УДК 004.413.4
DOI

УПРАВЛЕНИЕ РИСКАМИ IT-ПРОЕКТОВ С ИСПОЛЬЗОВАНИЕМ ОТЕЧЕСТВЕННОЙ СИСТЕМЫ RISKGAP

Чусавитина Г. Н., Новикова Т. Б., Старков А. Н., Плотникова Е. Д.

Федеральное государственное бюджетное образовательное учреждение высшего образования «Магнитогорский государственный технический университет имени Г. И. Носова», Магнитогорск, Российская Федерация, e-mail: tglushenko_2184@mail.ru

Эффективное управление рисками является критическим фактором успеха IT-проектов, однако классические подходы требуют адаптации к динамичной среде веб-разработки и инструментальной поддержки для практического применения. Целью работы является повышение эффективности управления рисками IT-проектов за счет разработки и апробации методики, интегрирующей принципы международного и национального стандартов (PMBOK и ГОСТ Р ИСО 31000) с функционалом отечественной системы управления проектными рисками RiskGap. Методологическую основу исследования составили системный анализ, моделирование бизнес-процессов (BPMN) и кейс-стади. Для сбора и обработки данных применялись методы экспертных оценок, количественного анализа рисков (расчет EMV, ESI) и экономического анализа. В качестве инструментария использовалась отечественная система RiskGap. Разработанная методика управления рисками IT-проектов представляет комплексный, процессно-ориентированный подход, реализующий полный цикл управления рисками в цифровой среде RiskGap. Апробация методики в проекте «Разработка веб-приложения для предприятия общественного питания» позволила идентифицировать и оценить риски проекта, спланировать и реализовать мероприятия по их предотвращению и реагированию. Проведенный экономический анализ подтвердил, что реализованные мероприятия привели к значительному снижению потенциального ущерба и сокращению влияния рисков на сроки проекта, а затраты на управление рисками оказались экономически оправданными. Теоретическая и практическая значимость результатов заключается в создании адаптируемого, инструментально поддержанного подхода к управлению рисками, который может быть применен для повышения управляемости и устойчивости широкого спектра IT-проектов.

Ключевые слова: управление рисками, IT-проект, методология, цифровая платформа, RiskGap, автоматизация, экономический эффект

RISK MANAGEMENT OF IT PROJECTS WITH RUSSIAN RISKGAP SYSTEM

Chusavitina G. N., Novikova T. B., Starkov A. N., Plotnikova E. D.

Federal State Budgetary Educational Institution of Higher Education "Magnitogorsk State Technical University named after G. I. Nosov", Magnitogorsk, Russian Federation, e-mail: tglushenko_2184@mail.ru

Effective risk management is critical to the success of IT projects, but classic approaches require adaptation to a dynamic web development environment and instrumental support for practical application. The aim of the work is to increase the efficiency of risk management of IT projects by developing and approving a methodology that integrates the principles of international and national standards (PMBOK and GOST R ISO 31000) with the functionality of the domestic project risk management system RiskGap. The methodological basis of the study was system analysis, business process modeling (BPMN) and case studies. Methods of expert assessments, quantitative risk analysis (EMV calculation, ESI) and economic analysis were used for data collection and processing. The domestic RiskGap system was used as a toolkit. The developed risk management methodology for IT projects represents an integrated, process-oriented approach that implements a full risk management cycle in the RiskGap digital environment. Approbation of the methodology in the project "Development of a web application for a public catering enterprise" made it possible to identify and assess the risks of the project, plan and implement measures to prevent and respond to them. The economic analysis confirmed that the implemented measures led to a significant reduction in potential damage and a reduction in the impact of risks on the project timeline, and the costs of risk management were economically justified. The theoretical and practical significance of the results lies in the creation of an adaptable, instrumentally supported approach to risk management, which can be applied to increase the manageability and sustainability of a wide range of IT projects.

Keywords: risk management, IT-project, methodology, digital platform, RiskGap, automation, economic effect

Введение

Управление рисками играет ключевую роль в успешности любого проекта, поскольку оно позволяет минимизировать неопределенность и повысить вероятность достижения целей проекта в установленные сроки в рамках определенного бюджета и требований по качеству. Успешная реализация IT-проектов критически зависит от эффективного управления рисками, которые в цифровой сфере отличаются высокой динамичностью, технологической сложностью и зависимостью от внешних интеграций [1]. Согласно отраслевым исследованиям (например, Standish Group CHAOS Report), доля полностью успешных IT-

проектов остается низкой (около 31 %), а ключевыми причинами неудач называются слабое управление изменениями и недостаточное планирование рисков. Это формирует устойчивую научно-практическую проблему: необходимость адаптации классических подходов риск-менеджмента к специфике IT-проектов и их инструментальной поддержки специализированными цифровыми решениями. Управление рисками в IT-проектах является одной из центральных тем в современных исследованиях. Особенности цифровой среды, высокая степень неопределенности, гибкие методы разработки и зависимость от внешних поставщиков формируют специфическую конфигурацию рисков, требующую особых подходов к их идентификации, анализу и контролю. Анализ современных исследований показывает многоаспектность данной проблемы. Анализ трудов отечественных исследователей, затрагивающих как общие вопросы риск-менеджмента (А. В. Щербак [1], В. С. Николаенко [2]), так и его прикладные аспекты в конкретных методологиях (например, управление рисками в Scrum-проектах [3]), позволяет сделать сводный вывод. Несмотря на проработанность теоретических основ и отдельных методов, наблюдается дефицит целостных, инструментально поддержанных методик, которые могли бы быть гибко адаптированы под специфику современного IT-проекта (включая веб-разработку) и реализованы с помощью конкретной, в том числе отечественной, цифровой платформы. В исследовании О. Н. Ильиной изложены ключевые концепции зрелости проектного управления и системный подход к интеграции риск-менеджмента в организационные процессы [4, с. 15–24]. Особое внимание уделяется необходимости адаптации методик под специфические условия конкретной отрасли. Эту мысль поддерживает Н. В. Капустина, которая акцентирует внимание на развитии организаций на основе риск-менеджмента, раскрывая механизм стратегического подхода к идентификации и классификации рисков, а также предлагая практические инструменты мониторинга и оценки [5, с. 125–148; 6, с. 32]. Т. Ю. Серебрякова и О. Г. Гордеева рассматривают прикладные аспекты учета, анализа и контроля организационных рисков [7, с. 141–152]. Их подход, основанный на построении карт рисков и матриц вероятности и воздействия, позволяет структурировать потенциальные угрозы и использовать визуальные инструменты в управлении. Таким образом, Н. В. Капустина [5; 6], Т. Ю. Серебрякова и О. Г. Гордеева [7] развивают инструментарий для качественного анализа и визуализации рисков (матрицы, карты). В свою очередь, О. Г. Тихомирова подчеркивает значимость комплексной диагностики проектной среды, включая внешние и внутренние неопределенности, и предлагает системный подход к обеспечению устойчивости проекта [8, с. 260]. Особую ценность для IT-проектов представляет предложенная модель интеграции управления рисками в общий процесс проектного управления с акцентом на контроль ключевых параметров – времени, стоимости и качества. В работе V. Nikolaenko, A. Sidorov рассматривается, как повысить вероятность успешного завершения ИТ-проектов путем выявления источников 105 универсальных рисков, а также установления причинно-следственных связей между этими рисками [9]. Е. В. Маслова в своей работе рассматривает этапы жизненного цикла IT-сервиса как точки концентрации рисков и предлагает набор моделей для управления ими [10, с. 5–15]. В работах К. С. Мирзаянц, О. А. Воробьевой, О. Д. Головиной рассматривается управление рисками проекта при создании приложений в сети Интернет [11]. В работе С. А. Баркалова, А. В. Белоусова, Е. О. Пужановой рассматриваются основные подходы к управлению проектами ИТ-профиля в оперативном режиме, особенно при внесении корректировок в состав проектов, который несомненно имеет свои специфические особенности [12]. Исследования, фокусирующиеся на цифровых платформах (Е. Д. Плотникова, Г. Н. Чусавитина [13]), часто ограничиваются их обзором, не предлагая целостных методик применения.

