DOI 10.35775/PSI.2025.67.2.012
УДК 339

ПИН ФЭН
аспирант Российского университета дружбы
народов имени Патриса Лумумбы, Китай
E-mail: 1042228220@rudn.ru
ORCID id: 0000-0002-0121-9552

С.Б. ЗАЙНУЛЛИН
кандидат экономических наук, доцент кафедры
национальной экономики Российского университета дружбы
народов имени Патриса Лумумбы, Россия, г. Москва
E-mail: zaynullin-sb@rudn.ru
ORCID id: 0000-0001-9818-4706

РИСКИ И МЕРЫ ПРОТИВОДЕЙСТВИЯ ЦИФРОВОЙ ТРАНСФОРМАЦИИ ПРЕДПРИЯТИЯ В СОВРЕМЕННОМ МИРЕ

Цифровая трансформация стала для предприятий и организаций единственным способом повышения конкурентоспособности и достижения устойчивого развития. Однако в процессе цифровой трансформации риски безопасности также возрастают, становясь ключевым фактором, ограничивающим успех трансформации. В данной работе исследуются основные риски безопасности, связанные с цифровой трансформацией, и анализируются вызовы безопасности, возникающие в процессе цифровой трансформации, такие как утечка данных, кибератаки, уязвимость системы, недостаточная система управления и халатность персонала. Исходя из этого, в настоящем документе предлагается ряд стратегий и предложений по устранению рисков безопасности цифровой трансформации, направленных на оказание помощи предприятиям и организациям в создании надежной системы управления безопасностью, улучшении возможностей защиты безопасности и обеспечении плавного прогресса цифровой трансформации.

Ключевые слова: *цифровизация, трансформация предприятия, цифровая экономика, цифровая безопасность, управление рисками.*

Введение. Цифровая трансформация относится к систематическому и целостному процессу трансформации, в рамках которого предприятия, организации или отдельные лица оптимизируют и перестраивают свои бизнес-процессы, модели управления и бизнес-модели путем применения цифровых технологий нового поколения, таких как большие данные, облачные вычисления, искусственный интеллект и интернет вещей, для удовлетворения потребностей выживания и развития в условиях цифровой экономики, а также для достижения роста бизнеса и непрерывных инноваций.

Следует подчеркнуть, что в работах российских и китайских авторов, опубликованных в последние годы, освещается широкий спектр вопросов близких к данной предметной области [2; 3; 4; 6; 7; 9; 10; 11; 12; 13; 18; 20; 22; 23].

Однако проблему безопасности цифровой трансформации, направленной на оказание помощи предприятиям и организациям нельзя назвать однозначно исчерпанной. В силу многих объективных обстоятельств изучение обозначенной темы продолжает сохранять высокий уровень актуальности.

Цифровая трансформация – это трансформация высокого уровня, основанная на цифровой модернизации, которая еще больше затрагивает основные процессы компании и направлена на создание новой бизнес-модели. Цифровая трансформация – это развитие цифровых технологий и поддержка возможностей для создания новой и эффективной бизнес-модели [2].

Цифровая трансформация заключается в использовании информационных технологий нового поколения для построения замкнутого цикла сбора, передачи, хранения, обработки и обратной связи данных, разрушения информационных барьеров между разными уровнями и отраслями, повышения общей операционной эффективности отрасли и построения новой цифровой экономической системы [19].

