УДК 338.242

***С. П. Гурская*** (kafedra-kitt2007@rambler.ru),
*канд. экон. наук, доцент*
*Белорусский торгово-экономический университет потребительской кооперации*
*г. Гомель, Республика Беларусь*

# ЦИФРОВАЯ ЭКОНОМИКА: ВОЗМОЖНОСТИ И УГРОЗЫ ДЛЯ БИЗНЕСА

В статье рассматриваются возможности и угрозы для ведения бизнеса в условиях цифровой экономики.

The article discusses the opportunities and threats for doing business in the digital economy.

*Ключевые слова*: цифровая экономика; интернет-технологии; электронная коммерция; риски; киберпреступность.

*Key words*: digital economy; internet-technologies; e-commerce; risks; cybercrimes.

Цифровая экономика является одним из ключевых направлений развития многих стран, включая Республику Беларусь, и оказывает значительное влияние на социально-экономическое развитие общества в целом.

Цифровые технологии активно проникают в бизнес-процессы организаций. По данным национальной статистики 96,7% организаций имеют широкополосный доступ в интернет [1, с. 18]. Это создает благоприятные условия для цифровизации бизнеса. Необходимо отметить, что валовая добавленная стоимость организаций сектора ИКТ составляет 6,2% от общей валовой добавленной стоимости экономики [1, с. 11].

Рассмотрим, какие возможности открывает цифровая экономика для бизнеса.

*Появление новых видов услуг, которые были недоступны до того, как возник интернет*. Начиная с 1990 г. по настоящее время формировались новые рынки товаров и услуг, основанные на использовании возможностей онлайн-технологий и сети интернет. Ярким примером новых видов услуг стала электронная коммерция, которая заняла заметную долю в розничной торговле различных стран. Так, в 2024 г. в розничном товарообороте Республики Беларусь она составила 11,7% [1, с. 15].

Современный период характеризуется появлением новой услуги облачного хранения данных, которая открывает новые возможности бизнесу для того, чтобы отказаться от собственных огромных дата-центров, от вложения существенных инвестиций в информационные системы и офисные площадки облачного хранения.

*Изменение характера конкурентной борьбы. Появление на рынке агрегаторов и других компаний нового типа*. Под воздействием цифровой экономики и новых технологий электронной коммерции меняются бизнес-модели. Например, это привело к тому, что офлайновые традиционные компании были вынуждены трансформировать свой бизнес, встраивать электронные каналы продаж в существующие бизнес-модели либо полностью уходить в онлайн. Это мотивировало предпринимателей создавать бизнес в сети интернет.

При построении электронного бизнеса необходимо было создать прогрессивную цепочку добавленной стоимости, обеспечить взаимодействие деловых партнеров, потребителей и всех заинтересованных сторон, используя возможности информационных технологий. В Беларуси развит сектор онлайн-торговли: популярны маркетплейсы Wildberries, Ozon, EMall, Shop.by, Kufar.by, а также локальные лидеры: 21vek.by, «Евроопт» (доставка продуктов), ОМА (стройматериалы), Xistore.by (техника) и «Онлайнер» (каталог). Всего зарегистрировано более 30 тыс. интернет-магазинов.

*Цифровая экономика открыла для бизнеса возможности осуществлять поиск новых идей на основе оперативной бизнес-аналитики и осуществлять быструю обратную связь с клиентами*, что позволило компаниям быстро реагировать на инновационные ожидания потенциальных клиентов. Этому способствовало появление бесплатных сервисов Google Analytics, «Яндекс. Метрика» и др.

*Растущая роль социальных сетей в формировании у потребителей знаний о продуктах (услугах)*. Развитие интернет-рекламы позволило электронному бизнесу зарабатывать на рекламе, т. е. модель «расходы на рекламу» изменилась на модель «доходы от рекламы». Сегодня компании, выстраивающие бизнес в сети интернет, зарабатывают на рекламе больше, чем затрачивают на нее. Раньше традиционно на рекламе зарабатывали только рекламные агентства.

*Бизнесмены получили возможность продавать не только материальные, но и электронные, цифровые товары*. На фоне растущего рынка интернет-торговли наблюдается устойчивый рост доходов от продажи цифровых товаров и билетов, прежде всего продажи авиа- и железнодорожных билетов.

*Возможности совместного потребления материальных благ, что изменило отношения многих членов общества к вопросу владения материальными благами*. Например, молодежь все больше увлечена сбором впечатлений и связывает ощущение свободного перемещения (на учебу, работу) в разные регионы мира без необходимости приобретения собственного имущества и владения им.

Однако вместе с возможностями, которые предоставляет цифровая экономика, она также представляет новые угрозы и вызовы для экономической безопасности экономики любого государства.

Прежде всего, применение технологий цифровой экономики порождает новые информационные риски. Одной из основных угроз является увеличение числа кибератак на организации и государственные учреждения. В 2024 г. Беларусь оказалась на втором месте после России в мире по доле пользователей, атакованных киберугрозами из интернета, – это 43,5% интернет-пользователей нашей страны [2].

К основным группам рисков в бизнесе можно отнести: кибернетические, организационные и кадровые, правовые и антимонопольные, репутационные и рыночные риски.