Совокупный анализ исследований по теме позволяет нам сделать вывод о том, что, несмотря на развитую теоретическую базу, существует дефицит целостных методик, которые бы не только описывали процессы, но и детально регламентировали их применение с помощью конкретных цифровых инструментов, особенно отечественных, что актуально в условиях политики импортозамещения. Таким образом, научная проблема заключается в отсутствии адаптированной методики управления рисками для IT-проектов, которая бы сочетала строгость стандартов (PMBoK, ГОСТ Р ИСО 31000) с практической реализуемостью в отечественной цифровой среде.

Цель исследования – повышение эффективности управления рисками IT-проектов за счет разработки и апробации методики, интегрирующей принципы стандарта PMBoK с функциональными возможностями отечественной системы RiskGap.

Выделим задачи исследования:

1. Проанализировать современные подходы и выявить потребность в автоматизации управления рисками IT-проектов.

2. Разработать методику управления рисками IT-проектов, включающую процессную модель, шаблон реестра и алгоритмы оценки.

3. Апробировать методику на реальном проекте веб-разработки, реализовав полный цикл управления рисками в системе RiskGap.

4. Дать количественную оценку экономического эффекта от внедрения методики на основе расчета предотвращенного ущерба и индекса эффективности затрат.

Материалы и методы исследования

Методологическую основу исследования составили принципы стандартов PMBOK Guide и ГОСТ Р ИСО 31000 [14; 15], обеспечивающие комплексный подход к управлению проектами и рисками. В качестве ключевого инструмента использовалась отечественная система управления рисками RiskGap (реестровый номер № 5502), которая предоставляет функциональные модули для идентификации, оценки, планирования реагирования и мониторинга рисков, применяется для систематизации процесса риск-менеджмента и обеспечения его прозрачности. Система выбрана по результатам сравнительного анализа как наиболее сбалансированное решение, поддерживающее необходимые методологии и обладающее удобным интерфейсом для IT-проектов [13].

В работе применялся следующий комплекс методов:

1. Системный анализ. Использован для изучения нормативной базы, проектной документации и научной литературы с целью формирования требований к методике.

2. Моделирование бизнес-процессов (в нотации BPMN). Применено для визуализации и формализации разработанной методики управления рисками, что обеспечило четкое описание последовательности действий, ролей и артефактов.

3. Метод экспертных оценок. Использован на этапах идентификации и качественного анализа рисков в рамках проектной команды. Вероятность (P) и влияние (I) рисков оценивались по 10-балльной шкале, согласованной экспертами.

4. Количественный анализ рисков. Реализован с применением формулы ожидаемой денежной стоимости (Expected Monetary Value, EMV) для оценки потенциального ущерба и анализа влияния на сроки (Expected Schedule Impact, ESI). Расчеты выполнялись как вручную, так и с использованием функционала RiskGap.

5. Кейс-стади (case study). Применен для комплексной апробации разработанной методики в условиях реального IT-проекта «Разработка веб-приложения для предприятия общественного питания» (бюджет 530 тыс. руб., срок 6 мес.).

6. Экономический анализ. Использован для расчета затрат на управление рисками (RRC), индекса эффективности затрат (CPI) и оценки предотвращенного ущерба, что позволило доказать экономическую целесообразность применения методики.

Методика управления рисками IT-проектов с использованием системы RiskGap

Методика управления рисками IT-проектов с использованием системы RiskGap – это комплексный, процессно-ориентированный подход, интегрирующий этапы управления рисками по стандарту PMBOK (от планирования до мониторинга) в цифровую среду специализированной отечественной платформы RiskGap. Методика управления рисками IT-проектов реализует полный цикл управления рисками, состоящий из семи взаимосвязанных этапов, визуализированных в нотации BPMN (рис. 1). Данная модель служит пошаговым руководством для проектной команды.

Методика включает следующие взаимосвязанные этапы-процессы:

1. Планирование управления рисками. Начальный этап, на котором в RiskGap создается карточка проекта, определяются роли (риск-менеджер, ответственные исполнители), устанавливаются регламенты, критерии оценки (шкалы вероятности и воздействия) и правила отчетности.

2. Идентификация рисков. Систематическое выявление угроз с использованием шаблонов, мозгового штурма, анализа документации и интервью. Результат фиксируется в цифровом реестре рисков.

3. Качественный анализ рисков. Первичная приоритизация. Каждому риску в карточке RiskGap вручную присваиваются значения: первое, вероятность (P) от 1 (почти невозможно) до 10 (практически неизбежно); второе, влияние (I) от 1 (незначительное) до 10 (критическое). Система автоматически рассчитывает уровень риска ($R = P \times I$) и относит его к зоне: зеленая (1–20), желтая (21–40), красная (41–100).

4. Количественный анализ рисков. Для рисков в «красной» зоне выполняется оценка в денежном и временном выражении (потенциальный ущерб в тыс. руб., влияние на сроки в днях). Это основа для расчета ожидаемой денежной стоимости (EMV) и формирования резервов.