Цифровая трансформация является важным путем для достижения предприятиями устойчивого развития. Понятие цифровой трансформации имеет множество определений в разных странах, и существуют определенные различия в том, как оно выражается. Еще в 2011 году в США была выдвинута концепция «цифрового двойника», которая отражает все характеристики реального объекта от микро до макро через цифровое выражение актуальной сцены, а через технологию «цифрового двойника» большое количество предприятий нашли эффективные инструменты промышленного цифрового управления из всего жизненного цикла проектирования изделия, производство, эксплуатация и техническое обслуживание. В 2015 году Китай также выдвинул стратегию «Сделано в Китае 2025» с точки зрения цифровой трансформации, в которой четко сформулированы ключевые положения, такие как «комплексное развитие нового поколения информационных технологий и производственных технологий», «сосредоточение внимания на развитии интеллектуального оборудования и интеллектуальных продуктов» и «продвижение интеллектуального уровня производственного процесса». В контексте стратегий цифровой трансформации, предлагаемых различными странами, все больше предприятий начали применять различные цифровые технологии для трансформации. IDC, всемирно известная исследовательская организация, ранее провела опрос 2000 генеральных директоров транснациональных корпораций, и результаты показывают, что 67% из 1000 крупнейших компаний мира и 76% из 1000 крупнейших компаний Китая будут использовать цифровую трансформацию в качестве основы своей корпоративной стратегии.

В эпоху цифровой экономики технологии больших данных находятся в постоянном прогрессе, широко используется искусственный интеллект и другие

производные инструменты, и на этой основе постоянно обогащаются различные новые технологии, новые отрасли и новые модели, так что данные стали новым фактором производства за счет продвижения цифровой экономики [19], и данные постепенно стали корпоративным активом. Тем не менее, у быстрого развития новых технологий есть две стороны: усиление рисков безопасности создало большие препятствия для дальнейшего использования данных, а частые инциденты, такие как утечка данных и злоупотребление данными, в определенной степени ограничили дальнейшее развитие цифровой экономики [19].

В большом количестве практик предприятия создали более сложную и большую базу данных, а также более открытые и разнообразные сценарии применения данных, которые заставляют предприятия получать массу возможностей для развития и инноваций, и в то же время предприятиям приходится иметь дело с уникальными рисками в процессе трансформации. Согласно отчету PwC Digital Trust Insights China Report за 2019 год, с точки зрения руководителей высшего звена и ИТ-специалистов, наиболее серьезным риском для цифровой трансформации является управление данными или конфиденциальность (28% ответов на опрос). Кроме того, вторым по величине риском стал инновационный риск, возникающий в процессе запуска новых продуктов и услуг (на него приходится 19% отзывов от опроса); Далее следуют риски кибербезопасности в традиционном понимании (18% ответов на опрос) [19].

Предыстория и методология. С развитием цифровой трансформации важность рисков безопасности становится все более очевидной. Цифровая трансформация означает, что предприятия и организации претерпевают глубокие изменения на многих уровнях, таких как бизнес, процесс, технологии и т.д., что неизбежно связано с большим объемом обработки, передачи и хранения данных. В этом процессе риски безопасности, такие как утечки данных, кибератаки и уязвимости систем, угрожают основным активам предприятий и организаций, что может привести не только к финансовым потерям, но и повлиять на репутацию и даже поставить под угрозу выживание предприятий [19].

Риски безопасности данных: в процессе цифровой трансформации данные стали основным активом предприятий и организаций. Утечка, изменение или потеря данных могут быть дорогостоящими. Утечки данных могут привести к раскрытию коммерческой тайны компании и информации о клиентах, что приведет к потере конкурентоспособности и кризису доверия.

Риск кибератаки: хакеры могут использовать уязвимости системы, слабые пароли и другие средства для кражи данных, повреждения систем и даже вымогательства денег. Кибератаки могут не только привести к прямым финансовым потерям, но и повлиять на нормальную работу и репутацию бизнеса.

Риск уязвимости системы: в процессе цифровой трансформации предприятиям и организациям необходимо внедрять большое количество новых технологий и систем. Эти системы могут иметь неизвестные уязвимости и недостатки, что приводит к сбоям системы, потере данных и многому другому. Кроме того,

внедрение новых систем также может привести к проблемам совместимости с другими системами, что еще больше увеличивает риск.

