

Николаенко В.С.

Разработка подходов к классификации рисков в ИТ-проектах*

Николаенко Валентин Сергеевич — ассистент, Томский политехнический университет, Томск, РФ.

E-mail: nikolaenkovs@tpu.ru

SPIN-код РИНЦ: [9301-1835](https://elibrary.ru/9301-1835)

Аннотация

В статье рассматриваются результаты анализа существующих отечественных и зарубежных подходов к классификации рисков, в том числе в проектах, реализуемых в сфере информационных технологий. Также в статье приводятся типичные и часто встречаемые негативные риски, полученные в ходе проведенных исследований в 12 ИТ-проектах, реализуемых в 5 ИТ-организациях, с их последующей верификацией с разработанными автором подходами к классификации рисков событий. Полученные результаты проведенного исследования будут интересны руководителям (менеджерам) проектов и проектным командам, т. к. разработанные подходы к классификации рисков в ИТ-проектах удовлетворяют таким требованиям, как повышение качества идентификации рисков, обеспечение управляемости проекта, улучшение контроля и мониторинга возможных угроз и опасностей.

Ключевые слова

Риск, классификация рисков, управление рисками, риск-менеджмент, ИТ-проект.

Введение

Общепризнанной проблемой зарубежных и отечественных сообществ, занятых изучением природы риска (вероятного события, способного оказать влияние на цели организации и / или проекта)¹, является разработка универсального и единого подхода к классификации рисков². Поиск решения данной проблемы представляет как научный, так и практический интерес, т. к. эффективность риск-менеджмента напрямую зависит от качественной классификации рисков событий³. Так, например, в проектах, реализуемых в сфере информационных технологий (ИТ-проектах), классификация рисков событий позволяет повысить качество их идентификации, сформулировать единые стандарты для мероприятий реагирования и ликвидации последствий от наступления риска, а также улучшить контроль и мониторинг возможных угроз.

Несмотря на актуальность задачи по разработке универсального и единого подхода к классификации рисков, научные ассоциации и институты, занятые

* Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-36-00031 мол а.

¹ ISO/IEC 31010:2009 “Risk management — Risk assessment techniques” (ИСО/МЭК 31010:2009 «Менеджмент риска. Методы оценки риска»).

² Соколов Д.В. Классификация рисков, как многозадачный инструмент риск-менеджмента организации // Управление экономическими системами: электронный научный журнал. 2011. № 30. URL: <http://uecs.ru/uecs30-302011/item/489-> (дата обращения: 30.04.2017).

³ The CHAOS Manifesto / The Standish Group International, 2014.

изучением природы риска, не имеют общей точки зрения по данному вопросу. Отсутствие единого мнения создает трудности, что, в свою очередь, выявляет актуальную проблему, связанную с формализацией подходов к классификации рисков событий, например, в ИТ-проектах. Необходимо отметить, что классификация рисков в ИТ-проектах должна представлять определенную практическую ценность для **руководителей проектов и проектных команд**, иначе, в связи с ограниченностью ресурсов в проекте, классификация рисков не будет проводиться⁴.

В этой связи **целью статьи** является разработка подхода к классификации негативных рисков событий для ИТ-проектов, удовлетворяющего следующим требованиям:

а) повышение качества идентификации рисков событий, например, классификация рисков должна способствовать выявлению скрытых и неявных рисков (шт.);

б) обеспечение управляемости проекта путем стандартизации мер реагирования на риски и ликвидации их последствий. Например, для определенных групп риска могут быть формализованы превентивные мероприятия по их нивелированию, переносу или ослаблению (шаблоны мер реагирования — «План А», и мер отступления (ликвидации) — «План Б», рекомендуемые к использованию)⁵;

с) улучшение контроля и мониторинга возможных угроз и опасностей. Так, например, зная актуальные риски для определенного этапа жизненного цикла ИТ-проекта, руководитель проекта может заблаговременно мобилизовать резервные ресурсы. Однако если данные рисковые события не наступили, то ресурсы высвобождаются, уменьшая предельную стоимость проекта (оценка трудозатрат на базе шаблонов мер «План А» и «План Б»)⁶.

Для достижения данной цели были решены следующие **задачи**:

1. анализ подходов к классификации рисков событий, в том числе и в проектах, реализуемых в сфере информационных технологий;

⁴ Nikolaenko V.S., Petuhov O.N., Petukhova O.V., Romanovsky V.V. Special Aspects of Risk Management in IT-Projects // The 28th International Business Information Management Accusation Conference 2016 (IBIMA), 2017. P. 241–260.

⁵ Грицаев Р.Т., Николаенко В.С. Управление рисками в проектах, реализуемых в сфере информационных технологий // Современные проблемы и тенденции развития экономики, управления и информатики в XXI веке: Сборник научных статей по материалам научно-практической конференции с международным участием / Финансовый университет при Правительстве Российской Федерации. СПб., 2015. С. 35–37.

⁶ Селиховкин И. Управление ИТ-проектом. Эффективная система «с нуля» в любой организации. СПб., 2010. URL: <http://www.lessonslarned.ru/sites/default/files/ITPM-Selikhovkin.pdf> (дата обращения: 30.04.2017).

2. идентификация типичных и часто встречаемых негативных рисков в ИТ-проектах;

3. разработка подходов к классификации негативных рисков событий для проектов, реализуемых в сфере информационных технологий.

