Электронный научный журнал «Век качества» ISSN 2500-1841 http://www.agequal.ru
2024, №2 http://www.agequal.ru/pdf/2024/AGE_QUALITY_2_2024.pdf

Ссылка для цитирования этой статьи:

Салютина Т.Ю., Франк И.А. Систематизация рисков развития бизнес-технологий в условиях глобального цифрового развития // Электронный научный журнал «Век качества». 2024. №2. С. 141-170. Режим доступа: http://www.agequal.ru/pdf/2024/224007.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 330.341

Систематизация рисков развития бизнес-технологий в условиях глобального цифрового развития

Салютина Татьяна Юрьевна,
заведующая кафедрой «Цифровая экономика, управление и бизнес-технологии»
Московского технического университета связи и информатики,
111024, Россия, г. Москва, Авиамоторная ул., д. 8А,
t.i.saliutina@mtuci.ru

Франк Ирина Александровна,
аспирант Московского технического университета связи и информатики,
111024, Россия, г. Москва, Авиамоторная ул., д. 8А,
i.a.vasileva@mtuci.ru

В статье систематизируются основные виды рисков, возникающие в процессе цифрового развития бизнес-технологий. Анализируются потенциальные угрозы, связанные с развитием цифровых технологий в условиях быстрого цифрового прогресса, рассматриваются методы и стратегии их управления. Уделяется внимание не только техническим, но и социально-экономическим рискам, влияющим на бизнес-технологии в условиях глобального цифрового развития. Предлагаются практические рекомендации по минимизации рисков и повышению устойчивости бизнеса в условиях цифровой трансформации.

Ключевые слова: бизнес-технологии; цифровое развитие; цифровая экономика; технические риски; цифровые технологии; социально-экономические риски; управление рисками.

Введение

С развитием цифровых технологий в мире все больше компаний ориентируются на использование современных информационных инструментов для оптимизации своей деятельности. Вместе с возможностями, которые

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

предоставляет цифровизация, возрастает и количество рисков, с которыми сталкиваются бизнес-технологии.

Кроме того, компании должны разработать четкие стратегии цифрового развития, которые помогут им адаптироваться к быстро меняющейся цифровой среде, минимизировать риски и максимизировать преимущества цифровых технологий. Это включает в себя постоянное обновление IT-инфраструктуры, внедрение современных систем защиты информации, поиск и развитие новых цифровых решений, а также обучение персонала новым навыкам.

Успешное развитие компаний в современном мире связано с внедрением инновационных технологий, но важно помнить и о рисках, которые могут возникнуть, поэтому нужно закладывать в расходы компании управление рисками. Оценка рисков предоставляет компаниям возможность оценить вероятность возникновения какого-либо неблагоприятного события, которое может негативно повлиять на бизнес.

Систематизация и методы анализа рисков развития бизнес-технологий в условиях глобального цифрового развития

Методы оценки рисков играют важную роль и помогают компаниям принимать продуманные стратегические решения в условиях неопределенности и изменчивости внешней среды [1]. На рис. 1 изображены методы анализа рисков. Каждый способ имеет свои преимущества и недостатки, поэтому, чтобы получить максимально достоверные результаты, необходимо использовать несколько вариантов.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Источник: составлено авторами

Рис. 1. Методы анализа рисков

Для успешного видения бизнеса и внедрения технологий необходимо систематизировать риски, поэтому на рис. 2 представлены основные этапы систематизации рисков развития бизнес-технологий в условиях глобального цифрового развития.

Источник: составлено авторами

Рис. 2. Основные этапы систематизации рисков

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

1. *Идентификация рисков*. Первый шаг в систематизации рисков развития бизнес-технологий - это их идентификация. Определяются все возможные риски, которые могут возникнуть с применением технологий в деятельности компании. Рассматриваются потенциальные угрозы, с которыми может столкнуться компания при внедрении и эксплуатации бизнес-технологий.
2. *Классификация рисков*. На этом этапе риски классифицируется на группы, что позволяет лучше организовать процесс анализа рисков и в будущем позволит эффективно распределить ресурсы на минимизацию угроз.
3. *Анализ рисков*. Для более глубокого понимания рисков необходимо провести их анализ. Выполняется оценка риска и величина потенциальных убытков. Оценка вероятности возникновения угроз и их потенциальных последствий позволит разработать эффективные стратегии управления рисками.
4. *Разработка мер по управлению рисками*. После проведённого анализа рисков необходимо разработать план действий, который будет применяться для уменьшения вероятности возникновения рисков или устранения их последствий. Данный пункт входит в задачи риск-менеджмента.
5. *Мониторинг и обновление стратегии управления рисками*. В бизнес-среде постоянно происходят изменения, связанные с внешними и внутренними условиями, поэтому необходимо постоянно пересматривать стратегию управления рисками и вносить корректировки в план действий компании.

Рассмотрев пять этих этапов, можно сделать вывод, что в основе успешной систематизации рисков (а после – в управлении ими) лежит необходимость в следующих процессах: идентификация, классификация и проведение анализа рисков развития бизнес-технологий [2]. На рис. 3 как результаты данного процесса представлены две группы рисков развития бизнес-технологий.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Источник: составлено авторами

Рис. 3. Риски развития бизнес-технологий

Риски технологий цифровой трансформации

1. Облачные технологии. Облачные технологии являются неотъемлемой частью современного бизнеса, предоставляют компаниям возможность хранить данные, управлять процессами и разрабатывать продукты и услуги. Как и любая другая технология, облачные технологии не лишены определенных рисков, которые компании должны учитывать [3].

Первоочередным риском, о котором задумывается большинство компаний, - это потенциальные угрозы безопасности данных. Облачные технологии используют для хранения данных удаленные серверы, поэтому существует вероятность несанкционированного доступа к ним со стороны злоумышленников. Это может привести к утечке конфиденциальных данных о компаниях или их

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

клиентах, что повлечет за собой финансовые потери и потерю доверия со стороны клиентов.

Вторым по важности риском является недоступность облачных технологий в случае сбоев или неполадок в работе. Если компания полностью зависит от облачных приложений и хранилищ, то даже кратковременные проблемы с доступом могут существенно нарушить бизнес-процессы, привести к потере доходов и навредить имиджу компании.

