УДК 338.24

ВЕРОЯТНЫЕ РИСКИ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Е. К. НИКОЛАЕВА
Научный руководитель Н. А. ЮДИНА, канд. хим. наук, доц.
ФГБОУ ВО «Казанский государственный энергетический университет»
Казань, Россия

Аннотация

В статье исследованы проблемы основных видов рисков, с которыми возможно столкнется российская экономика в условиях перехода к цифровому формату, вероятные направления деятельности, которые помогут сгладить негативные отклики рисков цифровой экономики. Государству рекомендуется качественно прогнозировать и вовремя реагировать на быстро формирующиеся тенденции социально-этической направленности, связанной с формированием национального глобального цифрового пространства.

Ключевые слова:

цифровая экономика, риск, оцифровывание, интерфейс, программисты, государство.

Цифровая экономика понимается не только как «оцифровывание» действующих государственных и бизнес процессов, но и как воплощение чего-то абсолютно нового и невозможного в «аналоговом» мире. Цифровая сущность несет в себе не только новые возможности и перспективы развития, но и видимые риски.

Все уже привыкли к элементам цифровой экономики. К примеру, множество интерфейсов с государством, банками и телекоммуникационными компаниями в настоящем – цифровые, можно обойтись без участия людей. Мы пользуемся переводом денежных средств, совершаем покупки, оплачиваем налоги и коммунальные платежи и др. В бизнесе тоже наблюдается активное использование элементов цифровой экономики, например, с помощью информационных систем можно привлекать и обслуживать клиентов, проводить закупки нужного сырья для производства и т. д. Все это воспринимается как данность, которая несет с собой помимо развития и проблемы тоже, которые логичнее назвать рисками. Обозначим основные риски.

Базовый риск связан с отсутствием кадров. Перейти в хозяйствовании к цифровым методам оказалось весьма выигрышно, обслуживать своих клиентов компаниям стало менее затратно, чем в офисах. Существенная экономия составляет на аренде помещения и содержании операторов. Но возникла проблема в кадрах, такого количества грамотных программистов, которые в силах разработать нужную обслуживающую систему, не оказалось на рынке труда. Наши таланты переманивают зарубежные компании. Из российских компаний не отстают в вербовке специалистов «Mail.ru» и «Яндекс». Конечно же, возник дисбаланс спроса и предложения на рынке.

В итоге удовлетворение спроса привело к подготовке неквалифицированных веб-программистов, т. к. невозможно за короткий срок, около месяца, все освоить. Команды из таких веб-разработчиков чаще всего побеждают в конкурсах или тендерах «кто меньше запросит за конкретный функционал». Такие специалисты стоят недорого. На таких быстрых курсах речь не идет о безопасной разработке и безопасной архитектуре. Что получаем на выходе? Более утлыми становятся веб-приложения, потому что весь фокус разработчиков направлен на функционал, хотя главной остается безопасность. То же можно сопоставить с сотрудниками информационной безопасности, которым поручили настроить средства защиты, или к инженерам, настраивающим инфраструктуру для приложений. Быстрый рост приложений цифровой экономики требует и рост тестеров, инженеров, разработчиков и разработчиков-«безопасников». Для подготовки отличных специалистов потребуются годы. Нужно составить достойную конкуренцию американцам и китайцам по заработной плате и интересным задачам. Если выпускать слабых специалистов, можно получить уязвимость и массу происшествий. Бизнес не стоит на месте и требует постоянных изменений, сегодня он реализуется в приложениях. Соответственно приложения тоже должны меняться, быть более гибкими. Нужно менять подход к цифровому бизнесу, начиная со специалистов и заканчивая каждым участником процесса. Некоторое время назад был объявлен «переход на agile», но т. к. людям тяжело переходить от старых привычек к новым, ожидаемых результатов пока нет. Agile – это различные новейшие подходы и методики к управлению, которые: фокусируют команду на целях и нуждах клиентов; значительно упрощают организационную структуру и процессы; активно используют обратную связь; работают короткими циклами; повышают полномочия сотрудников; основаны на гуманистическом подходе; являются образом мышления и образом жизни. Поэтому, не имея армии грамотных «оцифровщиков» в области бизнеса и области информационных технологий, не совсем понятно как же «оцифровать» экономику [1, 2].