Для решения **первой задачи** был проведен анализ трудов Ю.П. Волковой, Е.А. Олейниковой, М.В. Пирогова, В. Павлова, С.А. Филина и С. Хозяинова⁷, которые классифицируют риски по масштабу проявления и влияния на экономических агентов⁸, в частности:

- макроуровень имеет дело с политическими рисковыми событиями, последствия которых отражаются на экономических агентах, в том числе и на иностранных агентах⁹;
- мезоуровень — риски, специфичные для определенной сферы экономики, отрасли, региона. Мезориски имеют отраслевую или региональную природу;
- микроуровень (предпринимательские риски) — риски, специфичные для определенного субъекта экономики или отдельного проекта.

Отметим, что данный подход к классификации рисков событий не полностью раскрывает сферу информационных технологий, ограничиваясь только уровнем предпринимательских рисков (риски микроуровня).

И.Т. Балабанов и М.М. Максимцов¹⁰ предлагают классификацию рисков на основании финансового видения¹¹. Данная классификация рисков широко охватывает источники рисков событий, однако не учитывает источники рисков событий, актуальных для сферы информационных технологий. Отметим, что классификация рисков, предложенная М.М. Максимцовым, представляет интерес, т. к. дает возможность систематизировать значительную часть предпринимательских рисков.

Классификация, предложенная Т. Мерна и Ф. Ал-Хани¹², базируется на таких источниках рисков событий, как рынок, политика, экономика, технологии, люди, криминал, загрязнение окружающей среды и т.п., но не учитывает специфику и особенности рисков, актуальных для сферы информационных технологий и ИТ-проектов.

⁷ Волкова Ю.П., Олейникова Е.А., Филин С.А., Пирогов М.В. Инвестиционная политика современной России: Коллективная монография. М.: РЭА им. Г.В. Плеханова, 2001.

⁸ Филин С. Неопределенность — от недостатка информации // РИСК. 2000. № 2-3. С. 62–67.

⁹ Клейнер Г.Б. Мезоэкономика переходного периода: рынки, отрасли, предприятия. М.: Наука, 2001.

¹⁰ Максимцов М.М., Игнатъева А.В., Комаров М.А. и др. Менеджмент. М.: ЮНИТИ, 1998.

¹¹ Балабанов И.Т. Риск-менеджмент. М.: Финансы и статистика, 1996.

¹² Merna T., Al-Thani F. Corporate Risk Management. 2nd ed. Chichester, UK; Hoboken, N.J.: John Wiley & Sons, Ltd, 2008.

Система классификаций рисков Б. Мильнера и Ф. Лииса может быть использована для проведения классификации рисков в ИТ-проектах, однако данный подход имеет один существенный недостаток, а именно: распределение на внешние и внутренние риски не в полной мере отвечает современным представлениям о внешней и внутренней среде ИТ-организаций.

Классификация рисков, предложенная Д.Н. Колесником, также представляет определенный интерес, т. к. исследователем рассматриваются риски, характерные для ИТ-проектов¹³. Согласно концепции, предложенной Д.Н. Колесником, риски в ИТ-проектах можно распределить на три группы. К первой группе относятся организационные риски, которые подразделяются на:

- переговорные риски — риски, которые связаны с ожиданиями ключевых участников проекта;
- методологические риски — риски, связанные со степенью соответствия принимаемой методики реализации с требованиями проекта;
- информационные риски — риски, связанные с полнотой и качеством информации;
- коммуникационные риски — риски, связанные с обменом информацией между участниками проекта;
- риски внешней среды — риски, обусловленные необходимостью учета ограничений внешней среды. Под внешней средой Д.Н. Колесник понимает порядок работы подразделений организации, например, бухгалтерии, *HR*, службы внутренней безопасности и т. п.

Ко второй группе относятся проектные риски, связанные с:

- нечетким определением целей и задач проекта (содержание, сроки, длительность и качество проекта);
- заинтересованными в проекте сторонами, например, увольнение ключевых участников, болезнь, человеческий фактор и т. п.;
- недостаточно четким определением промежуточных и конечных результатов проекта, а также с избыточной или недостаточно проработанной картой проекта, его ключевыми вехами и ожиданиями (результаты и этапы проекта).

¹³ Колесник Д.Н. Практические аспекты внедрения информационных систем оценки деятельности предприятия // Системы управления бизнес-процессами. 2012. № 9. URL: <http://journal.itmane.ru/node/820> (дата обращения: 30.04.2017).

К третьей группе относятся технические риски. Анализ рисков данной группы направлен на ИТ-составляющую проекта, которую можно разделить на следующие области:

- область источников информации (риски, связанные с недостаточной интегрируемостью данных в различные информационные системы);
- область ИТ-архитектуры (риски, связанные с несоответствием ИТ-архитектуры требованиям проекта).

Несмотря на учет специфики сферы информационных технологий, подход к классификации Д.Н. Колесника не удовлетворяет ни одному из требований, сформулированных в цели статьи. Подход Д.Н. Колесника не позволяет выявить скрытые и неявные рисковые события, обеспечить управляемость проекта путем стандартизации мероприятий реагирования и ликвидации последствий от наступления риска, а также не улучшает контроль и мониторинг возможных угроз и опасностей.

Далее рассмотрим подход В.О. Ключникова¹⁴, где риски ИТ-проектов классифицируются по следующим категориям (Таблица 1):

- внутренние риски (специфичные для конкретной организации) — это риски, возникающие, в первую очередь, из-за влияния эндогенных факторов¹⁵;
- конкурентные риски — это риски, которые связаны с активностью конкурентного окружения;
- рыночные риски — это рисковые события, возникающие под влиянием экзогенных факторов.

Для того, чтобы охватить как можно больше рисков, которые могут оказать влияние на успешное завершение проекта, А.В. Полковников, М.Ф. Дубовик, Е.Ю. Песоцкая предлагают проводить классификацию в соответствии с:

- причинами возникновения риска (по типу источника риска);
- типами последствий риска, например, А — самое значительное влияние, В — значительное влияние¹⁶;
- типами мероприятий для управления рисками.