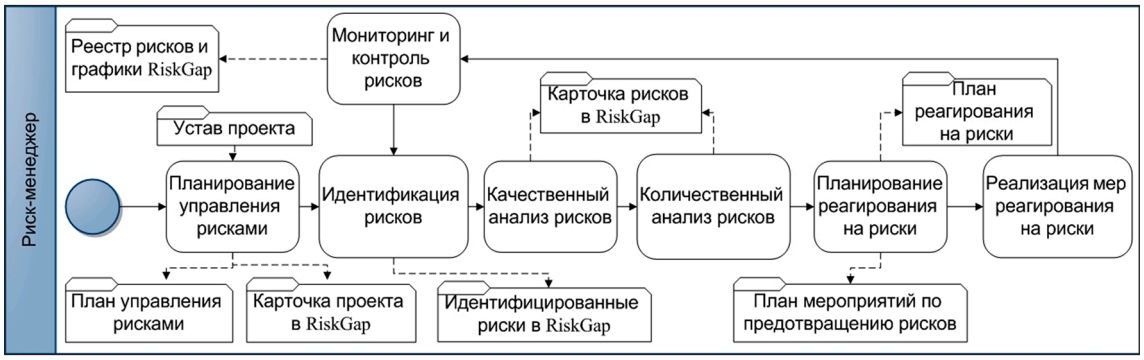


Рис. 1. Планирование управления рисками IT-проектов с использованием системы RiskGap в нотации BPMN
Примечание: составлен авторами по результатам данного исследования

5. Планирование реагирования на риски. Для каждого риска выбирается и детализируется стратегия: для угроз – Уклонение, Снижение, Передача, Принятие; для возможностей – Использование, Повышение, Совместное использование.

В RiskGap создаются конкретные задачи-мероприятия с указанием ответственных, сроков и бюджета, которые привязываются к карточке риска.

6. Реализация мер реагирования на риски. Оперативное выполнение запланированных мероприятий. RiskGap используется для контроля статуса задач, фиксации фактических дат и затрат.

7. Мониторинг и контроль рисков. Непрерывный процесс. Система предоставляет дашборды для отслеживания динамики уровня рисков, актуализации реестра, выявления новых угроз и формирования отчетов.

В ходе работы был разработан и интегрирован в RiskGap универсальный шаблон реестра рисков, адаптированный для проектов создания сайтов и веб-приложений. Шаблон структурирует риски по четырем категориям, что ускоряет процесс их идентификации:

− проектные (непостоянство требований, недооценка трудозатрат);

− организационные (уход ключевого сотрудника, коммуникационные сбои);

− технические (низкое качество кода, ошибки архитектуры, уязвимости безопасности);

− внешние (нестабильность интеграций с API, изменения в законодательстве).

Для каждого типового риска в шаблоне предопределены возможные причины, последствия и рекомендуемые стратегии реагирования, что минимизирует вероятность пропуска значимых угроз. Например, для риска «Нестабильность интеграции с платежной системой» (категория: внешние) шаблоном предусмотрены стратегия «Передача» и типовые мероприятия: внедрение механизмов повторных попыток, логирование транзакций, тестирование интеграции. Шаблон предназначен для применения в аналогичных проектах и может быть масштабирован в корпоративной практике.

Метод экспертных оценок был ключевым инструментом на этапах идентификации и качественного анализа рисков. В оценке участвовали семь ключевых специалистов проекта, обладающих необходимыми компетенциями: руководитель проекта (риск-менеджер), бизнес-аналитик, системный архитектор, ведущие frontend- и backend-разработчики, тестировщик и представитель заказчика. Метод был реализован в форме структурированных рабочих сессий (мозговых штурмов) на начальной фазе проекта. Для каждого из выявленных рисков эксперты коллегиально обсуждали и присваивали два параметра по утвержденной шкале: Вероятность (P) от 1 (почти невозможно) до 10 (практически неизбежно) и Влияние (I) от 1 (незначительное) до 10 (критическое). Оценки фиксировались непосредственно в карточках рисков в системе RiskGap.

Целью опроса была первичная приоритизация рисков для концентрации ресурсов на наиболее значимых угрозах. Результатом стали согласованные экспертные значения P и I для всех 27 рисков проекта, которые легли в основу расчета их интегрального уровня ($R = P \times I$) и построения матрицы приоритетов. Это позволило объективно выделить риски «красной» зоны (R = 41–100), требующие обязательного планирования реагирования.

На этапе планирования мер реагирования для каждого риска разрабатывается и фиксируется в RiskGap стратегия управ-

ления, определяющая общий подход к работе с угрозой [14]:

– уклонение – полное изменение плана проекта для устранения условия возникновения риска (например, отказ от использования непроверенной технологии);

– снижение – действия по уменьшению вероятности наступления риска или смягчению его последствий (например, внедрение дополнительного тестирования);

– передача – перекладывание ответственности за риск и его последствия на третью сторону (например, через страхование или фиксированную цену в договоре с подрядчиком);

– принятие – осознанное согласие с риском без активных действий, обычно при низком уровне угрозы или если затраты на реагирование превышают потенциальный ущерб. При этом формируется план на случай реализации риска.

Для позитивных рисков (возможностей) стратегии носят симметричный характер (использование, повышение, передача, принятие). В рамках проекта «Разработка веб-приложения для предприятия общественного питания» фокус был сделан на стратегии снижения (для большинства технических и проектных рисков) и принятия (для части маловероятных внешних рисков). Методика предусматривает использование следующих встроенных в RiskGap инструментов для анализа:

– матрица вероятности и воздействия для автоматического построения тепловой карты, на которой риски визуально распределены по зонам критичности, что позволяет мгновенно идентифицировать приоритеты;

– расчетные показатели:

• EMV (Expected Monetary Value) – оценка потенциального финансового ущерба по проекту. Расчет выполняется по формуле

$$EMV_{П} = \sum_{i=1}^{n=1} \frac{P_i}{10} \times C_i,$$

где C_i – потенциальные потери по i-му риску;

• ESI (Expected Schedule Impact) – оценка совокупного влияния рисков на сроки проекта:

$$ESI = \sum_{i=1}^{n} \frac{P_i}{10} \times D_i,$$

где D_i – потенциальная задержка по i-му риску;

– графики и дашборды для отображения динамики изменения уровня рисков, распределения ответственности в команде и влияния рисков на бюджет и критический путь.