Кроме того, стоит помнить, что при использовании облачных технологий нужно соблюдать законы о защите данных, ведь неправильное хранение или передача данных третьим лицам может привести к штрафам или длительным судебным разбирательствам, что будет иметь серьезные последствия для компании.

2. Дистанционная работа. Растущая популярность дистанционной работы предоставляет множество удобств как для компаний, так и для их сотрудников. При этом, несмотря на все преимущества, нужно учитывать и риски связанные с дистанционной работой.

Существует риск утечки конфиденциальной информации. При работе из дома сотрудники могут столкнуться с различными угрозами, например, при использовании незащищенных сетей может произойти взлом персональных устройств, что впоследствии приведет к краже данных.

Уменьшается уровень контроля и управления рабочим процессом сотрудников. При отсутствии возможности контролировать менеджеры могут столкнуться с проблемой отслеживания выполнения задач, контроля времени работы и поддержания дисциплины, что впоследствии может привести к убыткам компании.

3. Искусственный интеллект. В современном мире развитие искусственного интеллекта приводит к значительным изменениям во всех отраслях, включая бизнес. Искусственный интеллект предоставляет огромные возможности для повышения производительности, автоматизации процессов и создания новых

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

продуктов и услуг. Вместе с этим, существуют и риски, которые необходимо принимать во внимание при внедрении искусственного интеллекта [4, 5].

Самый значительный и наиболее опасный риск на данный момент связан с тем, что многие люди могут потерять свои рабочие места из-за автоматизации. Появление искусственного интеллекта может повлиять на сокращение рабочих мест, что приведет к социальным проблемам и ухудшению экономической ситуации в определенных регионах.

Необходимо помнить и о потенциальной зависимости от технологических компаний, которые предоставляют данную технологию. Если бизнес зависит от одного поставщика, то это может привести к уязвимости и риску для бизнеса в случае прекращения работы этого поставщика или изменения условий предоставления услуг. Зависимость от одного поставщика может приводить к постоянному увеличению затрат на данную технологию, при этом данные затраты со временем могут перестать окупаться.

4. Цифровые платформы. В настоящее время цифровые платформы становятся неотъемлемой частью бизнеса, предоставляя компаниям различные инструменты для повышения эффективности, улучшения качества обслуживания клиентов и расширения географии бизнеса. Даже при значительных преимуществах и здесь существуют также риски для бизнеса [6, 7].

Утечка конфиденциальной информации на данный момент является одним из основных рисков. Ведение бизнеса на цифровых платформах требует передачи и хранения большого объема конфиденциальных данных, включая данные о клиентах, финансовые отчеты и другую информацию. Несоблюдение соответствующих мер безопасности может привести к утечке данных и впоследствии к негативным последствиям для компании.

Недостаточная защита от кибератак также является риском для компаний. Цифровые платформы подвержены угрозам со стороны хакеров или другим онлайн-угрозам, которые могут нанести серьезный ущерб бизнесу, ведь

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

неправильно построенные системы защиты делают компанию уязвимой перед такими атаками и могут принести значительные убытки.

5. Робототехника. Область робототехники из года в год становится все более актуальной и востребованной. Для компаний появляются новые возможности для автоматизации процессов и улучшения производительности. Использование робототехники в бизнесе несет в себе некоторые риски, которые необходимо учитывать.

Высокая стоимость внедрения и поддержки - один из основных рисков. Приобретение и настройка технологий требует значительных инвестиций, а также постоянной технической поддержки. Не все компании могут позволить себе такие затраты, особенно если они только начинают внедрять робототехнику в свои процессы. Для малого и среднего бизнеса внедрение таких технологий практически не возможно из-за высоких затрат и невозможности окупить их за короткий срок.

Важным риском является потенциальная угроза рабочим местам. Автоматизация процессов может привести к сокращению рабочих мест, что может вызвать негативную реакцию со стороны работников и общественности. Компании должны тщательно обдумать, как они могут использовать робототехнику, чтобы улучшить процессы, не нанося ущерба своим сотрудникам.

Также следует учитывать риск дефектов и сбоев в работе. Техника все равно может подвергаться поломкам, ошибкам и сбоям, несмотря на высокую точность и эффективность, что может привести к нарушению производственных процессов и потерям для бизнеса [8].

6. Большие данные. Большие объемы информации, которые собираются и анализируются компаниями, помогают им принимать более обоснованные решения, что приводит к более эффективному применению ресурсов. Использование больших данных также несет определенные риски для бизнеса, которые важно учитывать.

Безопасность данных - это основной риск для бизнеса. Увеличение объемов информации делает компании более уязвимыми к кибератакам и утечкам

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

информации. Потеря контроля над данными и их передача в руки конкурентов могут нанести серьезный экономический и репутационный ущерб. Большие данные часто содержат конфиденциальные и личные данные клиентов, поэтому их безопасность должна быть приоритетом для любого бизнеса.

Большие данные могут помочь компаниям лучше понимать своих клиентов и рынок, но неправильное использование данных может привести к негативным последствиям. Например, использование данных о потребителях для продажи их личной информации третьим лицам может привести к репутационным потерям и юридическим проблемам.

Обработка и хранение больших объемов информации требуют значительных инвестиций в технологии и персонал, поэтому компания должна быть уверена, что она способна извлечь значимую пользу из этой технологии, тем самым способствуя увеличению прибыли в будущем.

7. Цифровой двойник. Виртуальные копии (модели) людей, физических объектов, процессов или систем интегрируются с данными, полученными с их физических прототипов с помощью сенсоров, чтобы удалённо управлять, отслеживать или предсказывать поведение реальных объектов [9]. В современном мире цифровые двойники в бизнесе приносят серьезные риски.

Хакеры могут использовать цифровые двойники, например, представляясь сотрудником компании или создавая копию сайта, а клиенты, обращаясь к мошенникам, могут передать им личную информацию или даже потерять свои средства. Такая ситуация может привести к потере репутации компании, так как клиент будет подозревать компанию в пособничестве.