¹⁴ Ключников В.О. Идентификация рисков ИТ-проектов // Государственное управление. Электронный вестник. 2009. № 20. URL: http://e-journal.spa.msu.ru/vestnik/item/20_2009klyuchnikov.htm (дата обращения: 30.04.2017).

¹⁵ Никулина И.Е., Тухватулина Л.Р., Черепанова Н.В. Основы современного менеджмента. Томск: Издательство Томского политехнического университета, 2009.

¹⁶ Ching Gu V., Hoffman J.J., Cao Q., Schniederjans M.J. The Effects of Organizational Culture and Environmental Pressures on IT Project Performance: A Moderation Perspective // International Journal of Project Management. 2014. No 32. P. 1170–1181.

Таблица 1. Классификация рисков В.О. Ключникова

Тип	Название риска
Внутренние риски	Монетарные риски (проект не может быть реализован из-за проблем, связанных с финансированием)
	Структурные риски (проект является сложным в реализации; у проектной команды отсутствуют необходимые навыки, адекватная система управления и т. п.)
	Функциональные риски (ожидаемая прибыль от использования продукта не была достигнута)
	Организационные риски (саботаж проектной команды)
Конкурентные риски	Конкурентные риски (непредсказуемое поведение конкурентов на рынке)
Рыночные риски	Риски внешней среды (неожиданные изменения экзогенной среды, например, конфликт между партнерами, потеря лояльности потребителя и т. п.)
	Системные риски (ошибки в выбранном сегменте рынка, индустрии и т. п.)
	Технологические риски (отсутствие опыта использования новых технологий у проектной команды)

Подход, предложенный А.В. Полковниковым, М.Ф. Дубовиком, Е.Ю. Песоцкой, удовлетворяет ряду требований, предъявляемых к цели статьи, так, например, данный подход позволяет выявлять скрытые и неявные рисковые события и обеспечивать управляемость проекта путем стандартизации мероприятий реагирования и ликвидации последствий от наступления риска. Однако требование по улучшению контроля и мониторинга возможных угроз и опасностей удовлетворено не в полной мере.

Рассмотрим классификацию рисков, предложенную Ю.П. Ехлаковым, которая также представляет интерес, т. к. классифицирует рискообразующие факторы¹⁷. Так, например, к внутренним рискообразующим факторам Ю.П. Ехлаков относит:

- продукт — недостаточное и нестабильное финансирование проекта, частые изменения требований и т. п.;
- персонал — отсутствие опыта, необходимого для реализации проекта, саботаж отдельных членов проектной команды и т. п.;
- технологии реализации проекта — устаревание применяемых технологий, ошибки при выборе программного обеспечения, использование новых программных средств;
- технологии управления процессом реализации проекта — отсутствие у менеджера эффективной методологии управления процессом разработки ИТ-проекта, отсутствие опыта управления у менеджера ИТ-проекта, ошибки в оценках трудоемкости и сроков разработки и т. п.

К внешним рискообразующим факторам Ю.П. Ехлаков относит:

¹⁷ Ехлаков Ю.П. Классификация и описание рискообразующих факторов при создании программных продуктов // Управление, вычислительная техника и информатика. 2013. № 3. С. 124–128.

- государство — изменение нормативно-правовых механизмов ведения бизнес-деятельности, изменение экономической ситуации в государстве и т. п.;
- финансовый рынок — колебание курса валют, изменение кредитных ставок и т. п.;
- рынок труда — отсутствие необходимых специалистов;
- рынок, к которому относятся потребители и партнеры, — не востребованность рынком разработанного ИТ-продукта, появление на рынке ИТ-продуктов-субститутов и т. п.

Несмотря на установление рискообразующих факторов, которые способствуют выявлению скрытых угроз и опасностей, подход к классификации рисков событий, предложенный Ю.П. Ехлаковым, не удовлетворяет остальным требованиям, таким, как обеспечение управляемости по средствам стандартизации мероприятий реагирования и ликвидации последствий от наступления риска, а также улучшение контроля и мониторинга возможных угроз и опасностей.

Таблица 2. Анализ особенностей подходов к классификации рисков

№	Авторы и разработчики подхода к классификации рисков событий	Особенности подхода к классификации рисков событий
1	Ю.П. Волкова, Е.А. Олейникова, М.В. Пирогов, В. Павлов, С.А. Филин и С. Хозяинов	Не полностью раскрывает сферу ИТ, ограничиваясь только уровнем предпринимательских рисков (микроуровень)
2	И.Т. Балабанов и М.М. Максимцов	Не учитывает источники рисков событий, актуальных для сферы информационных технологий. Чрезмерная разветвленность усложняет определение рисков, актуальных для ИТ-проектов
3	Т. Мерна и Ф. Ал-Хани	Не учитывает специфику и особенности рисков, актуальных для сферы информационных технологий и ИТ-проектов
4	Б. Мильнер и Ф. Лиис	Распределение на внешние и внутренние риски не в полной мере соответствует представлениям об организациях, работающих в сфере ИТ
5	Д.Н. Колесник	Не удовлетворяет ни одному из требований, сформулированных в цели статьи
6	В.О. Ключников	Не удовлетворяет ни одному из требований, сформулированных в цели статьи
7	А.В. Полковников, М.Ф. Дубовик, Е.Ю. Песоцкая	Требование по улучшению контроля и мониторинга возможных угроз и опасностей удовлетворено не в полной мере
8	Ю.П. Ехлаков	Не удовлетворяет таким требованиям, как обеспечение управляемости по средствам стандартизации мероприятий реагирования и ликвидации последствий от наступления риска и улучшение контроля и мониторинга возможных угроз и опасностей

Для решения **второй задачи**, идентификации типичных и часто встречаемых негативных рисков в ИТ-проектах, были проведены исследования 12 ИТ-проектов в 5 ИТ-организациях¹⁸. В результате проведенных исследований был сформирован рейтинг 10 негативных рисков событий (Таблица 3), где каждому риску присвоен один балл (если риск совпадает с рисковым событием, которое было идентифицировано в другом проекте, то их баллы суммируются).