Риски, связанные с соблюдением нормативных требований: цифровая трансформация включает в себя законы и нормативные акты во многих странах и регионах. Предприятия и организации должны убедиться, что их цифровая практика соответствует этим правилам, иначе они рискуют столкнуться с судебными тяжбами и штрафами. Например, GDPR Европейского Союза требует от предприятий строго защищать персональные данные, а нарушителям могут грозить крупные штрафы.

Риски культурных и организационных изменений: цифровая трансформация – это не только изменение на техническом уровне, но и включает в себя многие аспекты, такие как корпоративная культура, организационная структура и поведение сотрудников. Неспособность эффективно внедрить культурные и организационные изменения может привести к таким проблемам, как сопротивление сотрудников, отсутствие навыков или способность к адаптации, что, в свою очередь, может повлиять на успех цифровой трансформации.

Первопричины и причины возникновения рисков безопасности при цифровой трансформации предприятий многогранны, и с быстрым развитием технологий цифровая трансформация включает в себя множество сложных систем и платформ. Эти системы могут иметь уязвимость с точки зрения взлома или утечки данных. В то же время интеграция и совместимость между различными системами также могут привести к рискам безопасности. Сотрудники являются наиболее активным фактором цифровой трансформации и основным источником рисков для безопасности. Сотрудники могут проявлять небрежность или злонамеренность в своих действиях, что приводит к инцидентам безопасности, таким как утечка данных и неправильная работа. Кроме того, злоупотребление полномочиями со стороны инсайдеров или сговор с посторонними также может нанести существенные убытки бизнесу. Организационная структура и культура организации оказывают значительное влияние на риски безопасности, связанные с цифровой трансформацией. Если в компании отсутствует четкая политика и процессы безопасности или если сотрудники не осведомлены о безопасности, это может привести к рискам безопасности [19].

Обсуждение и результаты. Постоянно обновляя и совершенствуя технологии, разрабатывая инновационные технологии безопасности, создавая научно-исследовательские группы в области безопасности, укрепляя сотрудничество с другими организациями безопасности и уделяя внимание новым технологиям и тенденциям в области безопасности, предприятия могут построить более полную и эффективную систему защиты безопасности и эффективно реагировать на риски безопасности в процессе цифровой трансформации [19]. Включает:

А. Непрерывное обновление и модернизация технологий: предприятиям необходимо регулярно обновлять и модернизировать свои системы и платформы, чтобы обеспечить использование новейших технологий безопасности для защиты от потенциальных угроз. Это включает в себя обновление критически

важных компонентов, таких как операционные системы, базы данных, брандмауэры, системы обнаружения вторжений и многое другое.

Б. Исследования и разработки инновационных технологий безопасности: например, разработка новых алгоритмов шифрования, разработка более эффективных правил брандмауэра и применение искусственного интеллекта для защиты безопасности.

В. Создание команды по исследованиям и разработкам в области безопасности: предприятиям необходимо создать профессиональную команду по исследованиям и разработкам в области безопасности, которая будет отвечать за исследования в области технологий и инноваций. Он может своевременно находить и устранять уязвимости в системе безопасности и улучшать общую защиту безопасности.

Г. Обращайте внимание на новые технологии и тенденции в области безопасности: предприятиям необходимо уделять пристальное внимание новым технологиям и тенденциям в области безопасности, таким как безопасность облачных вычислений, безопасность Интернета вещей и блокчейн, а также своевременно корректировать и оптимизировать свои стратегии защиты безопасности, чтобы улучшить свою способность реагировать на будущие угрозы безопасности.

Формулируя и совершенствуя соответствующие законы и нормативные акты и создавая специальные регулирующие органы, правительство может обеспечить надежную гарантию цифровой трансформации предприятий и частных лиц, а также обеспечить безопасность и соответствие требованиям цифровой трансформации. Включает:

А. Формулирование и совершенствование соответствующих законов и нормативных актов: Правительство должно разрабатывать и совершенствовать соответствующие законы и нормативные акты для устранения рисков безопасности, которые могут возникнуть в процессе цифровой трансформации.