Возможность манипуляции реальными данными также несет определенные угрозы для компании. Цифровые двойники могут быть использованы для изменения информации в базах данных компании, что может привести к ошибочным решениям и убыткам. Кроме того, цифровые двойники могут подделывать коммуникацию, что может сбивать с толку заказчиков и партнеров.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

8. Интернет вещей. Интернет вещей стал неотъемлемой частью современного бизнеса, предоставляя компаниям возможность улучшить процессы, оптимизировать производство и повысить эффективность. С ростом использования технологии Интернета вещей возникают и риски, которые необходимо учитывать при внедрении этой технологии в бизнес.

Несмотря на то, что в бизнесе, особенно крупном, используются надежные системы аутентификации, к сожалению, про безопасность устройств Интернета вещей обычно забывают. Так как устройства соединяются с сетью через Интернет, это делает их уязвимыми для кибератак. Киберпреступники могут использовать уязвимости в устройствах для получения доступа к конфиденциальной информации компании или для проведения кибератак на её сеть. Это может привести к утечке данных, нарушению бизнес-процессов и финансовым потерям.

Устройства могут быть подвержены неисправностям и отказам, что влечет за собой простои в производственном процессе и убытки для компании. Следовательно, компании должны предпринять дополнительные меры по обеспечению надежности устройств и поддержанию их работоспособности.

9. Блокчейн, криптовалюты. Блокчейн-технология и криптовалюты только становятся частью современного бизнеса, но уже существуют значительные риски, с которыми связано использование этих технологий.

Первый и, пожалуй, самый заметный риск - это волатильность цен криптовалют. Цены на криптовалюты, например, такие как биткоин или эфириум, могут значительно колебаться за короткий период времени. Это создает риски для бизнеса, если он зависит от криптовалют с целью проведения платежей или инвестиций.

Во многих странах правительства только начинают разрабатывать законы, регулирующие использование криптовалют. Это может создать неопределенность и непредсказуемость для международных компаний и проведения транзакций.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Также стоит упомянуть риск потери доступа к средствам. Если компания хранит свои активы в цифровом кошельке, то есть вероятность потери доступа к этим средствам из-за утраты ключей или других проблем [10].

10. Чат-боты. Развитие технологий искусственного интеллекта привело к возникновению новых инструментов для ведения бизнеса. Чат-боты - это специально разработанная программа, которая имитирует общение людей и предназначена поддерживать ситуативный диалог с пользователем. Используется для автоматических ответов на ряд вопросов без участия людей. Как правило, чат-бот программируют для ответов на самые частые вопросы и выполнение типовых действий.

Один из основных рисков - это возможность выхода чат-бота из строя. Если программа не работает правильно или не отвечает на запросы клиентов, это может привести к негативному опыту пользователей и снижению доверия к компании, следовательно, к финансовым потерям.

Чат-боты могут обрабатывать конфиденциальную информацию, такую как персональные данные клиентов, поэтому они могут стать объектом кибератак. Ненадежно защищенные каналы связи могут стать источником утечки информации и нанести ущерб репутации компании.

Взаимодействие с человеком может быть более привлекательным для клиентов, поскольку оно чаще всего более эмоционально и индивидуально. Чат-боты могут уменьшить уровень персонализации обслуживания, что может привести к потере клиентов.

11. 3D-печать. Эта технология становится все более популярной, так как она позволяет создавать прототипы, запасные детали, украшения и многое другое. Как и любая новая технология, 3D-печать также несет определенные риски, которые могут повлиять на бизнес.

С развитием технологии все проще становится скопировать и распространить различные товары и изделия. Это может привести к ущербу для компаний, которые инвестировали в разработку уникальных продуктов. Поэтому владельцам бизнеса

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

необходимо обеспечить защиту своей интеллектуальной собственности и следить за тем, каким образом их продукты могут быть воспроизведены с помощью 3D-печати.

Также следует учитывать экологические риски 3D-печати. Использование пластика и других материалов в процессе печати может привести к увеличению выбросов и загрязнению окружающей среды. Поэтому компании, использующие 3D-печать, должны принимать меры для уменьшения влияния своей деятельности на окружающую среду.

На рис. 4 представлены перечисленные выше риски бизнес-технологий цифровой трансформации, расставленные на графике по степени влияния и вероятности их возникновения в условиях глобального цифрового развития.

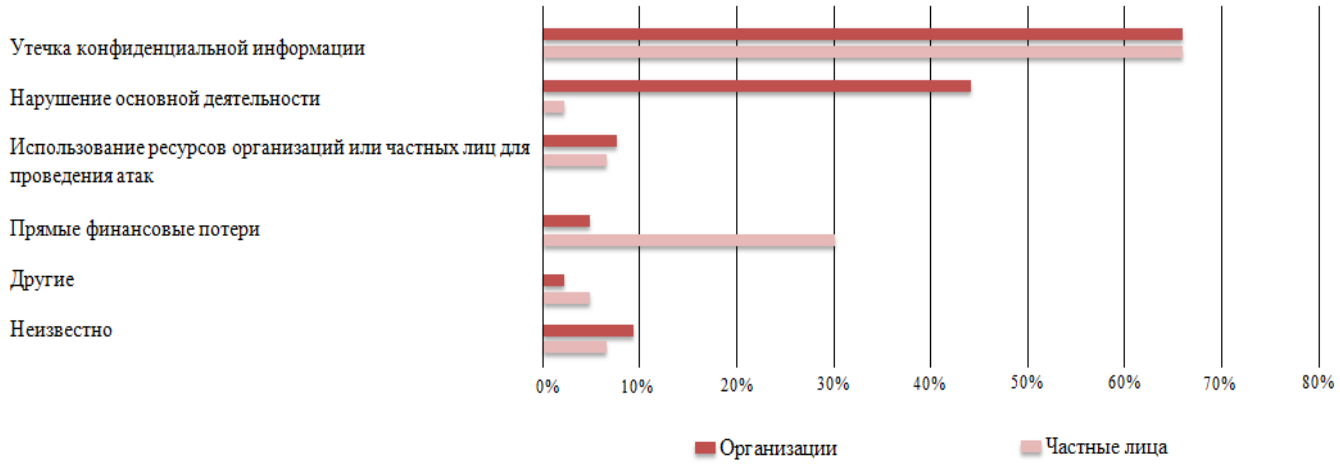
Источник: составлено авторами

Рис. 4. Вероятность возникновения рисков бизнес-технологий и степень их влияния

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Типовые риски цифровой трансформации

1. Хакерские атаки. Хакеры могут нанести серьезный ущерб бизнесу, выкрав важную информацию. Например, успешные кибератаки затрагивали предприятия малого и крупного бизнеса, а также частных лиц, данные о последствиях этих атак за 2023 г. представлены на рис. 5. Наиболее частыми последствиями атак были: получение злоумышленниками конфиденциальной информации и нарушение основной деятельности организаций. Таким образом, компания может потерять репутацию и доверие клиентов, что, в свою очередь, приведет к финансовым потерям.