Таблица 3. Рейтинг типичных и часто встречаемых негативных рисков в ИТ-проектах

№	Прогнозируемые риски в проекте	Количество повторений, шт.
1	Будет отставание от запланированных сроков	12
2	Изменяются требования в процессе реализации проекта	10
3	Заказчик будет не удовлетворен сроками реализации проекта	10
4	Участники проектной команды будут иметь низкую мотивацию	8
5	Менеджер сделает ошибочную оценку сроков, необходимых для реализации проекта	8
6	Менеджер будет занят на других проектах	7
7	Проектная команда будет допускать ошибки при реализации проекта (<i>bugs</i>)	7
8	Участники проектной команды могут заболеть	7
9	Менеджер сделает ошибочную оценку человеческих ресурсов, необходимых для реализации проекта	7
10	Будет большая временная задержка в получении ответов на задаваемые заказчику проекта вопросы	7

В результате решения **третьей задачи** был разработан подход к классификации негативных рисков событий для проектов, реализуемых в сфере информационных технологий (Таблица 4).

Для проверки того, насколько разработанный подход к классификации негативных рисков в ИТ-проектах удовлетворяет заявленным требованиям, описанным в цели статьи, проведем верификацию 10 выявленных типичных и часто встречаемых негативных рисков (Таблица 3) и подходов к классификации рисков событий, актуальных для проектов, реализуемых в сфере информационных технологий (Таблица 4).

¹⁸ Официальный сайт ООО «Аксимедиа Софт». URL: <http://www.aximediashoft.com> (дата обращения: 30.04.2017); Официальный сайт ООО «ЛидерГрупп». URL: <http://www.lunacharsky.ru> (дата обращения: 30.04.2017); Официальный сайт ООО «СИС». URL: <http://oosis.com/promo> (дата обращения: 30.04.2017); Официальный сайт ООО «Спейс-О технологии». URL: <http://www.spaceotechnologies.com> (дата обращения: 30.04.2017); Официальный сайт ООО «Контек Софт». URL: <http://www.contek.ru/> (дата обращения: 30.04.2017).

Таблица 4. Области рисковых событий актуальные для ИТ-проектов

Область рискового события	Значение рискового события
Среда	1. Внутренняя (в рамках выполнения проекта) 2. Внешняя (за рамками выполнения проекта)
Уровень риска	1. Катастрофический (тигр) ¹⁹ 2. Непредсказуемый (аллигатор) 3. Часто встречаемый (щенок) 4. Незначительный (котенок)
Уровень управления	1. Управляемый 2. Частично управляемый 3. Неуправляемый
Внутрипроектные источники	1. Руководитель (менеджер) проекта ²⁰ 2. Команда проекта 3. Сотрудники, работающие по субподряду 4. Каналы коммуникаций (коммуникация) 5. Технологии 6. Информация 7. Заказчики проекта. Для случая, если проект является «заказным» 8. Юриспруденция (право) 9. Пользователь (имеется в виду пользователь, который будет пользоваться разработанным ИТ-продуктом)
Цели ИТ-проекта	1. Длительность проекта ²¹ 2. Бюджет (стоимость) проекта 3. Качество продукта 4. Содержание продукта
Фаза жизненного цикла ИТ-проекта	1. Инициация 2. Планирование 3. Реализация 4. Завершение

Среда. Риски, представленные в Таблице 3, относятся к внутренней среде проекта по следующим причинам²²:

- источники рисковых событий не выходят за рамки проекта;
- возможный ущерб от реализации рисков оказывает прямое влияние на успешное завершение проекта;
- рисковые события могут быть нивелированы, ослаблены и / или перенесены на третье лицо руководителем (менеджером) проекта;
- рассматриваемые риски не относятся к макроуровню и мезоуровню.

¹⁹ Николаенко В.С. Внедрение риск-менеджмента в ИТ-проекты // Государственное управление. Электронный вестник. 2016. № 54. С. 63–88.

URL: http://e-journal.spa.msu.ru/vestnik/item/54_2016nikolaenko.htm (дата обращения: 30.04.2017).

²⁰ Дайбова К.Е., Николаенко В.С. Разработка инструментария оперативной идентификации рисков в ИТ-проектах // Ресурсоэффективным технологиям — энергию и энтузиазм молодых: Сборник научных трудов VI Всероссийской конференции. Томск: Издательство Томского политехнического университета, 2015. С. 254–257.

²¹ A Guide to the Project Management Body of Knowledge (PMBOK Guide). 4th edition / Project Management Institute (PMI), 2008. URL: https://www.works.gov.bh/English/ourstrategy/Project%20Management/Documents/Other%20PM%20Resources/PMBOKGuideFourthEdition_protected.pdf (accessed: 30.04.2017).

²² Гага В.А., Николаенко В.С. Создание системы управления проектами в организации с применением эвристических методов // Вестник Томского государственного университета. 2013. № 374. С. 137–140.

