УДК 004.9+338.2

РИСКИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ БИЗНЕСА

Меняйло Галина Владимировна, канд. экон. наук, доц.

Воронежский государственный университет, Университетская пл., 1, Воронеж, Россия, 394018; e-mail: mgalina27@mail.ru

Цель: цифровая экономика открывает для бизнеса новые направления развития информационных технологий. Появляются возможности обмена большими объемами данных, использования искусственного интеллекта, квантовых технологий, робототехники и т.д. Это позволяет обрабатывать большие массивы информации и принимать обоснованные управленческие решения. Но при этом возникают риски, связанные с потерей информации, с безопасностью данных, что в свою очередь приводит к необходимости классификации и идентификации рисков, возникающих в условиях цифровой трансформации. *Обсуждение*: рассмотрены сквозные цифровые технологии, которые лежат в основе цифровой трансформации, что позволило определить связанные с их использованием риски. *Результаты*: идентифицированы и описаны риски сквозных цифровых технологий в бизнесе, а именно риски больших данных, риски промышленного интернета, риски искусственного интеллекта, риски беспроводных технологий, риски робототехники, риски квантовых технологий, риски системы распределенного реестра.

Ключевые слова: риски, цифровая трансформация, сквозные цифровые технологии, безопасность.

DOI: 10.17308/meps.2020.3/2329

Введение

Все возможности, в том числе использование технологических инноваций, в частности цифровых технологий, несут определенный уровень риска. Предприятия не могут проводить цифровую трансформацию, не выявив потенциальные риски. Риск киберпреступлений и ответственности – это основные риски, которые связывают с применением цифровых технологий. На самом деле список потенциальных рисков в процессе цифровой трансформации в бизнесе достаточно обширный. Чтобы в полной мере осознать огромный потенциал цифровой трансформации, бизнес должен быть готов к рискам, с которыми он может столкнуться.

Основой цифровой трансформации является обеспечение технологической независимости государства, возможности коммерциализации отечественных исследований и разработок, а также ускорение технологического

развития российских компаний и обеспечение конкурентоспособности разрабатываемых ими продуктов и решений на глобальном рынке [9].

Цифровая трансформация приоритетных отраслей экономики возможна на основе внедрения отечественных продуктов, сервисов и платформенных решений, созданных на базе сквозных цифровых технологий: большие данные; новые производственные технологии; промышленный интернет; искусственный интеллект; технологии беспроводной связи; компоненты робототехники и сенсорика; квантовые технологии; системы распределенного реестра; технологии виртуальной и дополненной реальностей.

В общем виде в экономической литературе проблемы, связанные с развитием и широким внедрением «цифровых» технологий, сводятся к следующим основным рискам: угроза «цифровому суверенитету» страны и пересмотр роли государства в трансграничном мире «Цифровой» экономики; нарушение частной жизни (потенциальное наблюдение за гражданами); снижение уровня безопасности данных; уменьшение числа рабочих мест низкой и средней квалификации; повышение уровня сложности бизнес-моделей и схем взаимодействия; резкое усиление конкуренции во всех сферах экономики; изменение в моделях поведения производителей и потребителей; необходимость пересмотра Административного и Налогового кодексов [7].

Риски применения сквозных цифровых технологий в бизнесе

Рассмотрим цифровую трансформацию бизнеса и идентифицируем риски, которые могут возникнуть в процессе применения сквозных цифровых технологий.

1) Риски больших данных (Big Data). Любой бизнес несет в себе различные риски из-за возможности принять неверное решение в условиях информационных ограничений. С целью повышения эффективности принимаемых решений предприятия обращаются к большим данным. Термин Big Data используется для описания большого и растущего экспоненциально со временем набора данных. Преимущества, которые предоставляет Big Data: сбор данных из разных источников, улучшение бизнес-процессов через аналитику в реальном времени, хранение огромного объема данных. Но использованию больших данных сопутствуют определенные риски (табл. 1).