Источник: составлено авторами

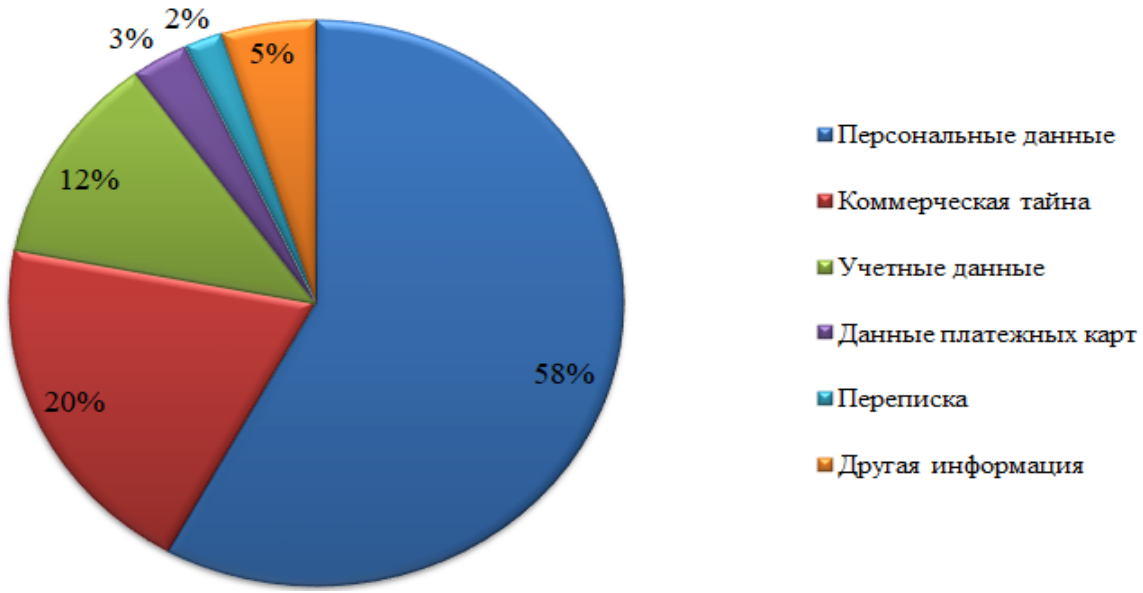
Рис. 5. Последствия хакерских атак за 2023 г.

Хакеры могут нанести ущерб бизнесу через блокировку доступа к веб-сайту компании, что приведет к потере клиентов и доходов. Также хакеры могут использовать вымогательские атаки, взламывая систему и требуя выкуп за возврат доступа к информации.

Важно отметить, что любой бизнес подвержен риску хакерских атак. Малые и средние предприятия считают, что они не являются целью для хакеров, но на самом деле они могут быть еще более уязвимы, так как у них отсутствуют надлежащие меры безопасности [11].

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

2. Утечка информации. Утечка конфиденциальных данных о клиентах и партнерах может произойти из-за небрежного обращения с данными, хакерских атак, кражи устройств с хранящимися на них сведениями и других ситуаций [12]. На рис. 6 представлены типы украденных данных за 2023 г., которые чаще всего интересовали злоумышленников. Из-за этого компания может столкнуться с юридическими проблемами и штрафами, а также потерей доверия со стороны клиентов и может понести значительные убытки.



Источник: составлено авторами

Рис. 6. Типы украденных данных за 2023 г.

Другим риском является утрата коммерческой тайны и интеллектуальной собственности. Несанкционированное раскрытие планов, идей, разработок и процессов может привести к усилению конкурентов на рынке, утрате конкурентных преимуществ и снижению доходов компании.

3. Потеря (искажение) информации. Информация служит основой для принятия стратегических решений, планирования деятельности, коммуникации с партнерами и клиентами, а также для контроля и анализа процессов. Существует ряд рисков, связанных с потерей или искажением информации, которые могут

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

серьезно подорвать эффективность бизнеса и привести к негативным последствиям.

В современном мире большинство компаний используют цифровые системы для хранения и передачи информации, и это создает уязвимости. Недостаточная защита от хакерских атак, ошибки в программном обеспечении или аппаратной части, а также неумышленные действия сотрудников – все это может привести к потере или искажению важной информации.

Неправильная передача информации является также важным риском, который необходимо учитывать. Например, при обмене данными между различными подразделениями компании или партнерами возникает вероятность искажения или утраты информации из-за недостаточной точности и своевременности передачи. Также важно помнить о риске человеческого фактора – неверная интерпретация информации может привести к неправильным решениям и действиям [13].

Потеря или искажение информации может иметь серьезные негативные последствия для бизнеса. Во-первых, это может привести к ухудшению качества принимаемых решений. Неправильная информация может ввести в заблуждение руководство компании или менеджмент, что приведет к убыткам и потере конкурентоспособности. Во-вторых, это может привести к проблемам с клиентами и партнерами. Неправильная информация может вызвать недовольство со стороны клиентов и партнеров, а также потерю доверия к компании. В-третьих, это может привести к проблемам с законодательством. Неправильная информация может привести к нарушению законов или нормативов, что повлечет за собой серьезные штрафы.

4. Риски связи. Связь играет важную роль в бизнесе, обеспечивая коммуникацию между сотрудниками, клиентами и поставщиками. Технические проблемы, такие как отключение сети, низкая скорость доступа в Интернет или сбои в работе телефонных линий могут привести к простоям в работе и потере

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

связи с клиентами и партнерами. Кроме того, существует риск утечки конфиденциальной информации при использовании ненадежных каналов связи.

Другим риском является недостаточная защита линий связи от внешних угроз, это могут быть кибератаки или вредоносные программы. Кража или утечка конфиденциальной информации может нанести серьезный ущерб репутации компании и клиентам.