Б. Создание специализированного регулирующего органа: Правительства должны создать специальный регулирующий орган для надзора и управления рисками безопасности в процессе цифровой трансформации.

В. Укрепление межведомственной координации: цифровая трансформация затрагивает множество областей и ведомств, и правительствам следует укреплять координацию между различными ведомствами для совместного устранения рисков безопасности в условиях цифровой трансформации.

Г. Укрепление международного сотрудничества: цифровая трансформация является глобальной тенденцией, и правительства должны укреплять международное сотрудничество для совместного устранения рисков безопасности в условиях цифровой трансформации.

Благодаря обучению и профессиональной подготовке, формированию культуры безопасности и кодекса поведения, обучению и инструктажу пользователей, технической поддержке и инструментальной поддержке, отработке учений по моделированию и реагированию на чрезвычайные ситуации, а также оценке

и аудиту безопасности, можно значительно повысить осведомленность предприятий и пользователей в области безопасности и возможности по профилактике [19]. Включает:

А. Обучение: с помощью внутренней рекламы, плакатов, электронных писем и т.д. постоянно напоминайте сотрудникам о необходимости уделять внимание безопасности личных и корпоративных данных, а также повышайте осведомленность сотрудников в вопросах безопасности.

Б. Культура безопасности и кодекс поведения: Руководство предприятия должно поддерживать и продвигать корпоративную культуру, ориентированную на безопасность, которая разъясняет нормы безопасности, которым сотрудники должны следовать при использовании корпоративных устройств, сетей и данных, например, не использовать слабые пароли и не делиться конфиденциальной информацией.

В. Обучение и руководство для пользователей: Предоставление пользователям подробных инструкций по безопасности. Регулярная отправка пользователям советов по безопасности по SMS, электронной почте и т.д., чтобы напомнить им о последних киберугрозах.

Г. Поддержка технологий и инструментов: Разработка простых в использовании инструментов и приложений для обеспечения безопасности, чтобы снизить барьер для обучения и использования.

Д. Имитационные учения и реагирование на чрезвычайные ситуации: Создание механизмов быстрого и эффективного реагирования на чрезвычайные ситуации для быстрого принятия мер и сокращения потерь в случае инцидента безопасности.

Создание системы управления безопасностью является одной из ключевых мер для обеспечения успеха цифровой трансформации предприятия. Включает:

А. Разработку стратегии безопасности цепочки поставок, предприятиям необходимо уточнить цели и принципы безопасности цепочки поставок и сформулировать соответствующую политику безопасности. Эти стратегии должны включать в себя идентификацию, оценку, мониторинг и реагирование на риски в цепочке поставок.

Б. Создание механизма оценки рисков в цепочке поставок, предприятиям необходимо провести оценку рисков всех звеньев цепочки поставок для выявления потенциальных рисков безопасности. Это включает в себя такие аспекты, как безопасность поставщиков, качество продукции, логистика и транспортировка и т.д.

В. Укрепление управления поставщиками, предприятиям необходимо проводить строгий отбор и оценку поставщиков, чтобы гарантировать, что поставщики имеют хорошую систему управления безопасностью и возможности обеспечения качества продукции.

Г. Усиление безопасности логистики и перевозок предприятиям необходимо усилить управление безопасностью логистики и перевозок, а также принять

ряд мер по обеспечению безопасности грузов в процессе перевозки. Например, использование передовых технологий отслеживания логистики, усиление обучения персонала транспорта технике безопасности, создание механизмов реагирования на чрезвычайные ситуации и т.д.