Уровень риска. Для определения того, к какому уровню относятся негативные рисковые события, был использован подход, предложенный Т. Мерна и Ф. Ал-Хани, который распределяет риски на четыре группы²³:

- катастрофические риски (тигры) — рисковые события, которые имеют высокую вероятность наступления и способны оказать значительное влияние на успешное завершение проекта;
- незначительные риски (аллигаторы) — рисковые события, которые имеют низкую вероятность наступления, но способны оказать значительное влияние на успешное завершение проекта;
- часто встречаемые риски (щеночки) — рисковые события, которые имеют высокую вероятность наступления, но способны оказать незначительное влияние на успешное завершение проекта;
- незначительные риски (котятта) — рисковые события, которые имеют низкую вероятность наступления и способны оказывать лишь незначительное влияние на успешное завершение проекта.

Подход к классификации по уровню риска представляет определенный практический интерес для руководителей (менеджеров) проектов, т. к., понимая, к какой группе относится рисковое событие, можно мобилизовать и запланировать дополнительные ресурсы, что, в свою очередь, обеспечивает управляемость проекта²⁴.

Таблица 5. Классификация рисков согласно подходу Т. Мерна и Ф. Ал-Хани

№	Прогнозируемые риски в проекте	Тип риска
1	Будет отставание от запланированных сроков	Тигр
2	Изменятся требования в процессе реализации проекта	Тигр
3	Заказчик будет не удовлетворен сроками реализации проекта	Тигр
4	Участники проектной команды будут иметь низкую мотивацию	Щеночек
5	Менеджер сделает ошибочную оценку сроков, необходимых для реализации проекта	Тигр
6	Менеджер будет занят на других проектах	Щеночек
7	Проектная команда будет допускать ошибки при реализации проекта (<i>bugs</i>)	Щеночек
8	Участники проектной команды могут заболеть	Щеночек
9	Менеджер сделает ошибочную оценку человеческих ресурсов, необходимых для реализации проекта	Тигр
10	Будет большая временная задержка в получении ответов на задаваемые заказчику проекта вопросы	Щеночек

²³ Николаенко В.С. Превентивный риск-менеджмент в ИТ-проектах // Государственное управление. Электронный вестник. 2016. № 55. С. 76–96.

URL: http://e-journal.spa.msu.ru/vestnik/item/55_2016nikolaenko.htm (дата обращения: 30.04.2017).

²⁴ Николаенко В.С. Разработка принципов управления ИТ-проектом // Вестник Томского государственного университета. 2015. № 390. С. 155–160.

В результате проведенного исследования 12 ИТ-проектов было установлено, что в большинстве случаев классификация рисков на основании подхода, предложенного Т. Мерна и Ф. Ал-Хани, и выявленные риски, представленные в Таблице 3, коррелируют между собой (Таблица 5).

Уровень управления. Так как для 10 рисков, представленных в Таблице 3, могут быть разработаны «План А» и «План Б», то можно сделать вывод, что рисковые события являются управляемыми. Примеры мер «Плана А» и «Плана Б» представлены в Таблице 6. Подобный подход к классификации рисков представляет практический интерес для руководителей (менеджеров) проектов, т. к. для 10 типичных и часто встречаемых рисков могут быть разработаны единые стандарты мер «Плана А» и «Плана Б».

Таблица 6. Меры «Плана А» и меры «Плана Б»

№	Прогнозируемые риски в проекте	План реагирования на риск «План А»	План принятия риска «План Б»
1	Будет отставание от запланированных сроков	А) Создание временных и финансовых резервов на случай форс-мажора	А) Использование временных и финансовых резервов
2	Изменятся требования в процессе реализации проекта	А) Использование гибких методологий <i>Agile</i> ²⁵ (<i>Scrum</i> , Канбан) ²⁶	
3	Заказчик будет не удовлетворен сроками реализации проекта	А) Разработка проектной документации (устав проекта, спецификация проекта, техническое задание); Б) Привлечение заказчика к процессу разработки; В) Создание плана-графика проекта: - если <i>waterfall</i> , то составление диаграммы Ганта и сетевого графика; - если <i>Agile</i> , то составление <i>backlog</i> с указанием оценок трудозатрат на разработку. Использование <i>scrum</i> -доски; Г) Управление ожиданиями заказчика	А) Использование временных и финансовых резервов
4	Участники проектной команды будут иметь низкую мотивацию	А) Неформальное общение (совместный завтрак, обед и т. п.); Б) Создание резервной команды проекта	А) Смена команды проекта
5	Менеджер сделает ошибочную оценку сроков, необходимых для реализации проекта	А) Создание плана-графика проекта: - если <i>waterfall</i> , то составление диаграммы Ганта и сетевого графика; - если <i>Agile</i> , то составление <i>backlog</i> с указанием оценок трудозатрат на разработку. Использование <i>scrum</i> -доски Б) Согласование трудозатрат с командой проекта; В) Согласование трудозатрат со сторонними	А) Использование временных и финансовых резервов

²⁵ Manifesto for Agile Software Development [Site]. URL: <http://agilemanifesto.org> (accessed: 30.04.2017).

²⁶ Уразбаев А., Филиппов Н. Agile Checklist. Очень краткое описание практик гибкой разработки. ICAgile; ScrumTrek, 2011.