5. Риски технических средств. Современный бизнес не может обойтись без использования технических средств. От компьютеров и программного обеспечения до оборудования для производства - все они несут в себе определенные риски, которые могут негативно сказаться на деятельности компании.

Все компании хранят и обрабатывают конфиденциальную информацию о своих клиентах, финансовых операциях, производственных процессах и т.д. Несоблюдение правил безопасности или уязвимости в системах могут привести к потере данных или кибератакам. Технические средства также могут стать объектом мошенничества и хищения [14, 15]. Например, компьютеры могут быть взломаны для получения доступа к конфиденциальной информации, а оборудование может быть похищено для перепродажи на черном рынке.

Существует и риск технических сбоев оборудования или программного обеспечения. Любые сбои в их работе могут привести к простоям и потере прибыли. Более того, неисправности оборудования могут привести к авариям и несчастным случаям на производстве.

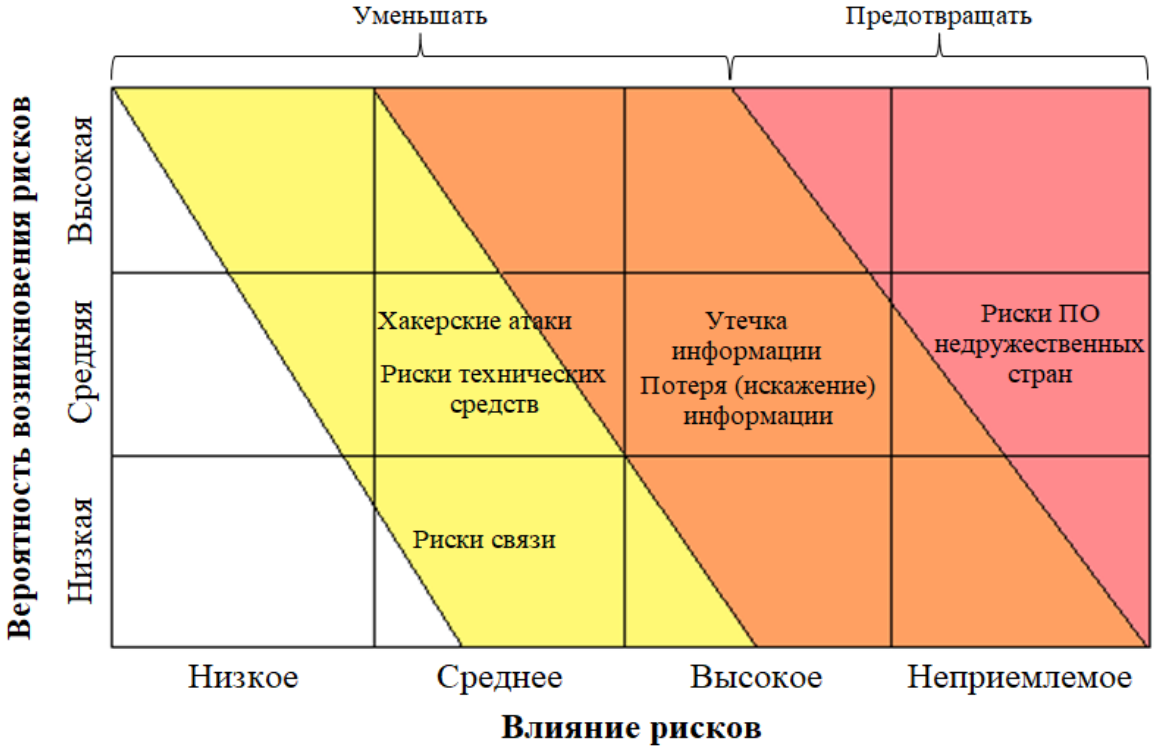
6. Риски программного обеспечения (ПО) недружественных стран. Во-первых, использование ПО недружественных стран может представлять угрозу для кибербезопасности. Возможность внедрения вредоносных программ или вирусов, разработанных в зарубежных странах, значительно выше, что может привести к утечкам конфиденциальной информации, взлому систем и другим серьезным последствиям для бизнеса.

Также следует учитывать риск технической зависимости от недружественных стран. В случае возникновения политических или

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

экономических конфликтов могут возникнуть проблемы с обновлениями ПО из этих стран, технической поддержкой и несоблюдением контрактных обязательств.

На рис. 7 представлены перечисленные выше типовые риски цифровой трансформации, которые расставлены на графике по степени влияния и вероятности их возникновения в условиях глобального цифрового развития.



Источник: составлено авторами

Рис. 7. Вероятность возникновения типовых рисков и степень их влияния

Стратегии управления рисками и способы их минимизации

Следующий этап систематизации рисков- это разработка мер по управлению рисками, поэтому далее будут предложены некоторые стратегии для минимизации рисков. Представленные риски бизнес-технологий могут привносить свои уникальные угрозы в бизнес-процессы. Для управления этими рисками предложены следующие меры.

1. Облачные технологии. Несмотря на вышеперечисленные риски, компании продолжают активно применять облачные технологии в своем бизнесе, так как преимущества перевешивают возможные угрозы. Для минимизации рисков при

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

выборе надежного облачного провайдера необходимо провести тщательный анализ, учитывать его репутацию, отзывы клиентов и наличие сертификатов, а также уровень безопасности. При использовании в работе облачных технологий важно регулярно обновлять политику безопасности для защиты данных, хранимых в облаке, и проводить регулярные аудиты безопасности, а также мониторинг доступа к облачным ресурсам [16]. Обеспечение безопасности данных в облаке является приоритетом для любой организации, и поэтому нужно принимать все необходимые меры для предотвращения утечек информации и других угроз.

2. Дистанционная работа. Рассмотрим способы минимизации рисков дистанционной работы. Обеспечение безопасности корпоративных данных во время дистанционной работы особенно важно, следовательно, необходимо, чтобы у сотрудников были установлены надежные средства удаленного доступа. Помимо этого, обучение сотрудников правилам безопасности при работе из дома становится обязательным шагом для защиты конфиденциальных данных компании. Важно также внедрить многофакторную аутентификацию, чтобы обеспечить дополнительный уровень защиты доступа к конфиденциальным данным и уменьшить риск несанкционированного доступа. Все эти меры объединяются в комплексный подход по обеспечению информационной безопасности и помогают минимизировать угрозы для бизнеса.