Выводы. В данной статье рассматриваются риски безопасности в процессе цифровой трансформации и предлагаются соответствующие стратегии и меры по их устранению. Цифровая трансформация стала важным драйвером развития бизнеса, однако с непрерывным развитием технологий и их широким применением риски безопасности также возросли. В этой статье рассматриваются многочисленные аспекты цифровой трансформации, включая технологии, людей, управление и цепочку поставок, чтобы выявить существующие угрозы безопасности и изучить эффективные способы противодействия им. На техническом уровне цифровая трансформация подвергает предприятия большему риску кибератак и утечек данных. Поэтому необходимо усилить защиту сети, усовершенствовать технологию шифрования данных и усилить контроль доступа. В то же время, с широким применением таких технологий, как облачные вычисления, большие данные и искусственный интеллект, предприятиям необходимо обеспечивать безопасность этих технологий и избегать потенциальных уязвимостей безопасности. На кадровом уровне цифровая трансформация требует от сотрудников более высокой цифровой грамотности и осведомленности в вопросах безопасности. В связи с этим предприятиям необходимо усилить подготовку и обучение сотрудников по вопросам безопасности, чтобы повысить их способность выявлять риски безопасности и реагировать на них. В то же время формировать культуру безопасности, поощрять работников к активному участию в управлении безопасностью и надзоре, совместно поддерживать безопасность и стабильность предприятия. На уровне управления предприятиям необходимо усовершенствовать систему управления безопасностью, уточнить обязанности и процессы в области безопасности, а также обеспечить эффективное внедрение системы управления безопасностью. В то же время создать механизм мониторинга безопасности и раннего предупреждения для своевременного выявления и решения проблем безопасности. Кроме того, укрепляйте коммуникацию и сотрудничество с внешними организациями, такими как поставщики и партнеры, для совместного устранения рисков безопасности цепочки поставок. На уровне цепочки поставок в этом документе основное внимание уделяется важности создания системы управления безопасностью цепочки поставок. Создав стратегию безопасности цепочки поставок, механизм оценки рисков, систему управления поставщиками, систему мониторинга безопасности логистики и транспорта, а также механизм планирования и реагирования на чрезвычайные ситуации, предприятия могут обеспечить безопасность и стабильность цепочки поставок и снизить риски безопасности в процессе цифровой трансформации.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Ань Тунлян и Вэнь Жуй.** Механизм влияния цифровой трансформации на инновации китайских предприятий и его эмпирическое обоснование. Дискуссия о современной экономике.
2. Артемьев Н.В., Новиков А.В., Гольцева О.С., Золкин А.Л., Новосельский С.О. Безопасность городской среды на основе развития цифровых сервисов в современных социально-экономических условиях // Вопросы политологии. 2024. № 11.
3. Ашмарина А.А. «Биобезопасность» и «биозащищенность» в России в условиях развития цифровых технологий // Вопросы политологии. 2024. № 1.
4. **Ван Хайсюань, Шувалова Н.А.** Интерес к электронной коммерции // Евразийский Союз: вопросы международных отношений. 2024. № 5.
5. **Гу Лимэй, Ли Хуаньхуань, Чжан Ян.** Исследование проблем и пути оптимизации цифровой трансформации городов – Тематическое исследование Шанхая[J]. Журнал Сианьского университета Цзяотун (Социальные науки). 2022. 42 (3).
6. **Гуров А.И.** Взаимосвязь между эффективностью государственного управления и внедрением цифровых систем управления, современных методик планирования и принятия решений // Вопросы политологии. 2023. № 12.
7. **Зайнуллин С.Б., Шишова Ю.А., Чжан Яци, Пин Фэн, Розмари Нвачукву Чидимма.** Проблематика интернет-торговли на российском и евразийском рынках // Евразийский Союз: вопросы международных отношений. 2024. № 1.
8. Исследовательская группа по развитию и политике цифровой экономики Китая, Исследовательский центр развития Государственного совета, Ма Минцзе, Тянь Цзетан, Дай Цзяньцзюнь, Ян Чао и Шэнь Хэнчао. (2019). Характеристики, проблемы и контрмеры цифровой трансформации обрабатывающей промышленности Китая. Исследования в области развития (6), 5.
9. **Ковригин Д.Э.** Применение теории полей для анализа взаимодействия государства и бизнеса в российском сегменте киберпространства // Вопросы национальных и федеративных отношений. 2024. № 7.
10. **Колесников А.И.** Технократическая легитимация и цифровизация в современной России // Вопросы национальных и федеративных отношений. 2024. № 7.
11. **Колосова О.А., Андреева А.Л., Бегичева О.Л., Комарова А.А., Новосельский С.О.** Цифровая трансформация маркетинга // Евразийский Союз: вопросы международных отношений. 2024. № 3.
12. **Комерцов В.В., Мрыхина О.Д., Григорян Д.К.** Социальная инженерия в киберпространстве как угроза национальной безопасности // Вопросы национальных и федеративных отношений. 2025. № 1.