*Кибернетические риски*. Кража персональных данных клиентов, утечки конфиденциальной информации и взлом платежных систем, что нарушает работу бизнеса. В условиях растущей клиентской базы компаниям становится все сложнее защищать данные пользователей. Утечки приводят к потере лояльности, падению продаж, финансовым потерям и репутационному ущербу. Всплеск киберпреступности фиксируется в Беларуси на протяжении последних лет. Если в 2016 г. таких преступлений было около 2,5 тыс., то с 2020 г. их регистрируется не менее 20 тыс. ежегодно. В 2025 г., например, было совершено 20 667 киберпреступлений (32% от общего числа преступлений), причем 96% из них – цифровые преступления против собственности [3].

Лидирует телефонное мошенничество (вишинг) – 38% всех случаев, 22% связано с онлайн-торговлей (в основном через инстаграм), 13% – фишинг (получение доступа к логинам и паролям), 6% – мошеннические действия с банковскими картами, 5% – мошенничество при оказании услуг, 3% – при аренде недвижимости, 7% – иное [3].

Еще 5% – это вымогательство. Почти 70% случаев в Беларуси связано с похищением пароля и блокировкой устройств Apple, 30% – с похищением и угрозой распространения персональных данных, 2% – с блокировкой важной информации субъектов хозяйствования.

Существенными последствиями киберпреступности для компаний является потеря документов и файлов (25%), утечка персональных данных (20%), нанесение ущерба или появление рисков для репутации компании (15%). Основная уязвимость в сфере кибербезопасности попрежнему связана с человеческим фактором – сотрудники нередко игнорируют правила информационной безопасности. Однако определенную роль играют и технические уязвимости.

*Технологические риски*. Зависимость от работоспособности IT-инфраструктуры, сбои в работе онлайн-платформ, высокая стоимость внедрения и поддержки новых решений.

*Организационные и кадровые риски*. Нехватка квалифицированных специалистов, низкая цифровая грамотность персонала, необходимость изменения бизнес-процессов.

Организационный риск – это потенциальная угроза убытков, вреда или негативного воздействия, с которыми сталкивается организация в процессе достижения своих целей и функционирования в окружающей среде. Он включает в себя различные факторы, такие как финансовые риски, операционные риски, стратегические риски, риски соблюдения нормативных требований, репутационные риски и мн. др.

Кадровые риски – это вероятность убытков или сбоев в работе организации из-за действий, бездействия или увольнения персонала. Ключевые примеры включают массовые увольнения ключевых специалистов (риск потери компетенций), ошибки персонала, приведшие к порче товара или штрафам, мошенничество, нарушение техники безопасности, а также неэффективное обучение. Необходимо обучать сотрудников защите конфиденциальных данных, распознаванию подозрительной активности и строгому соблюдению протоколов кибербезопасности для эффективного противодействия потенциальным атакам.

*Правовые и антимонопольные риски*. Сложности в регулировании цифровой среды, риски нарушения законодательства, споры, связанные с использованием интеллектуальной собст-

венности и данных. Хотя большинство случаев сотрудничества между конкурентами носят проконкурентный характер, потенциальные антимонопольные риски могут возникнуть, если взаимодействие конкурентов приводит к скоординированному поведению, такому как ценовой сговор, ограничение объемов производства или распределение рынка.

*Репутационные и рыночные риски.* Негативные отзывы в сети, высокая конкуренция, изменение потребительского спроса, риски потери контроля над репутацией.

В экономической литературе риски, связанные с электронной коммерцией, ассоциируются в основном с покупателями. Однако нельзя не отметить, что электронная коммерция также несет определенные риски и для продавцов (ретейлеров). В связи с этим охарактеризуем риски для продавцов.

Первый риск связан с нарастанием отставания знаний потребителей от ускоряющегося прогресса в информационных технологиях. Сегодня можно говорить об усиливающейся информационной асимметрии, которая проявляется в информационной безопасности, знании о брендах и репутации продавцов, конфиденциальности персональных данных. Покупатели онлайн все больше сталкиваются с большим объемом данных, который нарастает лавинообразно и затрудняет потребительский выбор. В итоге доверие покупателей к продавцам онлайн достигает своего предела, и развитие электронной коммерции останавливается на определенных сегментах рынка, как правило, недорогих и массовых товарах.

Второй риск – нарушение антимонопольного законодательства в сфере торговли вследствие усиления конкурентной борьбы на рынках электронной коммерции. Этот процесс прямо связан с увеличением числа сделок слияний и поглощений в мире в последнее десятилетие.

Третий риск – информационно-технологический, связанный с действиями третьих лиц-хакеров. Это свидетельствует о многократном возрастании информационно-технологического риска в будущем по мере роста продаж онлайн.

Человеческий фактор остается самым уязвимым звеном в системе безопасности. В сферах розничной торговли и электронной коммерции риски инсайдерских угроз особенно высоки из-за недостаточной подготовки сотрудников и подрядчиков в области кибербезопасности, что часто приводит к ошибкам и уязвимостям.