3. Искусственный интеллект. Эффективное управление рисками при использовании искусственного интеллекта в бизнесе - это меры по укреплению безопасности данных, обучению сотрудников работе с искусственным интеллектом и тщательному обоснованию принятия решений.

Для обеспечения безопасного и эффективного использования искусственного интеллекта в бизнесе необходимо внедрить регулярный мониторинг, обновление алгоритмов и моделей в работе, чтобы предотвратить непредсказуемые последствия. Также важно создать этические стандарты и правила для использования искусственного интеллекта, чтобы быть уверенным, что его применение соответствует нормам и ценностям общества.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

4. Цифровые платформы. Обеспечить безопасность цифровых платформ и их инфраструктуры могут регулярные проверки на предмет уязвимостей, что способствует их своевременному устранению. Минимизировать риск также поможет способ ограничивать доступ к информации в зависимости от роли пользователей на цифровой платформе, чтобы избежать утечек данных и несанкционированного доступа к конфиденциальной информации. Соблюдение всех мер безопасности поможет обеспечить надежное функционирование цифровых платформ и защитить их от возможных угроз [17].

5. Робототехника. Минимизировать риски робототехники помогут различные способы. Во-первых, регулярное обновление и обслуживание техники, а также периодическое обновление программного обеспечения и аппаратных компонентов помогут предотвратить неполадки и повысить эффективность работы системы. Важно также проводить профилактические работы. Во-вторых, обучение персонала правилам взаимодействия с техникой является неотъемлемой частью обеспечения безопасности. Работа с роботизированными системами требует соблюдения определенных протоколов и ограничений. Персонал должен быть грамотно обучен, чтобы предотвратить несчастные случаи и минимизировать риски возникновения травм. В-третьих, необходимо оценить возможные риски и разработать соответствующие меры предосторожности. Персонал должен знать, как правильно работать с техникой и как быстро реагировать на чрезвычайные ситуации [18].

6. Большие данные. Механизм шифрования является одним из способов минимизации рисков, он обеспечит надежную защиту конфиденциальных данных. В связи с растущим объемом информации, хранящейся в цифровом виде, необходимо предотвратить возможные утечки и несанкционированный доступ к этой информации.

Только механизмов шифрования недостаточно для полной безопасности данных. Вот почему необходимо внедрение систем мониторинга и контроля над доступом к большим данным. Эти системы будут отслеживать действия

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

пользователей, контролировать границы доступа и предоставлять информацию о любых незаконных или подозрительных действиях. Установленные системы мониторинга и контроля позволят оперативно реагировать на любые возможные угрозы и предотвращать несанкционированный доступ к конфиденциальным данным. Эти системы также позволят проанализировать типичные сценарии нарушения безопасности и разработать меры для их предотвращения.

7. Цифровой двойник. Перед использованием данной технологии необходимо разработать строгую политику защиты персональных данных. Эта политика должна включать в себя проверку и обновление технических механизмов защиты информации, чтобы обеспечить надежную защиту от утечек информации и несанкционированного доступа к данным.

Минимизировать риски также помогут современные технологии шифрования, многоуровневые системы аутентификации и регулярное обновление программного обеспечения. Для сотрудников компании необходимо проводить обучение с целью соблюдения мер безопасности.

8. Интернет вещей. Необходимо внедрить механизмы шифрования для обеспечения безопасности обмена данными между устройствами. Это позволит защитить информацию от несанкционированного доступа и обеспечит конфиденциальность передаваемых данных. Важно своевременно обновлять ПО и проводить аудит безопасности, чтобы обнаружить и устранить уязвимости, а также поддерживать высокий уровень защиты информации [19].

9. Блокчейн, криптовалюты. Формирование основных рисков, связанных с использованием блокчейна и криптовалют, позволит компании их минимизировать. Тщательное планирование и принятие мер предосторожности могут также помочь извлечь пользу из этих технологий. Одним из способов для обеспечения безопасности и надежности стоит считать внедрение системы мониторинга для контроля сделок и предотвращения мошенничества.

10. Чат-боты. Для уменьшения рисков, связанных с использованием чат-ботов в бизнесе, компании должны тщательно планировать и контролировать их

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

использование, например, проводить тщательный отбор партнеров по разработке и внедрению чат-ботов, а также проводить регулярное обновление и адаптацию программы к изменяющимся потребностям клиентов.

11. 3D-печать. Для успешной интеграции 3D-печати в бизнес необходимо уделить внимание безопасности, защите интеллектуальной собственности и экологической устойчивости. Внимательное обращение к этим аспектам может помочь компаниям избежать потенциальных проблем и получить максимальную выгоду от 3D-печати.

Перечисленные меры помогут управлять рисками технологий цифровой трансформации и тем самым способствовать увеличению безопасности компании, а также минимизации затрат на устранение последствий угроз. Теперь представим меры по управлению типовыми рисками цифровой трансформации в условиях глобального цифрового развития.

1. *Хакерские атаки.* Для минимизации рисков необходимо регулярное обновление и усиление мер безопасности сети, включая установку фаерволов, антивирусного программного обеспечения, систем обнаружения вторжения, регулярное обновление программного обеспечения и других средств защиты данных. Необходимо обучение сотрудников правилам безопасности информации, правилам обработки конфиденциальной информации и мерам предосторожности при общении по электронной почте.

2. *Утечка информации.* Чтобы избежать угроз утечки информации, нужно использовать средства мониторинга активности сети и обнаружения аномалий для своевременного обнаружения и предотвращения утечек информации. Необходимо внедрить строгую политику безопасности, обучать сотрудников правилам обращения с конфиденциальной информацией, использовать современные технологии защиты данных, а также проводить регулярные аудиты и проверки на предмет утечек [20].

3. *Потеря (искажение) информации.* Рассмотрим ряд мер, способных минимизировать риски потери или искажения информации. Во-первых,

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

необходимо усилить системы защиты информации, что включает в себя регулярную проверку систем на наличие уязвимостей, установку современных антивирусных и антихакерских программ. Во-вторых, компании должны разработать процедуры обмена и хранения информации, чтобы минимизировать риск неправильной передачи данных. В-третьих, необходимо уделить внимание обучению сотрудников: чем компетентнее и опытнее будут сотрудники, тем меньше рисков возникновения проблем с информацией.