13. Литвин Л.А. Риски и перспективы внедрения электронного правительства в контексте трансформации государственного управления в Российской Федерации // Вопросы политологии. 2024. № 1.
14. **Ли Цзин.** Исследование влияния цифровой трансформации на управление предприятием. Маркетинг. 2023. (5).
15. **Лю Гоу, Ли Цзюньхуа, Тан Чангань.** Цифровая экономика, повышение эффективности сферы услуг и высококачественное экономическое развитие Китая[J/OL]. Южная экономика. 1-24.
16. **Лю Чжиюань.** Информационные риски и меры противодействия цифровой трансформации коммерческих банков. Цинхай Финанс. 2020. (8),3.
17. ПрайсуотерхаусКуперс. Отчет о цифровом доверии в Китае. 2019.
18. Сурма И.В. Вызовы и угрозы технологий искусственного интеллекта как универсального инструмента социально-политической и экономической трансформации современного общества // Вопросы политологии. 2024. № 6.
19. Форум развития Китая. (2018-03). Модели и пути цифровой трансформации традиционных отраслей // https://www.cdf.org.cn/cdf2018/xzbg/5445.htm?share=true#content.
20. **Фэн Шухань.** Влияние цифрового экономического управления на глобальное экономическое развитие в условиях цифровой экономики // Союз: вопросы международных отношений. 2023. № 7.
21. **Чэнь Цзинь, Ян Вэньчи, Юй Фэй.** Экологическая стратегия совместных инноваций в цифровой трансформации: на основе обсуждения стратегии Huawei Enterprise Business Group (EBG) в Китае[J]. Обзор управления Цинхуа. 2019(06).
22. **Шугаева О.В., Зайченко А.А., Золкин А.Л., Новосельский С.О., Петрушина О.В.** Цифровая трансформация администрирования платежно-расчетных отношений в деятельности таможенных органов // Евразийский Союз: вопросы международных отношений. 2024. № 4.
23. Юань Чэньчжао, Цянь Чэнь, Бычков А.А. Исследование и перспективы цифровой трансформации государственного управления // Вопросы политологии. 2024. № 5.

PING FENG
Postgraduate student of Peoples' Friendship
University of Russia named after Patrice Lumumba, China
ORCID id: 0000-0002-0121-9552

S.B. ZAINULLIN
PhD in Economics, Associate Professor,
Department of National Economics, Peoples' Friendship
University of Russia, named after Patrice Lumumba,
Moscow, Russia
ORCID id: 0000-0001-9818-4706

RISKS AND COUNTERMEASURES OF ENTERPRISE DIGITAL TRANSFORMATION IN THE MODERN WORLD

Digital transformation has become the only way for enterprises and organizations to enhance their competitiveness and achieve sustainable development. However, in the process of digital transformation, security risks also increase, becoming a key factor restricting the success of transformation. This paper studies the main security risks involved in digital transformation, and analyzes the security challenges faced in the process of digital transformation, such as data leakage, cyber attacks, system vulnerability, insufficient management system, and personnel negligence. On this basis, this paper proposes a series of strategies and suggestions to deal with the security risks of digital transformation, aiming to help enterprises and organizations establish a sound security management system, improve security protection capabilities, and ensure the smooth progress of digital transformation.

Key words: *digitalization, enterprise transformation, digital economy, digital security, risk management.*