Оглавление

Бизнес-риски:

Риск	Негативный эффект	Меры по предотвращению
Недостаточное финансирование	Урезание важных функциональных возможностей. Прекращение проекта	Составление детального бюджета проекта. Анализ чувствительности бюджета. Анализ чувствительности помогает оценить, как изменения в ключевых переменных (например, стоимости ресурсов, сроках проекта) могут повлиять на общий бюджет. Мониторинг и пересмотр бюджета. Разработка плана действия на случай недостаточного финансирования.
Изменение в бизнес-требованиях	Быстро меняющиеся бизнес-цели и требования могут привести к постоянным изменениям в проекте, увеличивая его стоимость и сроки реализации.	1. Идентификация потенциальных источников изменений. Это могут быть требования регулятора, изменение рыночных условий, новые бизнес-стратегии компании и т.д. 2. Оценка вероятности возникновения и возможное воздействие на проект каждого потенциального источника изменений. 3. Разработка стратегии управления изменениями, которая включает в себя процессы документирования и утверждения изменений, адаптацию плана проекта и бюджета, а также механизмы для минимизации влияния изменений на проект. 4. Применение гибкого планирования и адаптивных методологий. Гибкое планирование с итерационной разработкой и частыми пересмотрами позволяет вносить изменения с минимальными потерями. 5. Создание временных и финансовых резервов на случай необходимости внесения изменений.

Технические риски:

Риск	Негативный эффект	Меры по предотвращению
Сложность интеграции	Проблемы совместимости, задержки в передаче данных и потерю данных	1. Анализ существующей инфраструктуры и систем. 1.1. Инвентаризация существующих систем и технологий. Подробная документация всех существующих IT-систем, с которыми должна интегрироваться новая

		информационная система, включая их тех. характеристики, интерфейсы и используемые технологии. 1.2. Оценка степени совместимости. Анализ как легко новая система может быть интегрирована с каждой из существующих систем с технической точки зрения. 2. Понимание бизнес-процессов. 2.1. Анализ бизнес-процессов. Выявление и документирование ключевых бизнес-процессов, которые будут взаимодействовать с новой системой. Необходимо понять какие данные и функции должны быть интегрированы для поддержки этих бизнес-процессов. 2.2. Оценка изменений в процессах. Определите, какие изменения в бизнес-процессах потребуются для интеграции новой системы и как они повлияют на работу различных подразделений. 3. Анализ технических деталей интеграции 3.1. Оценка интерфейсов и API. Необходимо изучить интерфейсы и API, доступные для интеграции между новой и существующими системами, оцените их полноту, производительность и уровень поддержки. 3.2. Анализ данных и форматов. Необходимо оценить форматы данных, используемых в существующих системах, и их совместимость с новой системой, включая потребности по преобразованию данных.
Масштабируемость и производительность	Проблемы с масштабируемостью и производительностью могут привести к снижению скорости работы системы и ухудшению пользовательского опыта.	1. Определение требований к производительности и масштабируемости. 1.1. Анализ требований: определение ключевых требований к производительности и масштабируемости, исходя из бизнес-целей, объемов данных, ожидаемого числа пользователей и типичных сценариев использования. 1.2. Прогнозирование роста. Необходимо проанализировать ожидаемый рост и развитие системы в будущем. Необходимо оценить, как это повлияет на необходимые ресурсы, объемы данных и нагрузку на систему. 2. Моделирование и тестирование производительности.