Четвертый риск – субъектный, связанный с недобросовестными действиями продавцов в области недобросовестного маркетинга (введение покупателей в заблуждение и предоставление ложной информации о ценах, качестве, условиях поставок и пр.). В 2025 г. в республике проверке подверглись 295 интернет-магазинов. Нарушения законодательства были установлены в отношении 257 из них, что составляет 87,1%. За 2025 г. в Министерство антимонопольного регулирования торговли Республики Беларусь поступило около 400 жалоб, связанных с нарушением законодательства при совершении покупок на различных маркетплейсах. Основной перечень проблем, с которыми сталкиваются потребители, включает: приобретение товаров ненадлежащего качества, неудовлетворительное обслуживание, предоставление недостоверной информации о характеристиках товаров, а также необоснованные задержки с возвратом денежных средств [4].

Пятый риск – правовой, связанный с осуществлением интернет-магазинами незаконной деятельности, такой как: отсутствие или неактуальность регистрации в Торговом реестре; продажа товаров, запрещенных к реализации или ввозу на территорию Беларуси согласно действующим нормативным актам; случаи дистанционной торговли товарами, для которых такой способ продажи не допускается; незаконные предложения по продаже иностранной валюты; размещение объявлений о товарах, содержащих признаки экстремистской символики и атрибутики, что свидетельствует об опасности для репутации всей отрасли в целом [4].

Анализ составляющих элементов системы электронной коммерции и рисков, сдерживающих ее развитие, позволил сделать следующие выводы. Прежде всего, электронная коммерция включает в себя различные связи между субъектами бизнеса, потребительского рынка и государства, в которых формируются как новые возможности для развития, так и риски.

В условиях ускорения развития интернет-технологий и влияния внешних факторов спрос на покупки в онлайн-магазинах растет экспоненциально, что создает определенную «критическую массу» будущих инвестиций в данной сфере и усиление ее конкурентоспособности. С другой стороны, возрастают и риски, ставя под угрозу темпы развития электронной коммерции, инвестиций и создаваемых рабочих мест.

Далее технологические составляющие электронной коммерции во многом определяют ее риски для покупателей, связанные с передачей данных в интернет и через платежные шлюзы, с размещением информации в социальных сетях и ее анализом в больших данных. Значитель-

ная информационная асимметрия между разработчиками цифровых технологий и покупателями в онлайн-магазинах выводит риск нарушения кибербезопасности на первое место среди угроз электронной коммерции.

Наряду с рисками технологического характера для онлайн-торговли характерны и другие риски – антимонопольный, правовой, субъектный, информационный. Данные риски требуют долгосрочного сотрудничества бизнеса и государства, нацеленного на создание благоприятной институциональной среды.

Долгосрочные мероприятия по снижению рисков должны исходить от государства и должны включать:

– противодействие незаконной конкуренции и ущемлению прав потребителей на законодательном уровне;

– совершенствование инфраструктуры электронных транзакций, хранения и анализа баз персональных данных покупателей;

– продвижение новых знаний о сделках в интернете в широкие массы населения.

Также важным является государственное регулирование защиты конфиденциальности коммерческой информации в интернете, в особенности в условиях диффузии технологий биоидентификации (по скану лица или сетчатки глаза), виртуальной и дополненной реальности.

Существующие риски цифровой экономики привлекают внимание к ее социально-этическим аспектам. Цифровизация экономики способна помочь решить насущные социальные и глобальные проблемы, упрощая коммуникации между государством, бизнесом и гражданским обществом, повышая качество социальных услуг, повышая производительность, создавая новые возможности для предпринимательства и трудовой деятельности, повышения и расширения профессиональных квалификаций, позволяя учитывать особые потребности социально незащищенных групп, создавая новые возможности для социально значимых научных исследований в области смягчения рисков изменения климата, нехватки питьевой воды, энергии и продовольствия.

Таким образом, Республика Беларусь обладает значительным потенциалом для успешной реализации стратегий цифровизации национальной экономики, однако для этого необходимо обеспечение кибербезопасности и защиты персональных данных, повышение уровня финансирования цифровых проектов и развитие инновационной инфраструктуры.

**Список использованной литературы**

1. **Информационное** общество в Республике Беларусь : стат. сб. – Мн. : Нац. стат. ком. Респ. Беларусь, 2025. – 58 с.

2. **Беларусь** за год поднялась с 7-го на 2-е место по доле пользователей, подвергшихся кибератакам. – URL: https://belretail.by/news/belarus-za-god-podnyalas-na-2-mesto-po-kiberatakam?utm_source=sendpulse&utm_medium=email&utm_campaign=WeekReview-16-dec-2024 (дата обращения: 21.02.2026).

3. **Криминальная** цифровизация. – URL: https://neg.by/novosti/otkrytj/kriminalnaya-tsifrovizatsiya/ (дата обращения: 21.02.2026).

4. **МАРТ** проверил три сотни интернет-магазинов – нарушения нашли почти в 90% случаев. – URL: https://myfin.by/article/rynki/mart-proveril-tri-sotni-internet-magazinov-narusenia-nasli-pocti-v-90-slucaev-43209#:~:text (дата обращения: 21.02.2026).