

УДК 33**Идентификация и классификация экономических рисков
разработки ПО в сфере веб-разработки****Комлев Сергей Юрьевич**

Аспирант,
Московский университет "Синергия",
125190, Российская Федерация, Москва, Ленинградский просп., 80–Г;
e-mail: sk@graftype.com

Ерофеев Владислав Денисович

Аспирант,
Московский университет "Синергия",
125190, Российская Федерация, Москва, Ленинградский просп., 80–Г;
e-mail: vladiis.eroff@yandex.ru

Аннотация

В статье исследуются методологические аспекты управления рисками в проектах веб-разработки с акцентом на процесс идентификации потенциальных угроз как ключевого элемента обеспечения успешной реализации ИТ-проектов. Проведен системный анализ существующих методик выявления рисков в разработке программного обеспечения, включая FMEA-анализ, SWOT-анализ и экспертные оценки. На основе критического осмысления теоретических подходов и практического опыта предложена оригинальная многоуровневая классификация рисков веб-разработки, структурированная по пяти основным категориям: экономические (финансовая нестабильность, колебания рыночной конъюнктуры), технологические (устаревание стека технологий, проблемы совместимости), организационные (ошибки планирования, неэффективная коммуникация), ресурсные (дефицит квалифицированных кадров, недостаток вычислительных мощностей) и внешние (изменения законодательства, действия конкурентов). Детально рассмотрены этапы процесса идентификации рисков - от первичного сбора информации до верификации полученных данных, сформулированы практические рекомендации по формированию комплексного реестра рисков, включая критерии приоритизации и методы оценки вероятности возникновения. Особое внимание уделено вопросам адаптации классических методов риск-менеджмента к специфике веб-разработки, характеризующейся высокой динамикой изменений и короткими жизненными циклами продуктов. Полученные результаты представляют значительную практическую ценность для проектных менеджеров и разработчиков, позволяя оптимизировать процессы выявления и оценки рисков на ранних стадиях реализации веб-проектов, что в конечном итоге способствует повышению качества управления проектами в целом.

Для цитирования

Комлев С.Ю., Ерофеев В.Д. Идентификация и классификация экономических рисков разработки ПО в сфере веб-разработки // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 3А. С. 721-727.

Ключевые слова

управление рисками, веб-разработка, идентификация рисков, классификация рисков, ИТ-проекты, риск-менеджмент.

Введение

Современная веб-разработка характеризуется высокой динамичностью, жесткой конкуренцией и быстрыми изменениями требований пользователей. В таких условиях проекты по созданию и поддержке веб-приложений неизбежно сопряжены с многочисленными рисками. Риск в проектном контексте понимается как событие или условие, при наступлении которого проект может получить негативный (или позитивный) эффект. Эффективное управление рисками критично для успешного результата: руководитель проекта должен определить, оценить, расставить приоритеты и управлять всеми основными рисками на всех этапах разработки [Соколов, Савченко, Соловьев, Схведиани, 2024; Тихонов, Субботина, 2022; Щербак, 2023].

Веб-проекты имеют свои особенности: необходимость быстрой адаптации под меняющиеся требования рынка, использование новых технологий, высокая роль пользовательского опыта и безопасность данных. Эти факторы обуславливают разнообразие рисков, актуальных для веб-разработки. Исследование рисков в ИТ-проектах неоднократно отмечало низкий процент успеха (по некоторым оценкам, доля успешных ИТ-проектов редко превышает 30 %). На основе анализа литературы и практического опыта определим ключевые направления работы по идентификации рисков и предложим схему их классификации, специфичную для веб-разработки.

Основное содержание

Идентификация рисков – это процесс систематического выявления возможных угроз и проблем, которые могут повлиять на цели проекта, и документирования их характеристик. Обычно это итеративный процесс, продолжающийся на протяжении всего жизненного цикла проекта. Для качественной идентификации задействуется вся команда проекта, а также, при необходимости, внешние эксперты. Начинают с анализа исходной документации (технических заданий, планов, исторических данных) и описания продукта. Источниками информации служат бизнес-требования, предположения, опыт предыдущих проектов и др.

