

УДК 330

Кеко Вансиси Серж Гилло, Мба Нтутуму Пелахиа Нчама
(Российская Федерация)

Научный руководитель Л.В. Минько, к.э.н., доцент
Тамбовский государственный технический университет

ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ В УСЛОВИЯХ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Развитие цифровой экономики несет в себе потенциал, а ее практическое применение необходимо для оценки социально-экономических трансформаций в системе экономической безопасности, особенно на национальном и на мировом уровнях.

В настоящее время актуальность темы исследования не вызывает сомнения, поскольку устойчивая и развитая система цифровой экономики является гарантией ее независимости, комфортной и стабильной жизнедеятельности общества. Большую роль развитие цифровой экономики имеет для укрепления экономической безопасности страны, и особенно важно в критические периоды ее существования, а именно сегодня, в условиях продолжающихся санкционных войн. Это необходимо для прогнозирования динамики развития экономики и разработки эффективных стратегий обеспечения безопасности. Решить данные задачи, выявить угрозы и вызовы безопасности возможно с помощью качественной диагностики с использованием инструментария информационных технологий.

Экономическая безопасность страны – это такое состояние экономики, при котором созданы приемлемые условия для жизни и развития личности и сохранения целостности государства, а также успешного противостояния влиянию внутренних и внешних угроз.

Обеспечению экономической безопасности и росту экономики способствует развитие ее цифровизации. Цифровая экономика генерирует высокие темпы прогресса, быстрые инновации и широкое применение.

Цифровая трансформация первой десятки экономик мира к настоящему времени составила уже 1,36 триллиона долларов, а в странах «Большой двадцатки» – 4,2 триллиона долларов и обеспечивает до 8 % внутреннего валового продукта (ВВП), способствуя росту и созданию рабочих мест. Вклад цифрового сектора в экономику Рос-

сии невелик в сравнении с экономиками развитых стран. Так, в 2022 году его доля составила всего 3,2 % ВВП. В аналогичный период в большинстве развитых стран размер цифрового сектора в среднем составил 6–9 % ВВП (например, Франция – 5,7 %, Германия – 6,3 %, США – 7,4 %, Швеция – 8,6 %).

Большая часть российского сектора цифровой экономики приходится на оптовую и розничную торговлю – 91,6 %, на обрабатывающие производства – 91,3 %, на систему связи, доступа к сети Интернет – 89,9 %, при этом со значительной долей государства. Вместе с тем серьезное отставание наблюдается в сфере операций с недвижимым имуществом, арендой и предоставлением услуг – 69,9 %, транспорта – 72,9 %, гостиничных услуг и ресторанного бизнеса – 75,3 %.

Таким образом, стратегическим направлением в развитии цифровых технологий должно стать стимулирование «слабых» отраслей, безусловно, не забывая продолжать развивать уже относительно «продвинутые» отрасли.

Однако исследования показывают, что Россия отстает по качественным показателям цифровизации в вопросах вовлеченности граждан и бизнеса. Присутствует достаточно низкий уровень применения цифровых технологий по ключевым аспектам социально-экономической жизни. В сравнении с развитыми странами, для России в 2022г. удельный вес организаций, которые используют системы планирования ресурсов (ERP), управления взаимоотношениями с клиентами (CRM) и радиочастотную идентификацию (RFID) в 2 раза меньше.

Кроме плюсов в использовании цифровой экономики, есть возможности, риски и угрозы ее применения и обеспечения экономической безопасности в России в условиях санкций:

1. Кратный рост угроз кибербезопасности. Многие сценарии, о которых говорилось как о теоретических, стали реальностью – бизнес вынужден защищаться.

2. Регуляторное давление. Государство усилило давление как на бизнес, так и на собственные структуры с целью повышения киберзащиты. Прежде всего, это Указ Президента РФ от 01.05.2022 № 250, Указ Президента Российской Федерации от 30.03.2022 № 166 и ряд других нормативных документов.

3. Нехватка специалистов, а также уход многих технологических компаний при возросшем уровне атак вынуждает российские организации искать сервисных подрядчиков, которые могли бы взять на себя работы по резкому усилению киберзащиты и постоянному поддержанию этого высокого уровня

4. Благоприятная налоговая политика для ИТ-компаний

5. Импортозамещение в результате чего, сегмент среднего и малого предпринимательства в 2022 году сильно сократил свои затраты на киберзащиту.

6. Значительная утечка/нехватка талантов/специалистов области.

7. Ограниченное использование глобальных облачных сервисов из-за санкционного риска, правил защиты персональных данных и политики импортозамещения.

8. Уход западных игроков – затраты на иностранные (покупка, эксплуатация) СЗИ составляли существенную часть затрат на кибербезопасность.

Российские решения есть не во всех сегментах, также они чаще всего дешевле западных аналогов. В результате компании не покупают ни обновления иностранных решений (они недоступны), ни российские решения, если они не работают, как требуют клиенты, что приводит к фактическому падению затрат в 2022 году и в целом к замедлению роста рынка.

Для мировой экономики развитие цифровизации также несет определенные угрозы. Это может быть выражено в монополизации, рисках потери конфиденциальности информации и ухудшения прав человека. Обострение борьбы в вопросах распространения стандартов и норм регулирования, в контроле над инновационными экосистемами и тотальный контроль талантов может привести к цифровой торговой войне.

Самые большие проблемы для России в этом процессе связаны с интеграцией четвертой промышленной революции в экономику, стимулированием малых и средних предприятий и превращением монопольных компаний в более конкурентоспособные структуры с присутствием на мировых рынках. Чтобы решить данные проблемы необходимо содействовать расширению экономических прав и возможностей страны, объединять регионы с использованием цифровой инфраструктуры и своевременно определять тенденции в глобальной цифровой среде.