№	Прогнозируемые риски в проекте	План реагирования на риск «План А»	План принятия риска «План Б»
		экспертами; Г) Использование <i>PERT</i> ; Д) Создание временных и финансовых резервов на случай форс-мажора	
6	Менеджер будет занят на других проектах	А) Иметь базу данных соискателей, которые могут заменить менеджера проекта; Б) Создание временных и финансовых резервов на случай форс-мажора	А) Использование временных и финансовых резервов
7	Проектная команда будет допускать ошибки при реализации проекта (<i>bugs</i>)	А) Создание временных и финансовых резервов на случай форс-мажора	А) Использование временных и финансовых резервов
8	Участники проектной команды могут заболеть	А) Создание временных и финансовых резервов на случай форс-мажора	А) Использование временных и финансовых резервов
9	Менеджер сделает ошибочную оценку человеческих ресурсов, необходимых для реализации проекта	А) Создание плана-графика проекта: - если <i>waterfall</i> , то составление диаграммы Ганта и сетевого графика; - если <i>Agile</i> , то составление <i>backlog</i> с указанием оценок трудозатрат на разработку. Использование <i>scrum</i> -доски Б) Согласование трудозатрат с командой проекта; В) Согласование трудозатрат со сторонними экспертами; Г) Использование <i>PERT</i> ; Д) Создание временных и финансовых резервов на случай форс-мажора	А) Использование временных и финансовых резервов
10	Будет большая временная задержка в получении ответов на задаваемые заказчику проекта вопросы	А) Создание временных и финансовых резервов на случай форс-мажора	А) Использование временных и финансовых резервов

Внутрипроектные источники риска. Для определения внутрипроектных источников риска воспользуемся методом «Почему-почему»²⁷. Результаты анализа риска «Будет отставание от запланированных сроков» представлены в Таблице 7. Поиск внутрипроектных источников представляет практический интерес для руководителя (менеджера) проекта по следующим причинам:

1. анализ рисков методом «Почему-почему» способствует обнаружению неявных и скрытых рисков событий;
2. обнаружение источника рисков события обеспечивает управляемость проекта, т. к. позволяет разрабатывать меры «Плана А» и «Плана Б», воздействующие на причины появления риска вплоть до его нивелирования.

²⁷ Ефимов В.В. Сборник методов поиска новых идей и решений управления качеством. Ульяновск: УлГТУ, 2011.

Таблица 7. Результаты анализа рисков методом «Почему-почему»

Прогнозируемые риски в проекте	Почему	Почему	Внутрипроектный источник риска
Будет отставание от запланированных сроков	Руководитель (менеджер) проекта делает неправильную оценку трудозатрат	Руководителя (менеджера) проекта не подготовил проектную документацию приемлемого качества	Руководитель (менеджер) проекта
		У руководителя (менеджера) нет необходимых компетенций для проведения оценки трудозатрат	Руководитель (менеджер) проекта
		У руководителя (менеджера) проекта нет необходимой информации	Информация
	Форс-мажорные обстоятельства		
	Руководитель (менеджер) проекта неправильно планирует трудовые ресурсы	Руководителя (менеджера) проекта не подготовил проектную документацию приемлемого качества	Руководитель (менеджер) проекта
		У руководителя (менеджера) нет необходимых компетенций для проведения оценки трудозатрат	Руководитель (менеджер) проекта
У руководителя (менеджера) проекта нет необходимой информации		Информация	

Цели ИТ-проекта. Согласно стандарту проектного управления *Project Management Body of Knowledge (PMBOK)*, рисковые события могут оказать влияние на ключевые цели проекта (содержание, длительность, стоимость, качество). Результаты проведенного исследования рисков приведены в Таблице 8. Необходимо отметить, что наступление ряда часто встречаемых рисковых событий не оказывает прямого влияния на цели ИТ-проекта. Однако последствия от наступления данных рисков могут отразиться опосредованно, в виде увеличения сроков реализации проекта и / или увеличения стоимости проекта, а также снижения качества и / или изменения содержания планируемого ИТ-продукта²⁸. Данная классификация рисков представляет практический интерес для руководителей (менеджеров) проектов по следующим причинам:

1. Для рисков, которые оказывают прямое влияние на цели проекта, могут быть разработаны единые стандарты мер реагирования на риск («План А») и мер по ликвидации последствий от наступления рискового события («План Б»);

2. Для рисковых событий, которые не оказывают прямого влияния на цели проекта, должно быть проведено дополнительное исследование с целью обнаружения внутренних проектных источников риска, например, методом «Почему-почему»,

²⁸ Николаенко В.С. Анализ инструментария по обеспечению функции управления рисками в ИТ-проектах // Государственное управление. Электронный вестник. 2015. № 49. С. 105–120. URL: http://e-journal.spa.msu.ru/vestnik/item/49_2015nikolaenko.htm (дата обращения: 30.04.2017).

после чего могут быть разработаны единые стандарты мер реагирования на риск («План А») и мер по ликвидации последствий от наступления рисковогото события («План Б»).

Таблица 8. Анализ часто встречаемых негативных рисков согласно оказанию влияния на цели ИТ-проекта

№	Прогнозируемые риски в проекте	Влияние на цели проекта
1	Будет отставание от запланированных сроков	Длительность
2	Изменятся требования в процессе реализации проекта	Содержание
3	Заказчик будет не удовлетворен сроками реализации проекта	Длительность
4	Участники проектной команды будут иметь низкую мотивацию	Нет прямого влияния на цели проекта
5	Менеджер сделает ошибочную оценку сроков, необходимых для реализации проекта	Длительность
6	Менеджер будет занят на других проектах	Нет прямого влияния на цели проекта
7	Проектная команда будет допускать ошибки при реализации проекта (<i>bugs</i>)	Качество
8	Участники проектной команды могут заболеть	Нет прямого влияния на цели проекта
9	Менеджер сделает ошибочную оценку человеческих ресурсов, необходимых для реализации проекта	Качество
10	Будет большая временная задержка в получении ответов на задаваемые заказчику проекта вопросы	Длительность

Фаза жизненного цикла ИТ-проекта. Согласно международному стандарту проектного управления *PMBoK*, жизненный цикл проекта включает в себя следующие фазы: инициация, планирование, реализация, завершение. В этой связи риски могут быть актуальны только для определенной фазы жизненного цикла (Таблица 9). Данная классификация негативных рисковогото события представляет практический интерес для руководителей (менеджеров) проектов по следующим причинам:

1. заблаговременная мобилизация ресурсов на определенной фазе жизненного цикла для нивелирования, ослабления, переноса на третье лицо либо принятия риска;

2. высвобождение ресурсов, планируемых для использования в «Плане А» и «Плане Б», после прохождения определенной фазы жизненного цикла, что снижает предельную стоимость проекта;

3. улучшение контроля и мониторинга возможных угроз и опасностей; для улучшения контроля и мониторинга могут быть использованы графические карты, показанные на Рисунке 1.