Методика предусматривает четкое распределение обязанностей между участниками проекта внутри RiskGap:

– риск-менеджер / руководитель проекта – инициатор процесса, ответственный за общее планирование, мониторинг и отчетность;

– бизнес-аналитик, архитектор, технические специалисты – участники идентификации и экспертной оценки рисков в своей области;

– ответственные исполнители – члены команды, которым в системе назначаются конкретные задачи по реагированию на риски.

Таким образом, методика представляет собой не просто перечень этапов, а целостную систему – от теоретических основ через формализованную процессную модель к практической реализации в конкретном программном продукте (RiskGap) с готовыми артефактами (шаблон реестра, критерии оценки). Это обеспечивает ее воспроизводимость и адаптируемость для различных IT-проектов.

Результаты исследования и их обсуждение

Авторами разработана методика управления рисками ИТ-проектов с использованием системы RiskGap (ориентирована на ГОСТ и ISO 31000, элементы PMBoK), включающая в себя этапы управления рисками, структуру реестра рисков, критерии оценки, стратегии реагирования, роли и ответственность. В ходе работы был создан шаблон реестра рисков для проектов веб-разработки, включающий типовые угрозы, рекомендуемые стратегии и критерии оценки. Шаблон предназначен для применения в аналогичных проектах и может быть масштабирован в корпоративной практике.

Разработанная методика управления рисками была апробирована в проекте «Разработка веб-приложения для предприятия общественного питания». В системе RiskGap был создан и настроен проект с учетом его ограничений (бюджет 530 тыс. руб., срок 6 мес.) и определен состав команды (8 чел.). В рамках реализации определена цель риск-менеджмента – минимизация влияния рисков на сроки, бюджет и качество проекта; сформирована команда, распределены роли, в системе RiskGap был создан и задокументирован «План управления рисками проекта», включающий формализованные цели, критерии оценки и распределение ролей. Его оперативную часть составляет график выполнения процессов управления рисками, ключевые этапы которого представлены в табл. 1.

Таблица 1

График ключевых процессов управления рисками в проекте

№	Наименование и содержание задачи	Начало	Окончание	Ответственный
1	Планирование управления рисками Утверждение подходов, ролей, критериев	11.11.2024	16.11.2024	Риск-менеджер
2	Идентификация рисков	17.11.2024	29.11.2024	Бизнес-аналитик
3	Проведение мозгового штурма	02.12.2024	03.12.2024	Вся проектная команда
4	Передача результатов штурма на экспертную оценку	04.12.2024	05.12.2024	Риск-менеджер
5	Построение причинно-следственных диаграмм	06.12.2024	09.12.2024	Системный архитектор
6	Формирование реестра рисков	10.12.2024	11.12.2024	Бизнес-аналитик
7	Качественный анализ и оценка рисков (экспертная оценка P и I)	12.12.2024	16.12.2024	Бизнес-аналитик, риск-менеджер
8	Построение матрицы вероятности и последствий	17.12.2024	18.12.2024	Бизнес-аналитик
9	Обновление реестра рисков	19.12.2024	20.12.2024	Бизнес-аналитик
10	Количественный анализ рисков (расчет EMV, анализ влияния на сроки)	23.12.2024	25.12.2024	Риск-менеджер
11	Проведение анализа ожидаемой денежной стоимости проекта	26.12.2024	27.12.2024	Риск-менеджер
12	Планирование мероприятий по реагированию на риски	06.01.2025	09.01.2025	Риск-менеджер, Backend-разработчик
13	Обновление реестра рисков	10.01.2025	10.01.2025	Бизнес-аналитик
14	Описание мероприятий по снижению рисков (внедрение мер)	13.01.2025	17.01.2025	Все исполнители по категориям
15	Регулярный мониторинг и контроль рисков (еженедельно)	29.11.2025	10.05.2025	Риск-менеджер

Примечание: составлена авторами на основе полученных данных в ходе исследования.

Таблица 2

Фрагмент шаблона реестра рисков IT-проектов в системе RiskGap

Название риска	Описание шаблона риска
Потеря доступа к внешним сервисам	Временная или длительная недоступность сторонних сервисов (например, API или облачные платформы), используемых в проекте, приводит к нарушению функциональности продукта, задержкам в выполнении задач и снижению качества обслуживания пользователей. Потеря доступа может быть вызвана техническими сбоями, изменениями в политике провайдера или блокировками, что увеличивает риски простоев и требует разработки альтернативных решений и стратегий резервирования
Утечка данных	Несанкционированный доступ, потеря или раскрытие конфиденциальной информации, включая персональные данные пользователей, коммерческие тайны и внутренние документы, приводит к репутационным потерям, юридическим санкциям и финансовым штрафам. А также утечка данных негативно влияет на доверие пользователей и клиентов, что может привести к снижению лояльности, оттоку аудитории и ухудшению имиджа компании на рынке
Задержка внешнего подрядчика	Несоблюдение подрядчиками или поставщиками согласованных сроков выполнения работ или поставки ресурсов приводит к задержкам в общем графике проекта. Это может вызвать каскадное смещение сроков, увеличить нагрузку на команду и повысить риски срывов релизов

Примечание: составлена авторами на основе полученных данных в ходе исследования

Конкретные мероприятия по реагированию для каждого приоритетного риска были детализированы в виде задач в системе RiskGap с назначением ответственных, сроков и оценкой затрат. Механизмом контроля был установлен регулярный (еженедельный) мониторинг статуса рисков и выполнения задач через дашборды RiskGap с последующим обсуждением на плановых проектных совещаниях.

В качестве основы для идентификации использовался разработанный типовой шаблон реестра рисков для веб-приложений, реализованный в системе RiskGap, который представлен в табл. 2. Его применение позволило систематизировать процесс выявления угроз и сформировать первоначальный реестр, который затем был дополнен и адаптирован под специфику проекта.

На этапе идентификации, с использованием разработанного шаблона и в ходе экспертных сессий, в системе RiskGap был сформирован реестр для предприятия общественного питания (рис. 2), включающий 27 рисков, классифицированных по четырем категориям проектные – 7, организационные – 4, технические – 12, внешние – 4.

Наполнение реестра было обосновано комплексным анализом специфики проекта, включающим:

1. Анализ проектной документации и требований. Выполнено изучение технического задания, пользовательских сценариев (онлайн-заказ, доставка, бонусная система), в рамках которого были выявлены риски, связанные с функционалом (например, WEB-06 «Некорректные расчеты параметров доставки», WEB-13 «Ошибки в алгоритме начисления бонусов за заказ»).