Для сбора информации о рисках применяются разнообразные методы: мозговой штурм, экспертные интервью, опросы, метод Дельфи, сценарный анализ и пр. Часто используется анализ по диаграмме Исикавы (рыбья кость), когда ключевые факторы риска разбиваются по тематическим ветвям (технологии, процессы, люди и др.). Такой многомерный подход обеспечивает широкое покрытие потенциальных рисковых событий.

Завершающим этапом идентификации является формирование реестра рисков – структурированного списка выявленных рисков. Каждая запись реестра обычно содержит название риска, описание причин и условий его возникновения, потенциальное влияние на проект и возможные меры реагирования (предотвращения и снижения последствий). Таким образом формируется база для дальнейшего качественного и количественного анализа рисков.

Научная новизна данного исследования во многом состоит в предложении авторской

классификации рисков, характерных для проектов веб-разработки. С учетом специфики этой области выделены следующие основные категории рисков:

Технологические риски: связаны с технической частью проекта – выбранные фреймворки, языки, архитектура, инфраструктура. Например, риск несовместимости используемых технологий, недостаточной масштабируемости архитектуры, устаревания технологий или зависимости от внешних сервисов;

Организационные и управленческие риски: охватывают процессы и методы работы над проектом. Сюда относятся риски неточного планирования сроков, неясности требований заказчика, изменений ТЗ в ходе разработки, низкой эффективности коммуникации внутри команды или с клиентом;

Кадровые риски: связаны с людскими ресурсами и компетенциями. Сюда входят недостаток специалистов нужного профиля или их высокая текучесть, ошибки разработчиков, нехватка опыта в применении новых технологий, риски связанные с распределенной (удаленной) работой команды;

Информационные и коммуникационные риски: риски нарушения информационных потоков и взаимодействия. Например, нехватка доступа к актуальной информации, слабое управление знаниями, недопонимание в процессе коммуникаций между заказчиком и разработчиками;

Риски безопасности: специфичны для веб-проектов и включают уязвимости веб-приложений, возможность хакерских атак, утечки конфиденциальных данных, DDoS-атаки, а также соответствие законодательным требованиям информационной безопасности;

Бизнес- и рыночные риски: внешние риски, влияющие на проект через изменение условий среды. Например, изменение требований рынка или конкуренция, экономические колебания, отказ интеграции с внешними платформами (социальные сети, платёжные системы), а также регуляторные изменения (например, новые законы о персональных данных);

Качество и пользовательские риски: выход проектного решения не соответствующим ожиданиям пользователей. Сюда относятся низкое качество UX/UI дизайна, ошибка в понимании потребностей конечного пользователя, низкая производительность сайта при росте нагрузки и пр.

Таким образом, предлагаемая классификация учитывает как традиционные категории ИТ-проектов (технические, организационные, ресурсные и внешние риски), так и специфичные для веб-разработки факторы (безопасность веб-приложений, требования конечных пользователей и т.д.).

Таблица 1 иллюстрирует предложенную классификацию рисков веб-проектов. В ней приведены основные классы рисков и типичные примеры событий, относящихся к каждому классу. Такая таблица позволит проектной команде при идентификации рисков ориентироваться на ключевые категории и заранее готовить список потенциальных угроз в каждой области.

Таблица 1 - Классификация рисков веб-разработки по категориям (с примерами типичных рисковых событий)

Класс рисков	Примеры рисковых событий
Технологические	Несовместимость технологий (фреймворков, библиотек); неисправности серверного оборудования; сбои API внешних сервисов; ограниченные возможности масштабирования архитектуры.
Организационно-управленческие	Частые изменения требований; неточный расчёт трудозатрат; отсутствие чётких процессов разработки; плохая коммуникация с заказчиком или внутри команды.