Таблица 9. Классификация типичных и часто встречаемых рисков в ИТ-проектах по актуальности риска на этапах жизненного цикла

№	Прогнозируемые риски в проекте	Актуальность риска на этапах жизненного цикла
1	Будет отставание от запланированных сроков	Постоянный
2	Изменяются требования в процессе реализации проекта	Реализация
3	Заказчик будет не удовлетворен сроками реализации проекта	Завершение
4	Участники проектной команды будут иметь низкую мотивацию	Постоянный
5	Менеджер сделает ошибочную оценку сроков, необходимых для реализации проекта	Реализация
6	Менеджер будет занят на других проектах	Постоянный
7	Проектная команда будет допускать ошибки при реализации проекта (<i>bugs</i>)	Постоянный
8	Участники проектной команды могут заболеть	Постоянный
9	Менеджер сделает ошибочную оценку человеческих ресурсов, необходимых для реализации проекта	Реализация
10	Будет большая временная задержка в получении ответов на задаваемые заказчику проекта вопросы	Постоянный

Необходимо отметить, что для ряда рисковых событий нет жесткой привязки к определенной фазе жизненного цикла, т. к. данные риски актуальны для всех фаз жизненного цикла постоянно.

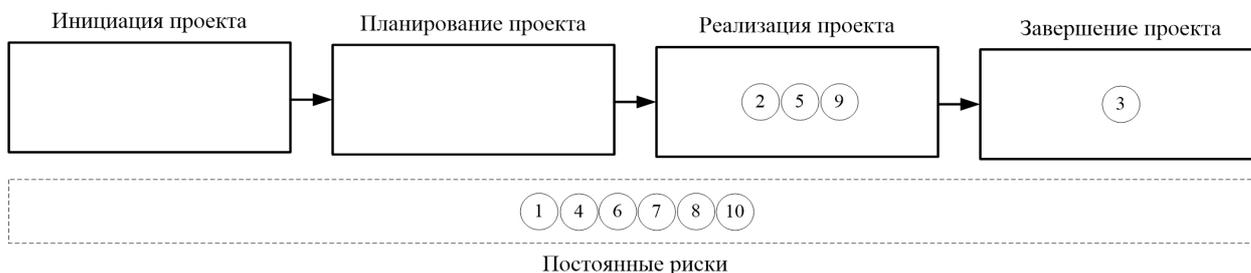


Рисунок 1. Классификация типичных и часто встречаемых рисков в ИТ-проектах по актуальности риска на этапах жизненного цикла

На основании проведенного исследования можно сделать следующие выводы:

1. существующие отечественные и зарубежные подходы не в полной мере удовлетворяют требованиям, предъявляемым к классификации рисков в ИТ-проектах;
2. для проектов, реализуемых в сфере информационных технологий, актуальны типичные и часто встречаемые рисковые события (Таблица 3);
3. разработанные подходы к классификации рисков в ИТ-проектах удовлетворяют таким требованиям, как повышение качества идентификации рисков (внутрипроектные источники риска), обеспечение управляемости проекта (уровень риска, уровень управления, внутрипроектные источники риска, цели проекта, фаза

жизненного цикла), улучшение контроля и мониторинга возможных угроз и опасностей (фаза жизненного цикла).

Таким образом, разработанные подходы к классификации рисков событий в ИТ-проектах могут представлять определенную практическую ценность для **руководителей проектов и проектных команд**, т. к. использование данных подходов позволяет увеличить шансы на успешное завершение проекта.

Список литературы:

1. Балабанов И.Т. Риск-менеджмент. М.: Финансы и статистика, 1996.
2. Волкова Ю.П., Олейникова Е.А., Филин С.А., Пирогов М.В. Инвестиционная политика современной России: Коллективная монография. М.: РЭА им. Г.В. Плеханова, 2001.
3. Гага В.А., Николаенко В.С. Создание системы управления проектами в организации с применением эвристических методов // Вестник Томского государственного университета. 2013. № 374. С. 137–140.
4. Грицаев Р.Т., Николаенко В.С. Управление рисками в проектах, реализуемых в сфере информационных технологий // Современные проблемы и тенденции развития экономики, управления и информатики в XXI веке: Сборник научных статей по материалам научно-практической конференции с международным участием / Финансовый университет при Правительстве Российской Федерации. СПб., 2015. С. 35–37.
5. Дайбова К.Е., Николаенко В.С. Разработка инструментария оперативной идентификации рисков в ИТ-проектах // Ресурсоэффективным технологиям — энергию и энтузиазм молодых: Сборник научных трудов VI Всероссийской конференции. Томск: Издательство Томского политехнического университета, 2015. С. 254–257.
6. Ефимов В.В. Сборник методов поиска новых идей и решений управления качеством. Ульяновск: УлГТУ, 2011.
7. Ехлаков Ю.П. Классификация и описание рискообразующих факторов при создании программных продуктов // Управление, вычислительная техника и информатика. 2013. № 3. С. 124–128.
8. Клейнер Г.Б. Мезоэкономика переходного периода: рынки, отрасли, предприятия. М.: Наука, 2001.