2. Экспертные интервью и мозговой штурм с командой, в рамках которых были проведены сессии с архитекторами, разработчиками и тестировщиками, что позволило выявить технические риски (WEB-12 «Низкое качество кода сервиса Cart (корзина)», WEB-19 «Низкая производительность фронтенда»), а также организационные (WEB-09 «Перегрузка сотрудников», WEB-11 «Недостаточная коммуникация»).

3. Анализ внешних зависимостей. Выявление критически важных интеграций (платежи, геолокация, онлайн-касса) определило группу внешних рисков (WEB-24 «Сбой определения адреса с помощью геолокационного сервиса», WEB-25 «Нестабильность функционирования онлайн-кассы», WEB-26 «Нестабильность интеграции с внешней платеж-ной системой»).

4. Использование типового шаблона. В качестве основы применялся разработанный в рамках методики шаблон реестра рисков для веб-разработки, что обеспечило полноту охвата стандартных для отрасли угроз (напр., WEB-17 «Уязвимость XSS/CSRF», WEB-22 «Истечение срока действия TLS/SSL-сертификата»).

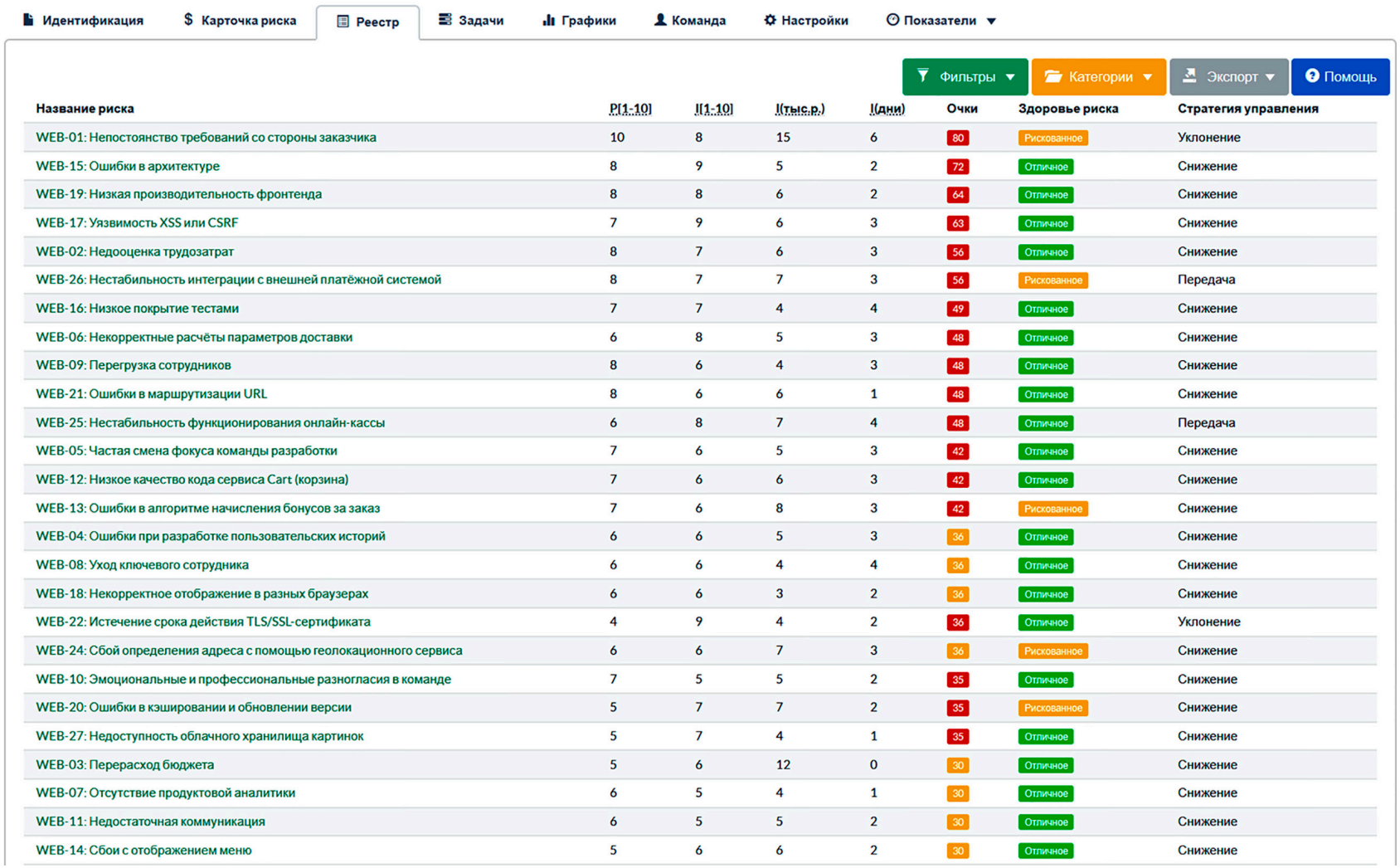
Таким образом, каждая из четырех категорий реестра (проектные, организационные, технические, внешние) наполнена конкретными рисками, логично вытекающими из целей, архитектуры и среды реализации проекта «Разработка web-приложения для предприятия общественного питания». Для каждого риска в карточке зафиксированы: описание, причины возникновения, потенциальные последствия, текущий статус и т. д. На рис. 3 представлена карточка риска «Непостоянство требований со стороны заказчика» в RiskGap.

С использованием встроенных инструментов RiskGap была проведена качественная и количественная оценка рисков. Применялась 10-балльная шкала для вероятности и ущерба, а итоговый уровень риска рассчитывался как произведение этих показателей. Все риски с высоким уровнем были включены в оперативное реагирование с обязательным контролем исполнения мероприятий.

На этапе планирования реагирования на риски для каждого приоритетного риска в системе RiskGap были определены конкретные мероприятия с указанием ответственных и сроков. Например, для риска WEB-01 «Непостоянство требований заказчика» ключевым мероприятием стало «Внедрение регламента управления изменениями требований» (ответственный: бизнес-аналитик). Для риска WEB-26 «Нестабильность интеграции с платежной системой» было запланировано мероприятие «Разработка промежуточного слоя абстракции для интеграции с платежным шлюзом» (ответственный: backend-разработчик).

Сформированы задачи на предотвращение рисков и стратегии реагирования: снижение, избежание, передача, принятие. Назначены мероприятия, сроки и ответственные лица в системе RiskGap. Фрагмент разработанного плана мероприятий по предотвращению рисков и плана реагирования на риски в случае их возникновения представлен на рис. 4.