Класс рисков	Примеры рисковых событий
Кадровые	Недостаток квалифицированных разработчиков; высокая текучесть команды; неравномерная загрузка специалистов; ошибки из-за непонимания требований.
Информационные/коммуникационные	Неудовлетворительная передача требований; разрозненность документов проекта; задержки с утверждением ТЗ; отсутствие единого реестра задач.
Безопасностные	Уязвимости веб-приложения (SQL-инъекции, XSS); атаки на сервер (DDoS); утечка персональных данных; несоответствие стандартам информационной безопасности.
Бизнес-/рыночные	Внезапное изменение рыночного спроса; появление нового конкурента; отказ контрагентов от интеграции; изменение законодательства (например, требования GDPR).
Качество/пользовательские	Недовольство пользователей интерфейсом; низкая скорость отклика сайта при нагрузке; ошибки при работе на разных браузерах/устройствах; функциональные дефекты.

Процесс выявления рисков в проекте целесообразно разделить на несколько этапов. Таблица 2 отражает обобщенную схему этапов идентификации рисков в веб-проекте с указанием основных действий и методов на каждом этапе. Она может служить ориентиром для организаторов проектных работ.

На начальном подготовительном этапе формируется план работы по идентификации: анализируются бизнес-процессы и сценарии использования будущей системы, составляются предварительные контрольные списки рисков (например, опираясь на Таблицу 1 и реестр рисков компании), подготавливаются вопросы для опроса экспертов.

Таблица 2 - Этапы идентификации рисков веб-проекта (методы и действия)

Этап	Основные действия и методы
Подготовительный	Анализ требований и сценариев использования; составление предварительных контрольных списков рисков; подготовка регламентов и опросников; сбор информации по предыдущим проектам.
Идентификация	Проведение мозгового штурма и фокус-групп среди команды и экспертов; интервьюирование специалистов и заказчика; применение методики «Что если?»; построение диаграммы Исикавы.
Анализ и документирование	Качественная (и при возможности количественная) оценка рисков (вероятность и влияние); составление реестра рисков; приоритизация рисков; разработка стратегий реагирования (превентивные и корректирующие меры).

На этапе идентификации рисков привлекаются ключевые участники проекта (технический директор, ведущие разработчики, бизнес-аналитики, представители заказчика). Организуются сессии мозгового штурма, фокус-групповые обсуждения, экспертные интервью, опросы.

Далее на этапе анализа проводится оценка вероятности и влияния каждого риска (качественный и, при возможности, количественный анализ). Составляются качественные рейтинги рисков, формируется матрица рисков, в которой рисковые события располагаются по степеням вероятности возникновения и тяжести последствий. По результатам анализа составляется окончательный реестр рисков.

На практике эффективная реализация описанного процесса требует учёта опыта конкретных компаний. Так, в работе регулярно проводится аудит рисков на этапе планирования проектов. К наиболее частым технологическим рискам включают: устаревание используемого фреймворка, зависимость от нестабильных API сторонних сервисов, а также проблемы с

производительностью при резком росте трафика. Из организационных рисков отмечают: нечеткое формулирование требований от заказчиков, пропуски в коммуникации между разработчиками и менеджерами проекта, а также недостаточный резерв времени на тестирование.

При идентификации этих рисков можно применять комбинацию методов: совместные встречи команды и заказчика для выработки согласованного ТЗ, использование контрольных списков рисков (с включением позиций из Таблицы 1), а также регулярные ревью кода и архитектуры проекта. Так, диаграмма Исикавы применялась при планировании крупного веб-портала: команда сформировала дерево причин потенциального отказа (например, ветвь «Код» включала недоработки безопасности и технический долг, ветвь «Процессы» – плохую документацию и отсутствие регламента), что позволило выявить скрытые риски и заложить в план дополнительную экспертизу.

В практической части анализа проекта возможно использовать таблицы идентификации и матрица рисков. По итогам оценки формируется план реагирования: например, на риск потери доступа к базе данных составляется резервная копия (меры предотвращения) и план аварийного переключения на резервный сервер (меры смягчения). Такой подход соответствует рекомендациям специалистов: применение многоуровневой классификации и ранжирования рисков позволяет повысить качество мониторинга угроз.