Таблица 1

Риски больших данных

Риск	Описание
Риск конфиденциальности	– потеря контроля над данными и их передача конкурентам; – разглашение конфиденциальных данных в СМИ или в Сети.
Риск потери данных	– частичная или полная утрата данных из-за злоумышленников, из-за ошибочных действий специалистов и пользователей или чрезвычайных ситуаций.
Риск переполнения хранилища	– неоптимальная система сбора и хранения больших данных приведет к переполнению хранилища и утрате вновь получаемых данных при отсутствии места для физического их размещения.

Окончание табл. 1

Риск	Описание
Риск снижения эффективности больших данных	– четкость структуры собираемых и обрабатываемых данных, их управляемость и качество направлены на то, чтобы исключить снижение результативности работы с большими данными по мере разрастания их объемов.
Риск формирования неэффективного набора данных	– несоответствие больших данных и бизнес-модели. На базе таких данных аналитики и менеджеры сложно принять обоснованное решение.
Риск ошибок больших данных	– ошибки в содержании и структуре больших данных и ошибки в инструментах работы с ними.
Риск экономической нецелесообразности больших данных	– аналитики могут не найти ответы на проблемные вопросы бизнеса, обработав доступный им объем больших данных.
Риск неготовности к переменам	– большие данные и аналитика противоречат внутренней культуре компании и сложившемуся стилю руководства.
Риск мошенничества	– при покупке больших данных или при подключении платных сервисов сбора и обработки больших данных.

2) Риски промышленного интернета (Industrial Internet of Things, IIoT). Индустриальный интернет – инфокоммуникационная инфраструктура, объединяющая промышленные объекты и обеспечивающая обмен данными и взаимодействие между ними, образует основу «умных производств» [12], приводит к формированию новых бизнес-моделей при создании и товаров и услуг и, в частности, изменяет модель взаимодействия «поставщик – потребитель».

Технологическая архитектура промышленного интернета вещей включает следующие уровни: устройства IIoT; средства передачи данных; платформа; приложения [3]. Промышленный интернет вещей управляется при помощи специализированного программного обеспечения, что приводит к росту угроз и возможных атак на промышленные объекты. При этом возможности промышленного интернета вещей превосходят риски [5].

В ноябре 2018 года ENISA выпустило документ «Good Practices for Security of Internet of Things in the context of Smart Manufacturing», в котором собраны практики обеспечения кибербезопасности для промышленного интернета вещей [10]. В документе представлена классификация и описание возможных угроз применительно к области IIoT. Исходя из угроз, можно выделить следующие риски промышленного интернета, представленные в табл. 2.

Таблица 2

Риски промышленного интернета

Риск	Описание
Риск противоправных действий и различного рода манипуляций, производимых с устройствами IIoT, средствами передачи данных, платформой и приложениями	– внедрение вредоносного программного обеспечения, предназначенного для выполнения нежелательных и несанкционированных действий в системе без согласия пользователя. Реализуется на уровне приложений и платформы; – DDoS-атаки – распределенная атака с нескольких компьютеров на вычислительную систему с целью довести её до отказа. Реализуется на уровне платформы; – эксплойты. Эксплойт представляет собой программный код, предназначенный для использования уязвимости для доступа к системе. Реализуется на уровне приложений.
Риск взлома системы	Реализуется на уровне сети: – активная атака подслушивания (злоумышленник тайно ретранслирует и изменяет связь между двумя сторонами); – захват сессии – активная атака, когда злоумышленник перехватывается TCP-сеанс); – сетевая разведка (позволяет получать внутреннюю информацию о сети: подключенные устройства, используемый протокол, открытые порты, используемые службы и т.д.)
Риск ошибок в конфигурировании, администрировании и применении	– сбой системы – отказ программных услуг или приложений. Реализуется на уровне приложений.
Риски потери и электропитания, коммуникаций или сервисов	– сбой в сети – преднамеренный или случайный сбой в работе сети. Реализуется на уровне средств передачи данных; – сбой устройств – отказ или неисправности аппаратных устройств. Реализуется на уровне устройств и на уровне платформы;
Форс-мажорный риск	Природные явления (наводнения, сильные ветры, снегопады и пр.), которые могут физически повредить устройства. Реализуется на уровне устройств и на уровне платформы.
Риск вывода из строя устройства	Реализуется на уровне устройств: – модификация или разрушение устройства; – воровство.
Риск уязвимости программного обеспечения	Реализуется на уровне приложений: – слабые пароли; – ошибки программного обеспечения; – отказ сервисов провайдера.
Правовой риск	Отклонения от требований законов и контрактов.