Выбор запланированных мероприятий непосредственно вытекал из результатов качественного и количественного анализа рисков. Для каждого риска в «красной» и «желтой» зонах мероприятия разрабатывались с учетом его причины, категории и выбранной стратегии реагирования.



Название риска	P[1-10]	I[1-10]	I(тыс.р.)	I(дни)	Очки	Здоровье риска	Стратегия управления
WEB-01: Непостоянство требований со стороны заказчика	10	8	15	6	80	Рискованное	Уклонение
WEB-15: Ошибки в архитектуре	8	9	5	2	72	Отличное	Снижение
WEB-19: Низкая производительность фронтенда	8	8	6	2	64	Отличное	Снижение
WEB-17: Уязвимость XSS или CSRF	7	9	6	3	63	Отличное	Снижение
WEB-02: Недооценка трудозатрат	8	7	6	3	56	Отличное	Снижение
WEB-26: Нестабильность интеграции с внешней платёжной системой	8	7	7	3	56	Рискованное	Передача
WEB-16: Низкое покрытие тестами	7	7	4	4	49	Отличное	Снижение
WEB-06: Некорректные расчёты параметров доставки	6	8	5	3	48	Отличное	Снижение
WEB-09: Перегрузка сотрудников	8	6	4	3	48	Отличное	Снижение
WEB-21: Ошибки в маршрутизации URL	8	6	6	1	48	Отличное	Снижение
WEB-25: Нестабильность функционирования онлайн-кассы	6	8	7	4	48	Отличное	Передача
WEB-05: Частая смена фокуса команды разработки	7	6	5	3	42	Отличное	Снижение
WEB-12: Низкое качество кода сервиса Cart (корзина)	7	6	6	3	42	Отличное	Снижение
WEB-13: Ошибки в алгоритме начисления бонусов за заказ	7	6	8	3	42	Рискованное	Снижение
WEB-04: Ошибки при разработке пользовательских историй	6	6	5	3	36	Отличное	Снижение
WEB-08: Уход ключевого сотрудника	6	6	4	4	36	Отличное	Снижение
WEB-18: Некорректное отображение в разных браузерах	6	6	3	2	36	Отличное	Снижение
WEB-22: Истечение срока действия TLS/SSL-сертификата	4	9	4	2	36	Отличное	Уклонение
WEB-24: Сбой определения адреса с помощью геолокационного сервиса	6	6	7	3	36	Рискованное	Снижение
WEB-10: Эмоциональные и профессиональные разногласия в команде	7	5	5	2	35	Отличное	Снижение
WEB-20: Ошибки в кэшировании и обновлении версии	5	7	7	2	35	Рискованное	Снижение
WEB-27: Недоступность облачного хранилища картинок	5	7	4	1	35	Отличное	Снижение
WEB-03: Перерасход бюджета	5	6	12	0	30	Отличное	Снижение
WEB-07: Отсутствие продуктовой аналитики	6	5	4	1	30	Отличное	Снижение
WEB-11: Недостаточная коммуникация	6	5	5	2	30	Отличное	Снижение
WEB-14: Сбои с отображением меню	5	6	6	2	30	Отличное	Снижение

Рис. 2. Фрагмент реестра рисков проекта в системе RiskGap
Примечание: составлен авторами по результатам данного исследования

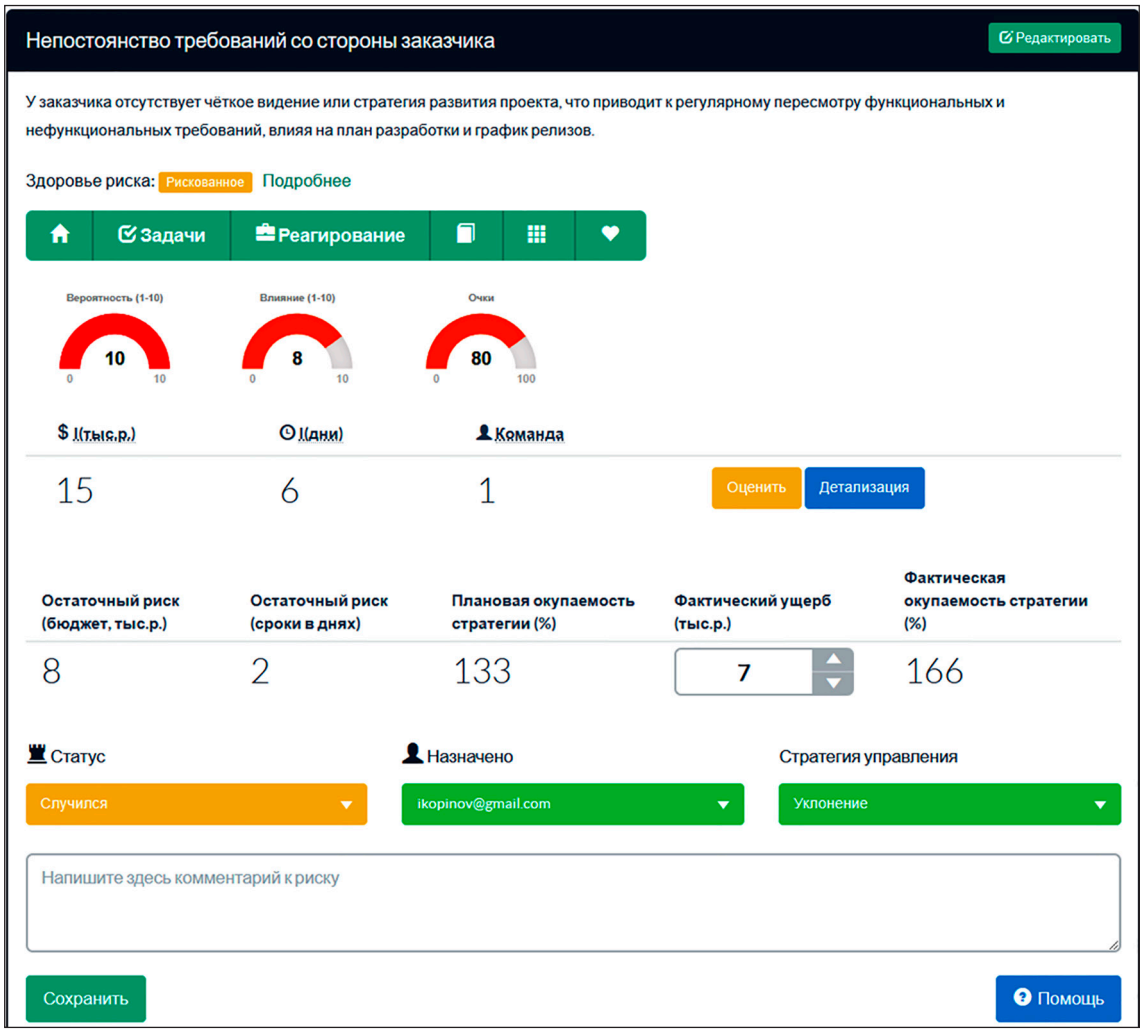


Рис. 3. Карточка риска «Непостоянство требований со стороны заказчика»
Примечание: составлен авторами по результатам данного исследования