Следующей проблемой «оцифровки» экономики, которая не так очевидна, является смена мест бизнеса и бизнеса информационных технологий. В традиционном бизнесе информационные технологии представляют собой его отражение, скажем с целью аналитики или учета. Сначала в бумажно-наличном мире происходят транзакции и договора, а затем все это заносится в информационные технологии системы с целью дальнейшего анализа и учета. Предположим, что с информационной технологией системы что-то пошло не так и данные исчезли. В таком случае бизнес не пострадает, придется лишь потратить много времени для восстановления данных. В цифровой экономике нет такого понятия как «первичка». Информационные технологии не отражают бизнес, они сами являются им. Все совершаемые сделки проходят в бизнес-приложениях и цифровом пространстве. Если раньше информационная технология выходила из

строя, то платежные поручения выписывались вручную, продолжалась работа. Сейчас же, если информационная технология выйдет из строя, это приведет к коллапсу – даже аналоговые процессы перестанут работать, потому что управление ими – цифровое. Таким образом, информационная технология – это ядро бизнеса и никак ни его служебная функция. Если затормозить процесс внедрения таких знаний, то цифровизация не скоро произойдет. Пока что в этом вопросе хорошо разбираются инноваторы и интернет-гиганты, или же банки без офисов.

Далее рассмотрим риск «интернета вещей». Интернет вещей крепко закрепился в нашей повседневной жизни. Мы имеем возможность управлять своим автомобилем, бытовыми приборами, стационарным видеонаблюдением и мобильным (дроны), можем открывать двери через применение мобильного приложения. Такие приложения вносят комфорт и оптимизируют ресурсы. За все это стоит сказать спасибо небольшим модулям-контролерам в наших устройствах. Модули-контролеры собирают и обрабатывают информацию, обмениваются командами с другими приборами и реагируют на команды. Чаще всего эта функция товара служебная и не ключевая, соответственно и дешевая. Отсюда следует, что производитель сэкономил на безопасности. Когда владелец устройства, по своей цифровой безграмотности, оставляет пароли в свободном доступе – это лазейка для злоумышленников. Минимальный ресурс модулей-контролеров не дают возможности вклинить в них «навесную» безопасность, тогда как производители еще не озадачились о «встроенной» безопасности. Были случаи мощнейших DDoS-атак, когда видеокамеры объединялись в бот-сеть. Перехват управления и блокировка систем участились в последнее время [1, 2].

Не менее важный риск искусственного интеллекта. Сегодня большим спросом пользуются такие технологии, как распознавание голосовых команд, сканирование по сетчатке глаза, распознавание лица с городских и домашних камер видеонаблюдения, анализ пользовательских предпочтений и многое другое. Если искусственный интеллект находится в руках злоумышленника, он легко подберет пароль и докажет, что не является роботом. С внедрением и использованием искусственного интеллекта в цифровой экономике, повышаются пути вредоносного использования его уязвимости с целью совершения преступлений. Вполне вероятно противостояние двух искусственных интеллектов в гражданской области или области вооружений. Есть вероятность и обратного развития.

Риск использования блокчейна. По сути, блокчейн является технологией хранения данных и информации об обработке самих данных. Но есть отличие от других систем, она имеет уникальный принцип работы. Призвание технологии в совершении революции в экономике. Если перевести процессы на блокчейн, то польза будет очевидна, как и угрозы. Блокчейн платформа, как быстроразвивающееся программное обеспечение, обладает

не идеальностью и уязвимостью, которые, в свою очередь, группируются с уязвимостью в других смарт контактах, разработанных специалистами на других блокчейн платформах. Уязвимость в блокчейн платформе может привести к ветвлениям («форкам») в экосистеме криптовалют. Основной принцип ветвления – неизменность проведенных транзакций. Например, если транзакция была подтверждена, но при этом была вызвана сбоем, оказалась ошибочной, неправильной или мошеннической – исправлению не подлежит ни в каком случае [1, 2].

Цифровая экономика – полезная цель и вполне перспективная. Достижения в процессе развития, несомненно, принесут пользу – оптимизируются неэффективные бизнес процессы, высвободятся огромные ресурсы, оптимизируются процессы государственного управления, повысится управляемость и прозрачность государства и бизнеса. Описанные выше серьезные риски могут подавить достижения в цифровой экономике. При проектировании цифровой системы, следует заранее продумать все возможные риски, с целью уменьшения их влияния и торможения развития цифровой экономики. При построении архитектуры системы и ее проектировании, должна в первую очередь быть учтена ее безопасность. Нужно искоренить принцип, который еще уместен – «вот вам система, которую мы сделали, а ваше дело теперь придумать защиту». Необходимо создавать информационную безопасность не навесной системой. Нужно сделать ее встроенной функцией для каждой информационной технологии системы. Только в таком случае есть вероятность избежать риски.

СПИСОК ЛИТЕРАТУРЫ

1. **Ахромеева, Т. С.** Стратегии и риски цифровой реальности [Электронный ресурс] / Т. С. Ахромеева, Г. Г. Малинецкий, С. А. Посашков. – Режим доступа: http://sec.chgik.ru/ctrategii-i riski-tsi -frovoy –realnosti.

2. **Андрияшин, Ю. Н.** О целях, возможных рисках и последствиях «цифровой экономики» [Электронный ресурс]. – Режим доступа: http://reosh.ru/yu-n-andriyashin-o-celyax-vozmozhnyx-riskax-i-posledstviyax-cifrovoj-ekonomiki.html.