3) Риски искусственного интеллекта. Искусственный интеллект – это технология создания аппаратно-программных средств, которые могут решать творческие задачи и генерировать новую информацию на основе имеющейся. Искусственный интеллект моделирует интеллектуальную деятельность человека [8] и включает машинное обучение, нейронные сети, распознавание объектов и образов, компьютерное зрение, распознавание лиц и другие технологии. Выделяются следующие направления развития искусственного интеллекта: использование существующих данных для принятия решений на базе чистой аналитики; сочетание машинного зрения и

анализа изображений, голосовой аналитики с машинным обучением; перенос технологий искусственного интеллекта в физический мир, появление роботов [1].

Искусственный интеллект в первую очередь позволяет сократить рутинные операции и, как следствие, увольнение сотрудников, занятых не творческим, формализуемым трудом [6]. При этом внедрение технологий искусственного интеллекта – процесс достаточно дорогой и рискованный (табл. 3).

Таблица 3

Риски искусственного интеллекта

Риск	Описание
Риск потери контакта с клиентом	Автоматизация полезна для бизнеса только в случае, если помогает сблизить предприятие с клиентом. Выявлено, что большинство людей предпочитают человеческий контакт.
Риск нехватки квалифицированных специалистов	Возникает проблема вытеснения рабочей силы искусственным интеллектом и появление новых профессий, например, цифровых специалистов в компании (специалист по обработке и анализу данных, инженер по работе с данными, архитектор данных и др.)
Риск информационно-технологической инфраструктуры	Недостаток машинных мощностей для решения задач, требующих просчета больших массивов данных, например, при создании виртуальных помощников или физических роботов.
Риск ошибок в управлении производством	Искусственный интеллект, воспроизводящий действия людей-экспертов, может унаследовать их ошибки и предубеждения, это приведет к недоработкам в системах управления производством.

4) Риски беспроводных технологий. С точки зрения технологий цифровая экономика предполагает подключение к инфраструктуре гигантского количества разнообразных устройств интернета вещей. В большинстве случаев подключение беспроводное и требует использования радиочастотного спектра и соответствующих стандартов [2].

Беспроводная связь гораздо менее безопасна по сравнению с проводной, в которой для связи используется кабель. Эфир – среда с общим доступом и практически полным отсутствием контроля. Обеспечить эквивалент физической безопасности проводных сетей невозможно. К беспроводным сетям подключиться можно откуда угодно при помощи специального оборудования, имеющего сигнал достаточной силы. Таким образом, беспроводные технологии, работающие без физических и логических ограничений своих проводных аналогов, значительно повышающие гибкость рабочего процесса и эффективность труда пользователей, снижающие затраты на развертывание сетей, также подвергают сетевую инфраструктуру и пользователей значительным рискам (табл. 4).

Таблица 4

Риски технологии беспроводной связи

Риск	Описание
Риск неавторизованного доступа к корпоративной сети	Самовольно установленные точки доступа, взламывающие сеть организаций. Использование злоумышленниками чужаков (Rogue Devices, Rogues).
Риск нефиксированной природы связи	Некорректно сконфигурированный беспроводной клиент автоматически ассоциируется и подключает пользователя к ближайшей беспроводной сети. Это позволяет злоумышленникам «переключать на себя» пользователя для последующего сканирования уязвимостей или атак.
Риск уязвимости сетей и устройств	Злоумышленники атакуют более уязвимые сетевые устройства (неправильно сконфигурированы, использовать слабые ключи шифрования или методы аутентификации с известными уязвимостями).
Риск новых угроз и атак	Появление новых способов реализации старых угроз: – имперсонация авторизованного пользователя; – атака «Отказ в обслуживании» авторизованных пользователей; – специализированные инструменты атакующего.
Риск утечки информации из проводной сети	Большинство беспроводных сетей соединяются с проводными. Беспроводная точка доступа может использоваться для атаки. Ошибки в конфигурации точек доступа и конфигурации проводной сети могут открывать пути для утечек информации.
Риск проблем функционирования беспроводных сетей	Низкая скорость, ухудшение качества связи, снижение производительности, повышение стоимости эксплуатации.

