
- инновационное развитие электронного производства;
- разработка мероприятий, направленных на повышение репутации, деловой активности, конкурентоспособности предприятия в сфере информационных технологий;
- регулирование этических аспектов размещения различных видов контента в интернете [7];
- развитие цифровых экосистем, форм экономической деятельности с гибкими потоками взаимодействия и др.

Таким образом, цифровизация выступает одним из наиболее динамичных факторов развития современного общества, так как, с одной стороны, открывает новые возможности и способствует росту уровня экономической безопасности, а с другой – порождает появление широкого перечня рисков и угроз. Среди ключевых вызовов экономической безопасности можно назвать цифровое неравенство, нехватку развитой цифровой экосистемы, изменения на рынке труда, а также киберугрозы. Полное использование преимуществ цифровизации и недопущение ее потенциальных угроз будут способствовать устойчивому экономическому росту, улучшению качества жизни населения и укреплению экономической безопасности. Как результат, экономическая безопасность государства положительным образом отразится на независимости, стабильности и эффективности функционирования страны.

#### Список использованных источников

1. Тесленко, И. Б. Цифровые технологии как современный фактор обеспечения экономической безопасности / И. Б. Тесленко, О. Б. Дигилина // Индустриальная экономика. 2022. №3. URL: <https://cyberleninka.ru> (дата обращения: 21.09.2024).
2. Крикунов, И. С. Цифровая экономика как фактор обеспечения экономической безопасности России / И. С. Крикунов // Прогрессивная экономика. 2023. №5. URL: <https://cyberleninka.ru> (дата обращения: 22.09.2024).
3. Осмоловец, С. С. Цифровые финансовые инструменты и финансовые риски их обращения / С. С. Осмоловец // Прогрессивная экономика. 2023. №5. URL: <https://www.nbrb.by> (дата обращения: 25.09.2024).

4. Milosh, D. V. Методические аспекты оценки развития цифровых финансовых активов на примере криптовалют / D. V. Milosh // SAI. 2024. №Special Issue 24. URL: <https://cyberleninka.ru> (дата обращения: 25.09.2024).
5. Жарницкая, К. Д. Влияние цифровой экономики на обеспечение экономической безопасности государства / К.Д. Жарницкая // Актуальные исследования. 2021. №11 (38). С. 53-56. URL: <https://apni.ru> (дата обращения: 30.09.2024).
6. Попов, Е. В. Проблемы экономической безопасности цифрового общества в условиях глобализации / Е.В. Попов, К. А. Семячков // Экономика региона. 2018. №4. URL: <https://cyberleninka.ru> (дата обращения: 29.09.2024).
7. Минаков, А. В. Обеспечение экономической безопасности России в условиях развития цифровой экономики / А. В. Минаков // Экономика и бизнес: теория и практика. 2019. №3-2. URL: <https://cyberleninka.ru> (дата обращения: 30.09.2024).