		2.1. Тестирование нагрузки и стресс-тестирование. Использование специализированных инструментов для моделирования реальных и пиковых нагрузок на систему, помогает выявить узкие места в производительности и оценить способность системы масштабироваться. 2.2. Тестирование масштабируемости. Необходимо проверить, насколько легко систему можно масштабировать, добавляя аппаратные ресурсы или изменяя конфигурацию. Это включает в себя как вертикальное масштабирование, так и горизонтальное. 3. Анализ архитектуры системы. 3.1. Архитектурный обзор. Проведите анализ архитектуры системы с точки зрения производительности и масштабируемости. Оцените, предусмотрены ил в архитектуре механизмы для гибкого масштабирования и оптимизации производительности. 3.2. Оценка технологий и инструментов. Оцените использованные технологии, фреймворки и базы данных с точки зрения их влияния на производительность и масштабируемость системы. 4. Идентификация потенциальных узких мест. 4.1. Анализ производительности компонентов. Используйте инструменты мониторинга и профилирования для выявления узких мест в производительности, таких как медленные операции с базой данных, неэффективный код или недостаточная оптимизация запросов. 4.2. Оценка внешних зависимостей. Учитывайте риски, связанные с внешними сервисами и API, на которые опирается система, так как они также могут влиять на производительность и масштабируемость.
Безопасность данных и уязвимости	Нарушение безопасности данных, включая утечки конфиденциальной информации, атаки хакеров, вирусы и другие киберугрозы, могут нанести вред бизнесу и подорвать доверие клиентов.	1. Идентификация активов и их классификация. 1.1. Инвентаризация данных и активов. Определите и документируйте все активы системы, включая данные, программное обеспечение,

		аппаратное обеспечение и сетевую инфраструктуру. 1.2. Классификация данных. Классифицируйте данные по степени конфиденциальности и значимости для бизнеса, чтобы определить, какие данные требуют более высокого уровня защиты.
Несоответствие техническим требованиям и стандартам	Разработанная система может не соответствовать всем техническим требованиям, нормативным актам и стандартам, что может привести к доработкам, штрафам, задержкам в выпуске.	2. Оценка угроз и уязвимостей. 2.1. Анализ угроз. Идентифицируйте потенциальные угрозы безопасности, такие как вирусы, фишинг, хакерские атаки, внутренние угрозы, утечки данных и другие. 2.2. Оценка уязвимостей. Выявите уязвимости в системе, которые могут быть использованы для реализации угроз. Это может включать слабые пароли, необновленное программное обеспечение, ошибки в коде и недостатки конфигурации. 3. Анализ рисков. 3.1. Оценка вероятности и воздействия. Для каждой идентифицированной угрозы оцените вероятность ее реализации и потенциальное воздействие на организацию. Это поможет определить уровень риска для каждой угрозы. 3.2. Приоритизация рисков. Ранжируйте риски на основе их вероятности и воздействия, чтобы определить, на какие угрозы и уязвимости следует сосредоточить внимание в первую очередь. 4. Регулярное тестирование и мониторинг. 4.1. Проведение пентестов. Регулярно проводите пентесты (тестирование на проникновение) и аудиты безопасности для выявления новых уязвимостей и проверки эффективности контрольных мер. 4.2. Мониторинг и логирование. Настройте системы мониторинга и логирования событий безопасности для обнаружения и реагирования на инциденты в режиме реального времени.
Зависимость от сторонних поставщиков и технологий	Использование сторонних компонентов, таких как библиотек, фреймворков, облачных сервисов, может привести к рискам, связанным с обновлениями, отказом от поддержки, уязвимостями и изменениями в лицензировании.	1. Инвентаризация сторонних технологий. 1.1. Составление списка используемых сторонних технологий. Первым шагом является создание подробного списка всех сторонних компонентов, включая библиотеки, фреймворки, программное обеспечение как