5) Риски роботизированных технологий. Роботизированные технологии решают различные производственные задачи. При этом при реализации робототехнических решений высока вероятность возникновения определенных рисков (табл. 5).

Таблица 5

Риски роботизированных технологий

Риск	Описание
Риск несоблюдения техники безопасности	Возможность совершения человеком ошибки при внедрении робототехники на рабочем месте
Риск кибербезопасности	Уязвимость робототехники (взломы, атаки): – нарушение производственной логики; – нарушение правил калибровки; – изменение параметров контроллера и др.

Международные стандарты безопасности содержат рекомендации по снижению рисков, связанных с обустройством совместного рабочего про-

странства и применением промышленных роботов в изолированных от людей зонах.

6) Риск квантовых технологий. В основе квантовых технологий лежат процессы квантовой физики. Квантовые технологии делятся на три основных субтехнологии: квантовые вычисления, квантовые коммуникации, квантовые сенсоры и метрология. Данные технологии востребованы для дальнейшего прогресса во всех стратегических направлениях цифровой экономики, при этом выделяются основной, связанный с ними риск – квантовая угроза кибербезопасности. Разработаны алгоритмы, которые позволят квантовому компьютеру сократить время подбора пароля и дешифровки информации до нескольких часов или минут. Данные, украденные сегодня, безопасны, если зашифрованы, но квантовые атаки сделают эти данные уязвимыми в будущем.

7) Риски системы распределенного реестра. Распределенный реестр – формируемая на определенный момент времени систематизированная база данных в виде транзакций, которая хранится, создается и обновляется в узлах участников реестра на основе заданных алгоритмов [4]. Ключевыми особенностями является: отсутствие центрального администратора; совместное использование с синхронизацией по заданному алгоритму; децентрализованное географическое распределение копий базы данных между всеми узлами связи. Распределительный реестр стал известен в основном благодаря его применению в блокчейне криптовалют, но вноситься в него могут любые данные: финансовые, юридические, статистические, электронные и другие. Риски системы распределенного реестра представлены в табл. 6.

Таблица 6

Риски системы распределенного реестра

Риск	Описание
Риски, связанные со смарт-контрактами	– блокировка средств из-за непредвиденного в коде смарт-контракта состояния; – потеря средств из-за уязвимости кода или зацикливание кода; – бесполезная трата денег пользователей публичной DLT-системы, если код смарт-контракта не очень хорошо разработан.
Риски, связанные с инфраструктурой	– в длительной перспективе мотивация для обеспечения сохранности данных может уменьшиться, особенно когда объем данных возрастает; – захват контроля благодаря доминирующим вычислительным мощностям, уязвимости программного обеспечения; – атаки, направленные на то, чтобы помешать узлам посылать или получать транзакции.

Окончание табл. 6

Риск	Описание
Риски, связанные с криптографией	– раскрытие или потеря ключей; – коллизия – возможность создания различных электронных объектов с одним и тем же значением хэш-функции; – обратимость хеширования – отыскание алгоритмического способа отыскания исходной цепочки битов, для которой хеш-функция выдает определенное значение хеша; – проблемы алгоритма генерации ключей – отыскание алгоритмического способа вычислить закрытый ключ на основе значения открытого ключа
Риски, связанные с процессом майнинга/ консенсуса	– узел не соблюдает все правила консенсуса, потому что у него для такого поведения есть более сильный стимул; – внешнее влияние на принимаемые узлами решения; – алгоритм консенсуса не работает при использовании в новых ситуациях; – атака «двойная трата» (double spend); – атака, при которой противник располагает достаточной вычислительной мощностью, чтобы пересилить честные узлы.
Риски, связанные с обеспечением неприкосновенности частной жизни и конфиденциальности, а также с контентом	– утечка персональных данных из-за того, как работает протокол или используется кошелек; – распределенное хранение информации предполагает наличие копии распределенного реестра на каждом узле – участнике сети, что затрудняет обеспечение конфиденциальности хранимых данных и разграничение доступа для различных участников сети.
Правовые риски	– отсутствие нормативного регулирования; – отсутствие подотчетности при использовании децентрализованных бизнес-моделей.