Название задачи	Назначена	Срок исполнения	Статус	Риск	Здоровье задачи
Регулярный аудит безопасности, внедрение защитных механизмов, обучение разработчиков	iograt@yandex.ru	22 апр.	Выполнена	Уязвимость XSS или CSRF	Отличное
Проведение тестирования расчётов, внедрение продуктовой аналитики, регулярные проверки корректности параметров	Данил	02 февр.	Выполнена	Некорректные расчеты параметров доставки	Отличное
Резервирование, локальное кэширование	fadeevtim@dcpa.net	10 мая	Выполнена	Недоступность облачного хранилища картинок	Отличное
Мониторинг состояния оборудования, тесное взаимодействие с технической поддержкой онлайн-кассы	Данил	27 марта	Отменена	Нестабильность функционирования онлайн-кассы	Отличное

Рис. 4. Фрагмент плана мероприятий по предотвращению и реагированию на риски проекта
Примечание: составлен авторами по результатам данного исследования

Рис. 5. Матрица влияния рисков на бюджет проекта
Примечание: составлен авторами по результатам данного исследования

Таким образом, каждое мероприятие в плане является адресным ответом на конкретную характеристику риска (его корневую причину, оцененное воздействие и вероятность), что обеспечивает целенаправленное использование ресурсов проекта на управление наиболее значимыми угрозами.

Бюджетирование мероприятий показало, что прямые затраты на меры предотвращения составили 21 тыс. руб., а на меры реагирования – 6 тыс. руб. Эти средства были распределены по мероприятиям, привязанным к приоритетным рискам в системе RiskGap. Для контроля за состоянием рисков в системе RiskGap использована матрица рисков, представленная на рис. 5, которая способствует оперативному отслеживанию изменений и приоритизации действий. Каждая точка на матрице соответствует конкретному риску, цветовая кодировка (зеленый, желтый, красный) отражает степень опасности, что облегчает восприятие информации и планирование мероприятий.

Мониторинг осуществлялся еженедельно с помощью дашбордов RiskGap. По итогам проекта 14 рисков (52 %) были предотвращены, 5 (18 %) реализовались, 8 (30 %) закрыты как неактуальные. Ни один из реализовавшихся рисков не привел к критическим отклонениям по срокам или бюджету.

На следующем этапе был произведен расчет экономического эффекта от использования разработанной авторами методики в проекте «Разработка web-приложения для предприятия общественного питания».

Методика расчета экономического эффекта основывалась на сопоставлении потенциальных и фактических потерь, а также затрат на управление рисками. Исходные данные для расчетов были получены в ходе выполнения проекта и зафиксированы в системе RiskGap: вероятность (P) и потенциальные потери (C) для каждого риска – из карточек реестра после этапа экспертной оценки; бюджеты мероприятий по реагированию – из планов мероприятий, созданных в RiskGap; фактические потери – из отчетов о реализации рисков; трудозатраты команды и стоимость лицензий – по данным учета рабочего времени и договорным условиям.

Расчет выполнен на основе данных RiskGap и показал следующее:

1. Суммарная оценка всех потенциальных убытков от рисков – Expected Monetary Value ($EMV_{п}$), отражающая средний объем убытков, которые проект может понести при наступлении конкретного риска, составил 107,1 тыс. руб.

2. Фактический ущерб от реализовавшихся рисков (*EMVфакт*): 26 тыс. руб. (5 рисков, включая WEB-01 и WEB-26).

3. Затраты на управление рисками (RRC) включали прямые затраты на мероприятия (27 тыс. руб.), непрямые трудозатраты команды (15,18 тыс. руб.), лицензии RiskGap (8 тыс. руб.) и резерв (10,6 тыс. руб.). Итого: 60,78 тыс. руб.

4. Ключевые показатели эффективности:

− Предотвращенный ущерб. Экономический эффект от управления рисками определяется как разница между $EMV_{п}$ и $EMV_{факт}$ по формуле

$$EMV_{эффект} = EMV_{п} - EMV_{факт}.$$

и составляет 81,1 тыс. руб.

− Индекс эффективности затрат (CPI), позволяющий оценить финансовую обоснованность инвестиций в управление рисками, рассчитывается как отношение ожидаемой денежной стоимости предотвращенных рисков ($EMV_{эффект}$) к общему бюджету риск-менеджмента (RRC) по формуле

$$CPI = EMV_{эффект} / RRC$$

и составляет 1,33.

− Эффект по срокам. Потенциальная задержка (ESIп) составила 48,4 дня, фактическая (ESIфакт) – 11 дней. Таким образом, эффект от управления рисками по срокам равен 48,4 – 11 = 37,4 дня. Это означает, что благодаря превентивным и корректирующим действиям, реализованным в процессе управления рисками, проекту удалось избежать более одного месяца просрочки.

Результаты исследования подтверждают высокую эффективность разработанной методики управления рисками ИТ-проектов. Ее практическая реализация осуществлялась с использованием отечественной системы RiskGap, которая выступала инструментальной платформой для формализации и документирования процессов управления рисками.

Разработанная методика позволила систематизировать процесс управления рисками, повысить прозрачность за счет централизованного реестра и визуализации, а также обосновать управленческие решения количественными расчетами (EMV, CPI). Значение CPI > 1 доказывает экономическую целесообразность вложений в риск-менеджмент.

Основными преимуществами методики являются: практическая ориентация, а именно четкая привязка к этапам проекта и функционалу конкретного инструмента (RiskGap); адаптивность, то есть возможность настройки шаблона реестра и критериев оценки под специфику разных IT-проектов; экономическая обоснованность. Встроенный механизм расчета эффекта позволяет оценивать отдачу от мероприятий по управлению рисками.

В то же время были выявлены отдельные ограничения. Во-первых, одним из основных ограничений, выявленных в ходе апробации, является субъективность экспертных оценок вероятности и влияния (P/I), что может влиять на точность приоритизации. Для нивелирования данного фактора в перспективе возможно дополнение методики механизмами анализа исторических данных по аналогичным проектам. Во-вторых, сложность количественной оценки для нетехнических рисков. Дополнительным направлением может стать расширение типового шаблона рисков, созданного в рамках исследования. На его основе возможно формирование отраслевых каталогов рисков и стратегий реагирования, что позволит повысить уровень стандартизации в управлении рисками ИТ-проектов.