		услугу (SaaS), платформы и API, которые используются в проекте. 1.2. Оценка критичности. Определите, насколько проект зависит от каждой сторонней технологии и какие компоненты являются критически важными для функционирования продукта. 2. Анализ рисков. 2.1. Уязвимости безопасности. Оцените риски безопасности, связанные с каждым компонентом. Учитывайте историю обнаруженных уязвимостей и реакцию провайдера на их устранение. 2.2. Надежность и доступность. Оцените риски, связанные с надежностью и доступностью сторонних услуг, включая вероятность простоев и их влияние на ваш проект. 2.3. Юридические и лицензионные риски. Анализируйте условия лицензирования и соблюдение прав интеллектуальной собственности, а также потенциальные ограничения на использование сторонних компонентов. 2.4. Совместимость и интеграция. Оцените риски, связанные с интеграцией сторонних технологий в вашу систему, включая возможные трудности при обновлениях или изменениях API. 2.5. Зависимость от поставщика. Рассмотрите риски, связанные с потенциальным изменением условий предоставления услуги, увеличением стоимости или прекращением поддержки. 3. Разработка стратегии снижения рисков. 3.1. Разнообразие поставщиков. Где это возможно, избегайте излишней зависимости от одного поставщика, рассмотрите альтернативы для критически важных компонентов. 3.2. Планы по обеспечению непрерывности бизнеса. Разработайте планы на случай сбоев или отказа сторонних технологий, включая резервное копирование данных и переключение на альтернативные решения. 3.3. Аудит и мониторинг безопасности. Регулярно проводите аудит безопасности и мониторинг уязвимостей в

		используемых сторонних компонентах. 3.4. Договорные обязательства. Убедитесь, что условия договоров с поставщиками сторонних технологий соответствуют вашим требованиям к безопасности, надежности и доступности.
Технологический долг	Компромиссы, сделанные в процессе разработки для экономии времени или средств, могут привести к накоплению технического долга, усложняющего будущие обновления и поддержку системы.	1. Аудит и документирование текущего технологического долга. 1.1. Анализ кода. Используйте инструменты статического анализа кода и ревью кода для выявления проблемных областей, включая «заплатки», дублирование кода и ненадежные конструкции. 1.2. Оценка архитектуры. Проведите обзор архитектуры системы, чтобы идентифицировать устаревшие технологии, зависимости и сложные для поддержки компоненты. 1.3. Проверка документации. Оцените полноту и актуальность технической документации, так как недостатки в документации могут усугублять технологический долг. 2. Оценка влияния на проект 2.1. Воздействие на производительность и надежность. Оцените, как технологический долг влияет на текущую производительность и надежность системы. 2.2. Воздействие на гибкость и масштабируемость. Оцените, насколько технологический долг ограничивает возможности дальнейшего развития и масштабирования системы. 2.3. Финансовые риски. Рассчитайте дополнительные затраты на поддержку и разработку, вызванные технологическим долгом, включая потенциальное увеличение стоимости владения системой. 3. Приоритизация и планирование устранения. 3.1. Приоритизация задач по устранению. Определите, какие аспекты технологического долга требуют немедленного внимания, исходя из их влияния на проект и бизнес-цели. 3.2. Разработка плана устранения. Составьте план действий по постепенному устранению технологического долга, включая рефакторинг кода, обновление технологий, улучшение документации и

		внедрение лучших практик разработки. 4. Принятие мер по предотвращению накопления технологического долга. 4.1. Внедрение стандартов кодирования и ревью кода. Установите строгие стандарты кодирования и регулярные процедуры ревью кода, чтобы минимизировать появление нового технологического долга. 4.2. Тестирование и контроль качества. Разработайте и поддерживайте комплексную систему автоматизированного тестирования, чтобы
Проблемы с обновлением и миграцией данных	Обновление системы и миграция данных могут сопровождаться техническими сложностями, потерей данных, несовместимостью форматов и простоями в работе системы.	1. Анализ текущей системы и данных 1.1. Понимание архитектуры и зависимостей. Оцените текущую архитектуру системы и ее компонентов, включая внешние зависимости и взаимодействие с другими системами. 1.2. Инвентаризация и классификация данных. Проведите детальный анализ и классификацию данных, которые будут мигрированы, чтобы определить их объем, структуру и чувствительность. 2. Оценка рисков обновления и миграции. 2.1. Совместимость системы. Изучите риски, связанные с обновлением компонентов системы и внешних зависимостей, и их совместимостью с новыми версиями. 2.2. Целостность и безопасность данных. Оцените риски потери данных, нарушения их целостности и безопасности в процессе миграции. 2.3. Производительность и доступность. Рассмотрите потенциальное влияние обновления и миграции на производительность системы и доступность сервисов для пользователей. 2.4. Планы тестирования. Разработайте стратегии тестирования для обновленной системы и мигрированных данных, чтобы минимизировать риски сбоев и ошибок. 3. Планирование и подготовка к миграции. 3.1. Разработка детального плана миграции: Составьте план миграции, включающий этапы, задачи, ответственных и временные рамки. 3.2. Подготовка инфраструктуры. Убедитесь, что целевая система и инфраструктура готовы к