Несмотря на представленные риски, технология распределительного реестра предоставляет частным компаниям способ хранения информации, позволяющий снизить объем ошибок и повысить уровень безопасности.

Заключение

Цифровая трансформация позволяет ускорить технологическое развитие российских компаний и обеспечить конкурентоспособность разрабатываемых ими продуктов и решений на глобальном рынке. По мере расширения масштабов и ускорения темпов цифровой трансформации современным компаниям для обеспечения безопасности от угроз применения сквозных цифровых технологий необходимо: идентифицировать риски использования цифровых технологий; разрабатывать планы управления рисками до начала реализации цифровых проектов; развивать у сотрудников навыки и компетенцию в отношении рисков реализации цифровых инициатив.

Список источников

1. Белкин А. *Искусственный интеллект: как его использовать в бизнесе уже сегодня.* Доступно: https://www.if24.ru/ai-kak-ispolzovat-v-biznese-uzhe-segodnya/ (дата обращения: 10.02.2020).

2. Бутенко В. Беспроводные технологии в инфраструктуре цифровой экономики // *Электросвязь*, 2017, no. 8 Доступно: http://elsv.ru/valerij-butenko-besprovodnye-tehnologii-v-infrastrukture-

tsifrovoj-ekonomiki/ (дата обращения: 10.02.2020).

3. Вардаков А.А., Перескоков В.Ю. Угрозы и уязвимости промышленного интернета вещей // *Научное сообщество студентов XXI столетия. ТЕХНИЧЕСКИЕ НАУКИ: сб. ст. по мат. LXIV Междунар. студ. науч.-практ. конф.*, no 4(63). Доступно: https://sibac.info/archive/technic/4(63).pdf (дата обращения: 10.02.2020).

4. Варнавский А.В., Бурякова А.О. Перспективы использования технологии распределенных реестров для автоматизации государственного аудита // *Управленческие науки*, 2018, no. 3, с. 88-107.

5. Дюбравак Ш., Ратти К. *Интернет вещей: эволюция или революция?* Доступно: https://www.aig.ru/content/dam/aig/emea/russia/documents/business/iotbroshure.pdf (дата обращения: 10.02.2020).

6. Заболотских З. Искусственный интеллект для бизнеса. Чего ожидать и как учесть в стратегии предприятия? // *Экономика и жизнь*, 2018, no. 46. Доступно: https://www.eg-online.ru/article/385590/ (дата обращения: 10.02.2020).

7. Кешелава А.В., Буданов В.Г., Румянцев В.Ю. и др. *Введение в «Цифровую» экономику*. Москва, ВНИИ Геосистем, 2017.

8. Остроух А.В., Суркова Н.Е. *Интеллектуальные информационные системы и технологии:* монография. Красноярск, Научно-инновационный центр, 2015.

9. Паспорт федерального проекта «Цифровые технологии». Доступно: https://digital.gov.ru/ru/activity/directions/878/ (дата обращения: 10.02.2020).

10. Скляр В. *Информационная безопасность интернета вещей: кто вещь, а кто хозяин?* Доступно: https://habr.com/ru/post/430822/ (дата обращения: 10.02.2020).

11. Филатова М. Процедура цифровой трансформации индустрии продовольствия // *Современная экономика: проблемы и решения*, 2018, no. 11, с. 31-39.

12. Чачин П. Индустриальный IoT: проблемы и перспективы // *Электроника: Наука, Технология, Бизнес*, 2017, no 7, с. 160-170.

RISKS OF DIGITAL BUSINESS TRANSFORMATION

Menyilo Galina Vladimirovna, Cand. Sc. (Econ.), Assoc. Prof.

Voronezh State University, University sq., 1, Voronezh, Russia, 394018; e-mail: mgalina27@mail.ru

Purpose: to analyze digital technologies, which allow determining the risks associated with their use. *Discussion*: digital economy provides for business new directions for development of information technology. New opportunities appear: to exchange Big Data, use artificial intelligence, quantum technologies, robotics, etc. This allows to process large amounts of information and make informed management decisions. But at the same time, there are risks associated with the loss of information and data security, which in turn leads to the need to classify and identify risks that arise in the conditions of digital transformation. *Results*: the risks of digital technologies in the business, such as risks of big data, the risks of the industrial Internet, the risks of artificial intelligence, the risks of wireless technologies, risks, robotics, quantum technology risks, risks of system of the distributed registry were identified and described.