Выводы

В результате проведенного исследования поставленная цель была достигнута – разработана и апробирована методика повышения эффективности управления рисками IT-проектов. К наиболее важным результатам, определяющим научную и практическую значимость работы, можно отнести следующие:

1. Создана целостная методика, которая обеспечивает неразрывную связь теоретических принципов стандартов PMBOK и ГОСТ Р ИСО 31000 с практической реализацией в конкретной отечественной цифровой платформе RiskGap.

2. Разработан готовый инструментарий в виде типового шаблона реестра рисков и формализованного процесса (BPMN), что обеспечивает воспроизводимость и позволяет тиражировать подход, сокращая время на внедрение риск-менеджмента в аналогичных проектах.

3. Доказана экономическая целесообразность методики. На примере конкретного проекта показано, что ее системное применение приводит к значительному снижению потенциального ущерба, а затраты на реализацию являются экономически оправданными.

Таким образом, работа предлагает руководителям проектов и риск-менеджерам структурированный, технологичный и экономически обоснованный инструмент, который позволяет перейти от фрагментарного учета рисков к системному управлению ими на протяжении всего жизненного цикла IT-проекта, повышая вероятность их успешного завершения.

Список литературы

1. Щербак А. В. Управление рисками в сфере ИТ: монография. М.: ИНФРА-М, 2023. 243 с. URL: https://znanium.ru/catalog/product/1900623 (дата обращения: 14.10.2025). ISBN 978-5-16-017972-8.

2. Николаенко В. С. Риск, риск-менеджмент и неопределенность: уточнение понятий // Государственное управление. Электронный вестник. 2020. № 81. С. 91–119. URL: https://cyberleninka.ru/article/n/risk-risk-menedzhment-i-neopredelennost-utochnenie-ponyatiy (дата обращения: 14.10.2025). DOI: 10.24411/2070-1381-2020-10080.

3. Дорохина Е. Ю. Управление рисками проектов в рамках методологии Scrum // Вестник Алтайской академии экономики и права. 2023. № 4–1. С. 39–44. URL: https://vaael.ru/ru/article/view?id=2760 (дата обращения: 18.12.2025). DOI: 10.17513/vaael.2760.

4. Ильина О. Н. Методология управления проектами: становление, современное состояние и перспективы развития: монография. М.: ИНФРА-М, 2025. 215 с. URL: https://znanium.ru/catalog/product/2183461 (дата обращения: 15.10.2025). ISBN 978-5-16-019624-4.

5. Капустина Н. В. Развитие организации на основе риск-менеджмента: теория, методология и практика: монография. М.: ИНФРА-М, 2024. 179 с. URL: https://znanium.com/catalog/product/1905228 (дата обращения: 15.10.2025). ISBN 978-5-16-010571-0.

6. Капустина Н. В. Теоретико-методологические подходы риск-менеджмента: монография. М.: ИНФРА-М, 2020. 140 с. URL: https://znanium.ru/catalog/product/1007996 (дата обращения: 15.10.2025). ISBN 978-5-16-010601-4.

7. Серебрякова Т. Ю., Гордеева О. Г. Риски организации: их учет, анализ и контроль: монография. М.: ИНФРА-М, 2020. 233 с. URL: https://znanium.com/catalog/product/1081000 (дата обращения: 16.10.2025). ISBN 978-5-16-014777-2.

8. Тихомирова О. Г. Управление проектом: комплексный подход и системный анализ: монография. М.: ИНФРА-М, 2024. 300 с. URL: https://znanium.com/catalog/product/2102184 (дата обращения: 16.10.2025). ISBN 978-5-16-006383-6.

9. Nikolaenko V., Sidorov A. Analysis of 105 IT Project Risks // Journal of Risk and Financial Management. 2023. Vol. 16 (1). P. 33. DOI: 10.3390/jrfm16010033.

10. Маслова Е. В. Модели и методы управления рисками на стадиях жизненного цикла ИТ-сервиса: автореф. дис. …канд. техн. наук. Новокузнецк, 2018. 21 с. URL: https://viewer.rsl.ru/ru/rsl01008714211?page=1&rotate=0&theme=white (дата обращения: 16.10.2025).

11. Мирзаянц К. С., Воробьева О. А., Головина О. Д. Искусственный интеллект в управлении проектами: тренды, возможности, первый опыт // Вестник Удмуртского университета. Серия «Экономика и право». 2025. № 4. С. 615–621. URL: https://cyberleninka.ru/article/n/iskusstvennyy-intellekt-v-upravlenii-proektami-trendy-vozmozhnosti-pervyy-opyt (дата обращения: 18.12.2025). DOI: 10.35634/2412-9593-2025-35-4-615-621.

12. Баркалов С. А., Белоусов А. В., Пужанова Е. О. Алгоритмы управления рисками в ИТ-проектах // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2025. № 3. С. 77–86. URL: https://cyberleninka.ru/article/n/algoritmy-upravleniya-riskami-v-it-proektah (дата обращения: 18.12.2025). DOI: 10.14529/ctcr250307.

13. Плотникова Е. Д., Чусавитина Г. Н. Отечественные цифровые платформы для управления рисками ИТ-проектов // Управление проектами: сборник статей по материалам III Всероссийской научной конференции (г. Магнитогорск, 19–20 декабря 2024 г.). Магнитогорск: Магнитогорский государственный технический университет им. Г. И. Носова, 2025. С. 393–400. URL: https://www.elibrary.ru/item.asp?id=82273702 (дата обращения: 17.10.2025).

14. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство: национальный стандарт Российской Федерации: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 10 декабря 2019 г. № 1379-ст: дата введения 2020-03-01. М.: Стандартинформ, 2020. 20 с. URL: https://rags.ru/gosts/gost/73107/ (дата обращения: 05.02.2026).

15. Павлов А. Н. Эффективное управление проектами на основе стандарта PMI PMBOKOR 6th Edition : учебное пособие. 2-е изд. М.: Лаборатория знаний, 2023. 367 с. URL: https://znanium.com/catalog/product/2032531 (дата обращения: 05.02.2026). ISBN 978-5-93208-635-3.

Конфликт интересов: Авторы заявляют об отсутствии конфликта интересов.

Conflict of interest: The authors declare that there is no conflict of interest.