4. *Риски связи.* Компании должны инвестировать в надежные и защищенные средства связи, такие как виртуальные частные сети, или использовать шифрование данных при передаче по открытым сетям. Также важно проводить регулярные аудиты безопасности и обучать сотрудников правильным методам использования линий связи.

Для снижения рисков, связанных с непредсказуемостью линий связи, компании могут использовать резервные каналы связи, такие как мобильные сети, или альтернативных провайдеров. Это поможет минимизировать простои в работе и обеспечить беспрерывную связь с клиентами и партнерами.

5. *Риски технических средств.* Для минимизации этих рисков необходимо проводить регулярное обновление и обслуживание технических средств, а также обучать персонал правилам безопасности и защиты информации. Также важно иметь запасные копии данных и план реагирования на возможные сбои и инциденты.

6. *Риски ПО недружественных стран.* Проведение тщательного анализа рисков при использовании ПО недружественных стран и оценка альтернативных вариантов являются важными шагами для обеспечения безопасности информационных систем. Разработка и внедрение строгих политик безопасности, включая контроль за использованием ПО и мониторинг возможных угроз, помогает предотвратить возможные кибератаки и утечки данных. Сотрудничество с компетентными специалистами в области кибербезопасности и защиты данных

также играет важную роль в обеспечении безопасного использования ПО недружественных стран и защите от возможных угроз.

Мониторинг и обновление стратегии управления рисками в области бизнес-технологий

Успех любого предприятия зависит от эффективного управления рисками, особенно в современном цифровом мире, где технологии играют ключевую роль в бизнесе. Мониторинг и обновление стратегии управления рисками в области бизнес-технологий становится все более актуальным для обеспечения безопасности и стабильности бизнес-процессов.

Управление рисками – это важный процесс, который направлен на идентификацию, оценку, анализ и управление рисками, касающимися проекта. Это помогает предотвратить непредвиденные проблемы и минимизировать их воздействие на временные, финансовые и качественные параметры [21].

Каждый член команды проекта имеет свою роль и свои обязанности. Успешное управление рисками состоит в эффективном планировании, раннем выявлении рисков и оперативном реагировании на них. Команда проекта должна работать совместно для минимизации последствий рисков и достижения целей проекта в срок и в рамках бюджета. На рис. 8 отображены задачи риск-менеджмента.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Источник: составлено авторами

Рис. 8. Задачи риск-менеджмента

Обновление стратегии управления рисками бизнес-технологий связано с изменениями в бизнес-модели компании, во внутренней и внешней среде, а также с появлением новых технологий и угроз. Необходимо постоянно анализировать ситуацию и вносить коррективы в стратегию управления рисками для обеспечения ее актуальности и эффективности.

Мониторинг рисков бизнес-технологий предполагает постоянное отслеживание и анализ потенциальных угроз, связанных с использованием технологий в деятельности компании. Это может быть утечка конфиденциальных данных, кибератаки, нарушения законодательства о защите персональных данных, сбои в работе систем и т.д. Понимание этих рисков позволяет принимать меры по их предотвращению и минимизации возможных ущербов.

Для успешного мониторинга и обновления стратегии управления рисками бизнес-технологий компания должна иметь компетентных специалистов в области информационной безопасности, использовать современные инструменты мониторинга и аналитики, уделять должное внимание обучению и осведомленности сотрудников о правилах безопасности.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Эффективный мониторинг и обновление стратегии управления рисками бизнес-технологий позволяют компании минимизировать угрозы, повысить уровень безопасности и защиты информации, улучшить операционную деятельность и защитить репутацию бренда. Поэтому данному процессу следует уделять должное внимание и выделять ресурсы для обеспечения успеха и стабильного развития бизнеса.

Заключение

В ходе исследования было выявлено, что глобальное цифровое развитие не только предоставляет огромные возможности, но и несет серьезные угрозы для бизнес-технологий. С одной стороны, новейшие технологии позволяют увеличить эффективность бизнес-процессов, улучшить сервисы для клиентов и выйти на новые рынки. С другой стороны, цифровое развитие увеличивает уязвимость компаний к кибератакам, изменениям в правовой сфере и нестабильности мировых рынков.

Для успешного развития бизнес-технологий в условиях глобального цифрового развития необходима систематизация рисков. Это позволит компаниям более осознанно подходить к формированию своей стратегии, прогнозировать возможные угрозы и принимать меры по их минимизации. Ключевым фактором в этом процессе является постоянное обновление знаний и навыков сотрудников, использование проверенных технологических решений и постоянный мониторинг ситуации на рынке.

Систематизация рисков развития бизнес-технологий играет ключевую роль в обеспечении устойчивости и успешности деятельности компаний в условиях глобального цифрового развития. Правильное управление рисками позволяет минимизировать потенциальные угрозы, обеспечить стабильность и рост бизнеса в долгосрочной перспективе.

Исследование также показало, что современные компании должны быть готовы к постоянным изменениям и быстро адаптироваться к новым условиям.

Гибкость, инновации и умение быстро принимать решения становятся все более важными качествами для успешного развития в условиях глобального цифрового рынка.

Таким образом, систематизация рисков развития бизнес-технологий является необходимым шагом для обеспечения устойчивого развития компаний. Понимание возможных угроз, правильное прогнозирование и принятие эффективных мер по их минимизации позволят компаниям выйти на новый уровень развития и обеспечить конкурентоспособность на рынке.

Список литературы

1. Кузовкова Т.А., Салютина Т.Ю. Методы комплексной оценки цифрового развития экономики и общества: учебное пособие. – М., 2022. - 118 с. ISBN 978-5-4497-1551-7.
2. Salutina T.Y., Platunina G.P., Frank I.A. Features of Risk Management of Digital and Infocommunication Development to Ensure a Unified Information Space of Companies in Modern Conditions // 2023 Intelligent Technologies and Electronic Devices in Vehicle and Road Transport Complex (TIRVED), 15-17 November 2023. Moscow, Russian Federation, 2023. - Pp. 1-4. DOI: 10.1109/TIRVED58506.2023.10332796.
3. Салютина Т.Ю., Васильева И.А. Исследование процессов трансформации и формирование основных бизнес-технологий цифровой экономики // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сб-к материалов (тезисов) 47-й Международной конференции. – М., 2021. - С. 31-35.
4. Бойченко И.В., Платунина Г.П., Кравченко Н.А., Степанова Д.В. Внедрение технологий искусственного интеллекта российскими компаниям // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сб-к материалов (тезисов) 51-й Международной конференции. – М., 2023. - С. 113-115.