Keywords: risks, digital transformation, end-to-end digital technologies, security.

References

1. Belkin A. *Iskusstvennyy intellekt: kak ego ispolzovat v biznese uzhe segodnya* [Artificial intelligence: how to use it in business today]. Available at: https://www.if24.ru/ai-kak-ispolzovat-v-biznese-uzhe-segodnya (accessed: 10.02.2020).

2. Butenko V. Besprovodnyye tekhnologii v infrastrukture tsifrovoy ekonomiki [Wireless technologies in the digital economy infrastructure]. *Elektrosvyaz*, 2017, no. 8. Available at: http://elsv.ru/valerij-butenko-besprovodnye-tehnologii-v-infrastrukture-tsifrovoj-ekonomiki/ (accessed: 10.02.2020).

3. Vardakov A.A., Pereskokov V.Yu. Ugrozy i uyazvimosti promyshlennogo interneta veshchey [Threats and vulnerabilities of the industrial Internet of things] // *Nauchnoye soobshchestvo studentov XXI stoletiya. TEKhNIChESKIye NAUKI: sb. st. po mat. LXIV mezhdunar. stud. nauch.-prakt. konf.*, no 4(63). Available at: https://sibac.info/archive/technic/4(63).pdf (accessed: 10.02.2020).

4. Varnavskiy A.V., Buryakova A.O. Perspektivy ispolzovaniya tekhnologii raspredelennykh reyestrov dlya avtomatizatsii gosudarstvennogo audita [The prospects of using the technology of distributed registries for automation of state audit]. *Upravlencheskiye nauki,* 2018, no. 3, pp. 88-107. (In Russ.)

5. Dyubravak Sh., Ratti K. *Internet veshchey: evolyutsiya ili revolyutsiya?* [Internet of things: evolution or revolution?]. Available at: https://www.aig.ru/content/dam/aig/emea/russia/documents/business/iotbroshure.pdf (accessed: 10.02.2020).

6. Zabolotskikh Z. Iskusstvennyy intellekt dlya biznesa. Chego ozhidat i kak uchest v strategii predpriyatiya? [Artificial intelligence for business. What to expect and how to take it into account in the company's strategy?]. *Ekonomika i zhizn*, 2018, no. 46. Available at: https://www.

eg-online.ru/article/385590/ (accessed: 10.02.2020).

7. Keshelava A.V., Budanov V.G., Rumyantsev V.Yu. i dr. *Vvedeniye v «Tsifrovuyu» ekonomiku* [Introduction to the «Digital» economy]. Moscow, VNII Geosistem, 2017. (In Russ.)

8. Ostroukh A.V., Surkova N.E. *Intellektualnyye informatsionnyye sistemy i tekhno-logii* [Intelligent information systems and technologies]. Krasnoyarsk, Nauchno-innovatsionnyy tsentr, 2015. (In Russ.)

9. Pasport federalnogo proyekta «Tsifrovyye tekhnologii» [Passport of the Federal project «Digital technologies»]. Available at: https://digital.gov.ru/ru/activity/directions/878/ (accessed: 10.02. 2020).

10. Sklyar V. *Informatsionnaya bezopasnost interneta veshchey: kto veshch. a kto khozyain?* [Information security of the Internet of things: who is the thing and who is the owner?]. Available at: https://habr.com/ru/post/430822/ (accessed: 10.02.2020).

11. Filatova M. Protsedura tsifrovoy transformatsii industrii prodovolstviya [Procedure for digital transformation of the food industry]. *Sovremennaya ekonomika: problemy i resheniya*, 2018, no. 11, pp. 31-39. (In Russ.)

12. Chachin P. Industrialnyy IoT: problemy i perspektivy [Industrial IoT: problems and prospects]. *Elektronika: Nauka. Tekhnologiya. Biznes*, 2017, no. 7, pp. 160-170. (In Russ.)