Заключение

Идентификация и классификация рисков являются ключевыми задачами успешного управления веб-проектами. Предложенный подход объединяет широко применимые методы выявления рисков и адаптированную к веб-разработке структуру классификации. Научная новизна работы заключается в авторском выделении категорий рисков, специфичных для веб-приложений и интернет-сервисов, а также в систематизации этапов их идентификации с учетом современных практик (многометодный анализ, экспертные оценивания, рисковно-ориентированное планирование).

Практическая значимость исследования подтверждается тем, что применение рекомендованной схемы позволяет командам заранее прогнозировать наиболее опасные области, уменьшать неопределённость и своевременно разрабатывать меры управления рисками. В частности, опыт компании Graftype демонстрирует эффективность комплексного подхода: применение авторской классификации рисков в сочетании с активным вовлечением команды разработки в процесс выявления угроз ведет к снижению числа непредвиденных проблем на этапе реализации.

Таким образом, данные рекомендации и представленные таблицы могут быть использованы проектными менеджерами и аналитиками для повышения эффективности риск-менеджмента в сфере веб-разработки, что в конечном счете способствует успешной реализации проектов и повышению качества программных продуктов.

Библиография

1. Соколов Д.А., Савченко Н.А., Соловьев М.В., Схведиани А.Е.. Методика оценки рисков ИТ-проектов // ЕГИ. 2024. №4 (54). URL: <https://cyberleninka.ru/article/n/metodika-otsenki-riskov-it-proektov> (дата обращения: 15.04.2025);
2. Майкова А. А., Кислицына С. И., Старченкова О. Д., Холина Е. Р. 2024. Оценка и анализ рисков ИТ-проекта по разработке инновационного продукта по развитию региона // Вестник Тюменского государственного

- университета. Социально-экономические и правовые исследования. Том 10. № 4 (40). С. 207–231. <https://doi.org/10.21684/2411-7897-2024-10-4-207-231>;
3. Тихонов А. Г., Субботина Т. Н. Управление рисками при разработке программного обеспечения // Экономика и бизнес: теория и практика. 2022. №5-3. URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-pri-razrabotke-programmnogo-obespecheniya> (дата обращения: 22.04.2025);
 4. Щербак, А. В. Управление рисками в сфере IT: монография / А.В. Щербак. - Москва: ИНФРА-М, 2023. - 243 с. - (Научная мысль). - DOI 10.12737/1900623. - ISBN 978-5-16-017972-8;
 5. Kaur R., Gabrijelčič D., Klobučar T. Artificial intelligence for cybersecurity: Literature review and future research directions //Information Fusion. – 2023. – Т. 97. – С. 101804.
 6. Amini M. et al. Mahamgostar. com as a case study for adoption of laravel framework as the best programming tools for php based web development for small and medium enterprises //Journal of Innovation & Knowledge, ISSN. – 2021. – С. 100-110.
 7. Hou X. et al. Large language models for software engineering: A systematic literature review //ACM Transactions on Software Engineering and Methodology. – 2024. – Т. 33. – №. 8. – С. 1-79.
 8. Vacca A. et al. A systematic literature review of blockchain and smart contract development: Techniques, tools, and open challenges //Journal of Systems and Software. – 2021. – Т. 174. – С. 110891.
 9. Khan R. A. et al. Security risks of global software development life cycle: Industry practitioner's perspective //Journal of Software: Evolution and Process. – 2024. – Т. 36. – №. 3. – С. e2521.
 10. Hutchinson B. et al. Towards accountability for machine learning datasets: Practices from software engineering and infrastructure //Proceedings of the 2021 ACM conference on fairness, accountability, and transparency. – 2021. – С. 560-575.