		приему мигрируемых данных и обновленных компонентов. 3.3. Обеспечение резервного копирования: Сделайте полные резервные копии всех данных и компонентов системы перед началом миграции для возможности восстановления в случае необходимости. 4. Минимизация рисков и реализация миграции. 4.1. Поэтапная реализация. Рассмотрите возможность поэтапного внедрения обновлений и миграции данных для минимизации рисков и возможности отката на предыдущие версии при возникновении проблем. 4.2. Мониторинг и поддержка. Настройте процессы мониторинга и предоставьте поддержку пользователей во время и после процесса миграции для быстрого устранения возникающих проблем. 5. Тестирование и верификация 5.1. Проведение тестирования. Организуйте тщательное тестирование обновленной системы и мигрированных данных, включая функциональное, производительное, безопасности и приемочное тестирование. 5.2. Верификация данных. Убедитесь, что все данные были корректно мигрированы, и их целостность не нарушена.
Неопределенность технологического ландшафта	Быстро меняющиеся технологии могут сделать выбранное решение устаревшим или привести к появлению более эффективных и экономичных альтернатив после начала проекта.	1. Исследование текущего технологического ландшафта. 1.1. Мониторинг технологических трендов. Оставайтесь в курсе последних технологических трендов, нововведений и предсказаний отраслевых аналитиков. 1.2. Анализ конкурентов и рынка. Изучите, как конкуренты и другие игроки на рынке адаптируются к изменениям в технологическом ландшафте. 2. Оценка воздействия на вашу организацию. 2.1. Анализ восприимчивости. Определите, насколько ваша текущая технологическая стратегия и инфраструктура восприимчивы к изменениям в технологическом ландшафте. 2.2. Оценка влияния на бизнес-процессы. Рассмотрите, как потенциальные изменения могут повлиять на ключевые бизнес-

		процессы, продукты и услуги вашей организации. 3. Идентификация и оценка рисков. 3.1. Технологическое устаревание. Оцените риск того, что используемые технологии станут устаревшими, и как это повлияет на конкурентоспособность и операционную эффективность. 3.2. Зависимость от ключевых технологий. Определите риски, связанные с сильной зависимостью от определенных технологий или поставщиков. 3.3. Проблемы совместимости и интеграции. Оцените риски, связанные с интеграцией новых технологий в существующую инфраструктуру. 4. Разработка стратегии управления рисками. 4.1. Гибкость и адаптивность. Разработайте гибкую и адаптивную технологическую стратегию, которая позволит быстро реагировать на изменения. 4.2. Инвестиции в инновации. Рассмотрите возможность инвестирования в исследования и разработки для изучения новых технологий и поддержки инноваций. 4.3. Разнообразие технологий. Избегайте излишней зависимости от одной технологии или поставщика, используя разнообразие технологических решений. 5. Регулярный пересмотр и адаптация. 5.1. Непрерывное обучение: Стимулируйте непрерывное обучение и развитие навыков сотрудников, чтобы поддерживать актуальность их знаний и умений. 5.2. Регулярный пересмотр стратегии. Проводите регулярный пересмотр технологической стратегии и инфраструктуры для ее корректировки.