5. Платунина Г.П. Совершенствование маркетинговых стратегий с помощью искусственного интеллекта // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сб-к материалов (тезисов) 51-й Международной конференции. – М., 2023. - С. 129-132.
6. Салютина Т.Ю., Васильева И.А. Тенденции развития и формирование цифровых платформ для применения в современной экономике на государственном уровне // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сб-к материалов (тезисов) 48-й Международной конференции. – М., 2021. - С. 38-41.
7. Франк И.А., Савина А.Д. Создание цифровых экосистем и их влияние на развитие малого и среднего предпринимательства // Технологии информационного общества: Сб-к трудов XVIII Международной отраслевой научно-технической конференции. – М., 2024. - С. 241-243.
8. Платунина Г.П., Васильева И.А. Автоматизации производственных процессов и новые возможности для бизнеса // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сб-к материалов (тезисов) 48-й Международной конференции. – М., 2021. - С. 57-61.
9. Косарев В. С. Нейронные сети в экономике и финансах: Монография / В.С. Косарев. – М.: Дело РАНХиГС, 2021. - 118 с.
10. Платунина Г.П., Васильева И.А. Криптовалюта: особенности и перспективы биткоин в условиях нестабильной экономической обстановки // Экономика и качество систем связи. - 2021. - № 1 (19). - С. 28-34.
11. Кузовкова Т.А., Салютина Т.Ю. Экономическая безопасность бизнеса в цифровой среде: Учебное пособие. – М.: Ай Пи Ар Медиа, 2023. - 128 с. - ISBN 978-5-4497-2278-2.
12. Григоренко Е.Р., Платунина Г.П., Васильева И.А. Создание государственных информационных систем и информационная безопасность персональных данных в условиях цифровой экономики // Технологии информационного общества: Сб-к трудов XV Международной отраслевой научно-технической

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

конференции «Технологии информационного общества». – М., 2021. С. 236-238.

13. Кузовкова Т.А., Салютина Т.Ю. Влияние нового технологического уклада на цифровую безопасность экономики // Методические вопросы преподавания инфокоммуникаций в высшей школе. - 2022. - Т. 11. - № 3. - С. 13-19.
14. Платунина Г.П., Васильева И.А. Экономическая безопасность и инвестиционная привлекательность предприятий: характер взаимосвязи и проблема оценки // Мобильный бизнес: перспективы развития и реализации систем радиосвязи в России и за рубежом: Сб-к материалов (тезисов) 47-й Международной конференции. – М., 2021. - С. 69-73.
15. Григоренко Е.Р., Платунина Г.П., Васильева И.А. Развитие информационной безопасности в рамках реализации государственной программы «Цифровая экономика» // Технологии информационного общества: Сб-к трудов XIV Международной отраслевой научно-технической конференции. – М., 2020. - С. 323-326.
16. Salutina T.Y., Kuzovkova T.A., Platunina G.P. Integrated Approach to Measuring Results and Managing the Process of Digital Transformation // 2023 International Conference on Engineering Management of Communication and Technology (EMCTECH), 16-18 October 2023. Vienna, Austria, 2023. – Pp. 1-8. DOI: 10.1109/EMCTECH58502.2023.10297008.
17. Salutina T.Y., Platunina G.P., Vasileva I.A. Transformation of Business Technologies into Digital Platforms and Evaluation of the Effectiveness of their Application // Proceedings of the 2021 IEEE International Conference «Quality Management, Transport and Information Security, Information Technologies», 2021 T and QM and IS 2021. Yaroslavl, 2021. - С. 888-892.
18. Platunina, G.P., Salutina, T.Y., Frank, I.A. Megatrends of Digital Engineering Technologies: Analysis of the Model of Integral Assessment of the State and Potential of Digital Development in the Conditions of the Fourth Industrial Revolution // 2023 Intelligent Technologies and Electronic Devices in Vehicle and

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Road Transport Complex (TIRVED), 2023: Conference Proceedings. - Moscow, Russian Federation, 2023. - Pp. 1-4. DOI: 10.1109/TIRVED58506.2023.10332570.

19. Ланских Ю.В. Управление IT-рисками: учебное пособие / Ю.В. Ланских, В.Г. Ланских, К.В. Родионов. - Киров: ВятГУ, 2022. - 80 с.
20. Григорьев В.К. Управление рисками информационных технологий: учебное пособие / В.К. Григорьев. – М.: РТУ МИРЭА, 2023. - 97 с. ISBN 978-5-7339-1687-3.
21. Дмитриева С.И. Управление рисками: учебное пособие / С.И. Дмитриева. – М.: СОЛОН-Пресс, 2022. - 104 с. ISBN 978-5-91359-523-2.

Online scientific journal «Age of Quality»
ISSN 2500-1841
info@agequal.ru

Systematization of business technology development risks in the context of global digital development

Salutina Tatyana Yuryevna,
Head of the Department of Digital Economics, Management and Business Technologies,
Moscow Technical University of Communications and Informatics,
111024, Russia, Moscow, 8A Aviamotornaya str.
t.i.saliutina@mtuci.ru

Frank Irina Alexandrovna,
Graduate student,
Moscow Technical University of Communications and Informatics,
111024, Russia, Moscow, 8A Aviamotornaya str.
i.a.vasileva@mtuci.ru

This article systematizes the main types of risks that arise in the process of digital development of business technologies. The potential threats associated with the development of digital technologies in the context of rapid digital progress are analyzed and methods and strategies for their management are considered. Attention is paid not only to technical risks, but also to socio-economic ones affecting business technologies in the context of global digital development. Practical recommendations on minimizing risks and increasing business sustainability in the context of digital transformation are offered.

Keywords: Business technologies; digital development; digital economy; technical risks; digital technologies; socio-economic risks; risk management.