Identification and Classification of Economic Risks in Software Development for Web Projects

Sergei Yu. Komlev

Postgraduate Student,
Moscow "Synergy" University,
125190, 80–G, Leningradsky ave., Moscow, Russian Federation;
e-mail: sk@graftype.com

Vladislav D. Erofeev

Postgraduate Student,
Moscow "Synergy" University,
125190, 80–G, Leningradsky ave., Moscow, Russian Federation;
e-mail: vladiis.eroff@yandex.ru

Abstract

The article examines methodological aspects of risk management in web development projects, focusing on threat identification as a key element for successful IT project implementation. Through systematic analysis of existing risk identification methodologies (including FMEA, SWOT analysis, and expert assessments), the authors propose an original multi-level classification system for web development risks, structured into five categories: economic (financial instability, market fluctuations), technological (technology stack obsolescence, compatibility issues), organizational (planning errors, ineffective communication), resource-related (skills shortage, insufficient computing power), and external (regulatory changes, competitor actions). The study details risk identification stages from initial data collection to verification, offering practical recommendations

for comprehensive risk register development with prioritization criteria and probability assessment methods. Special attention is given to adapting classical risk management approaches to web development's unique characteristics - rapid changes and short product lifecycles. The findings provide significant practical value for project managers and developers, enabling optimized risk identification and assessment during early project phases, ultimately enhancing overall project management quality.

For citation

Komlev S.Yu., Erofeev V.D. (2025) Identifikatsiya i klassifikatsiya ekonomicheskikh riskov razrabotki PO v sfere veb-razrabotki [Identification and Classification of Economic Risks in Software Development for Web Projects]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (3A), pp. 721-727.

Keywords

Risk management, web development, risk identification, risk classification, IT projects, risk assessment.

References

1. Sokolov D.A., Savchenko N.A., Soloviev M.V., Shvediani A.E.. Risk assessment methodology for IT projects // EGI. 2024. No. 4 (54). URL: <https://cyberleninka.ru/article/n/metodika-otsenki-riskov-it-proektov> (date of request: 04/15/2025);
2. Maikova A. A., Kislitsyna S. I., Starchenkova O. D., Kholina E. R. 2024. Assessment and risk analysis of an IT project for the development of an innovative product for the development of the region // Bulletin of the Tyumen State University. Socio-economic and legal studies. Volume 10. No. 4 (40). pp. 207-231. <https://doi.org/10.21684/2411-7897-2024-10-4-207-231>;
3. Tikhonov A. G., Subbotina T. N. Risk management in software development // Economics and Business: theory and practice. 2022. No.5-3. URL: <https://cyberleninka.ru/article/n/upravlenie-riskami-pri-razrabotke-programmnogo-obespecheniya> (date of request: 04/22/2025);
4. Erbak, A.V. Risk management in the world: a monograph / A.V. Erbak. Moscow: NAUKA-M, 2023. 243 p. (Initial thought). - DOI 10.12737/1900623. - ISBN 978-5-16-017972-8;
5. Kaur R., Gabrielcic D., Klobuchar T. Artificial intelligence for cybersecurity: a literature review and directions for future research //Merging of information. – 2023. – Vol. 97. – p. 101804.
6. Amini M. et al. Mahamgostar. com as an example of the implementation of the laravel framework as the best programming tool for php-based web development for small and medium-sized enterprises //Journal of Innovation & Knowledge, ISSN. – 2021. - pp. 100-110.
7. Howe H. and others . Models of large languages for software development: a systematic review of the literature //ACM Transactions on Software Engineering and Methodology. – 2024. – Vol. 33. – No. 8. – pp. 1-79.
8. Vacca A. and others. A systematic review of the literature on blockchain and smart Contract Development: Methods, Tools, and Open Challenges //Journal of Systems and Software. – 2021. – Vol. 174. – p. 110891.
9. Khan R. A. and others. Security risks of the global software development lifecycle: the view of an industry specialist //Journal of Software: Evolution and Processes. – 2024. – Vol. 36. – No. 3. – p. e2521.
10. Hutchinson B. et al. Towards Accountability for Machine Learning Datasets: Software and Infrastructure Development Practices //Proceedings of the ACM 2021 Conference on Equity, Accountability and Transparency. - 2021. – pp. 560-575.