9. *Ключников В.О.* Идентификация рисков ИТ-проектов // Государственное управление. Электронный вестник. 2009. № 20. URL: http://e-journal.spa.msu.ru/vestnik/item/20_2009klyuchnikov.htm (дата обращения: 30.04.2017).
10. *Колесник Д.Н.* Практические аспекты внедрения информационных систем оценки деятельности предприятия // Системы управления бизнес-процессами. 2012. № 9. URL: <http://journal.itmane.ru/node/820> (дата обращения: 30.04.2017).
11. *Максимцов М.М., Игнатьева А.В., Комаров М.А.* и др. Менеджмент. М.: ЮНИТИ, 1998.
12. *Николаенко В.С.* Анализ инструментария по обеспечению функции управления рисками в ИТ-проектах // Государственное управление. Электронный вестник. 2015. № 49. С. 105–120. URL: http://e-journal.spa.msu.ru/vestnik/item/49_2015nikolaenko.htm (дата обращения: 30.04.2017).
13. *Николаенко В.С.* Внедрение риск-менеджмента в ИТ-проекты // Государственное управление. Электронный вестник. 2016. № 54. С. 63–88. URL: http://e-journal.spa.msu.ru/vestnik/item/54_2016nikolaenko.htm (дата обращения: 30.04.2017).
14. *Николаенко В.С.* Превентивный риск-менеджмент в ИТ-проектах // Государственное управление. Электронный вестник. 2016. № 55. С. 76–96. URL: http://e-journal.spa.msu.ru/vestnik/item/55_2016nikolaenko.htm (дата обращения: 30.04.2017).
15. *Николаенко В.С.* Разработка принципов управления ИТ-проектом // Вестник Томского государственного университета. 2015. № 390. С. 155–160.
16. *Никулина И.Е., Тухватулина Л.Р., Черепанова Н.В.* Основы современного менеджмента. Томск: Издательство Томского политехнического университета, 2009.
17. Официальный сайт ООО «Аксимедия Софт». URL: <http://www.aximeditasoft.com> (дата обращения: 30.04.2017).
18. Официальный сайт ООО «Контек Софт». URL: <http://www.contek.ru/> (дата обращения: 30.04.2017).
19. Официальный сайт ООО «ЛидерГрупп». URL: <http://www.lunacharsky.ru> (дата обращения: 30.04.2017).
20. Официальный сайт ООО «СИС». URL: <http://oosis.com/promo> (дата обращения: 30.04.2017).
21. Официальный сайт ООО «Спейс-О технологии». URL: <http://www.spaceotechnologies.com> (дата обращения: 30.04.2017).

22. Селиховкин И. Управление ИТ-проектом. Эффективная система «с нуля» в любой организации. СПб., 2010. URL: <http://www.lessonslearned.ru/sites/default/files/ITPM-Selikhovkin.pdf> (дата обращения: 30.04.2017).
23. Соколов Д.В. Классификация рисков, как многозадачный инструмент риск-менеджмента организации // Управление экономическими системами: электронный научный журнал. 2011. № 30. URL: <http://uecs.ru/uecs30-302011/item/489-> (дата обращения: 30.04.2017).
24. Уразбаев А., Филиппов Н. Agile Checklist. Очень краткое описание практик гибкой разработки. ICAgile; ScrumTrek, 2011.
25. Филлин С. Неопределенность — от недостатка информации // РИСК. 2000. № 2-3. С. 62–67.
26. A Guide to the Project Management Body of Knowledge (PMBOK Guide). 4th edition / Project Management Institute (PMI), 2008. URL: https://www.works.gov.bh/English/ourstrategy/Project%20Management/Documents/Other%20PM%20Resources/PMBOKGuideFourthEdition_protected.pdf (accessed: 30.04.2017).
27. Ching Gu V., Hoffman J.J., Cao Q., Schniederjans M.J. The Effects of Organizational Culture and Environmental Pressures on IT Project Performance: A Moderation Perspective // International Journal of Project Management. 2014. No 32. P. 1170–1181.
28. ISO/IEC 31010:2009 “Risk management — Risk assessment techniques” (ИСО/МЭК 31010:2009 «Менеджмент риска. Методы оценки риска»).
29. Manifesto for Agile Software Development [Site]. URL: <http://agilemanifesto.org> (accessed: 30.04.2017).
30. Merna T., Al-Thani F. Corporate Risk Management. 2nd ed. Chichester, UK; Hoboken, N.J.: John Wiley & Sons, Ltd, 2008.
31. Nikolaenko V.S., Petuhov O.N., Petukhova O.V., Romanovsky V.V. Special Aspects of Risk Management in IT-Projects // The 28th International Business Information Management Accusation Conference 2016 (IBIMA), 2017. P. 241–260.
32. The CHAOS Manifesto / The Standish Group International, 2014.

Nikolaenko V.S.

Development of Approaches to Risk Classification in IT-projects

Valentin S. Nikolaenko — Teaching Assistant, Tomsk Polytechnic University, Tomsk, Russian Federation.

E-mail: nikolaenkovs@tpu.ru

Annotation

The article discusses the results of an analysis of the existing domestic and foreign approaches to risk classification in IT-projects. The article also presents the typical and commonly encountered adverse risks obtained in the course of the study of the 12 IT-projects implemented in 5 IT-organizations, and their subsequent verification using the author's approach to risk classification. The results of the study will be of interest to projects managers and project teams, as this approach to risk classification improves the quality of risk identification, software project manageability, threat control and monitoring.

Keywords

Risk, risk classification, risk management, risk management, IT-project.