Николаенко В.С.

Внедрение риск-менеджмента в ИТ-проекты

Николаенко Валентин Сергеевич — ассистент, Томский политехнический университет; аспирант, Томский государственный университет, Томск, РФ.
E-mail: nikolaenkovs@tpu.ru
SPIN-код РИНЦ: 9301-1835

Аннотация
В статье описаны основные аспекты внедрения риск-менеджмента в ИТ-проекты согласно разработанному организационно-методическому обеспечению. Оно устраняет противоречие, возникающее между требованиями, предъявляемыми к риск-менеджменту. Суть противоречия заключается в следующем: риск-менеджмент должен обеспечивать максимальное соответствие фактических и запланированных результатов, с допустимым отклонением не более 5%. При этом риск-менеджмент не должен менять существующее управление в ИТ-проектах (процессы *Waterfall, Agile* и т. п.). В статье описаны адаптированные методы и подходы, учитывающие специфику сферы информационных технологий, а также представлены результаты экспериментального внедрения риск-менеджмента в ИТ-проект. Отклонение факта от плана по итогам завершения ИТ-проекта составило 4,5%.

Ключевые слова
Риск, управление рисками, ИТ-проект, организационно-методическое обеспечение.

Проекты, реализуемые в сфере информационных технологий (далее — ИТ-проекты) представляют собой сложный комплекс научных, инженерных и технологических дисциплин, требующих длительного обучения, больших инвестиционных затрат, наукоемкой техники, опытных специалистов. Сложность реализации ИТ-проектов создает зоны риска, что приводит к уменьшению количества успешных ИТ-проектов, где фактические результаты должны быть равны запланированным[1].

Анализ статистических данных, представленных в Таблице 1, выявил актуальную проблему, которая связана с наступлением событий, способных оказать значительное негативное влияние на цели ИТ-проектов (длительность, стоимость, качество).

Таблица 1. Результаты реализованных ИТ-проектов в США (60%), в европейских (25%) и в других странах (15%) с 2004 по 2014 год[1]

	2004	2006	2008	2010	2012	2013	2014
Успешные проекты	29%	35%	32%	37%	39%	25%	16,2%
Незавершенные проекты	18%	19%	24%	21%	18%	25%	31,1%
Проекты, в которых проблемы повлекли изменение запланированных целей	53%	46%	44%	42%	43%	50%	52,7%

[1] CHAOS Manifesto 2014 / The Standish Group International, 2014. P. 16.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

ИТ-организация подвергается влиянию разнообразных факторов, порождаемых как внешней, так и внутренней средой[2]. Так, в своей работе О. Ли и Д. Бэби подтверждают это результатами проведенных исследований. Ученые приходят к выводу, что факторы внешней (природные факторы, бизнес-окружение) и внутренней (люди, технологии) среды являются главными источниками неопределенности, увеличивающими вероятность финансовых и других потерь[3]. Это означает, что потенциальные угрозы могут одновременно исходить как от эндогенной, так и от экзогенной среды[4]. Например, негативными рисками экзогенной среды могут быть угрозы, связанные с неправильно запланированным бюджетом, отсутствием профессиональных кадров и т. п.[5] К негативным рискам эндогенной среды могут быть отнесены опасности, связанные с колебанием валютных рынков, изменения в налоговом законодательстве, политические и экономические отношения между странами[6].

В настоящей статье под «риском» будет пониматься вероятное событие, которое может оказать как негативное, так и позитивное влияние на успешное завершение ИТ-проекта[7].

В результате проведенного анализа научных трудов, опубликованных по теме управления рисками, было установлено, что учеными в большей степени рассматриваются общие риски, которые не отражают особенности и специфику области информационных технологий. Причем риск в большинстве трудов трактуется только с негативной точки зрения. В этой связи многие специалисты-практики, руководители ИТ-организаций и менеджеры ИТ-проектов отказываются от использования риск-менеджмента, так как существующие способы управления рисками и их внедрение значительно усложняет процесс управления ИТ-проектами.

---

[2] *Никулина И.Е., Тухватулина Л.Р., Черепанова Н.В.* Основы современного менеджмента. Томск: Изд-во Томского политехнического университета, 2009.

[3] *Lee O.-K. D., Baby D.V.* Managing Dynamic Risks in Global IT Projects: Agile Risk-management Using the Principles of Service-oriented Architecture // International Journal of Information Technology & Decision Making. 2013. Vol. 12. No 6. P. 1121–1150.

[4] *De Bakker K., Boonstra A., Wortmann H.* Does Risk Management Contribute to IT Project Success? A Meta-Analysis of Empirical Evidence // International Journal of Project Management. 2010. No 28. P. 1–23.

[5] *Стрелец И.А.* Сетевая экономика: учебник. М.: Эксмо, 2006.

[6] *Petukhov O.N., Nikolaenko V.S.* Network Projects As a New Paradigm in e-Learning // International Multidisciplinary Scientific Conferences on Social Sciences and Arts, SGEM 2014. September 1-9, 2014. Book 1 Vol. 3. P. 579-586. URL: http://sgemsocial.org/ssgemlib/spip.php?article460 (accessed: 05.02.2016).

[7] *Николаенко В.С.* Разработка принципов управления ИТ-проектом // Вестник Томского государственного университета. 2015. № 390. С. 155−160.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

В связи с этим **целью статьи** является разрешение противоречия, которое возникает между требованиями, предъявляемыми к риск-менеджменту в ИТ-проектах, а именно:

- внедрение риск-менеджмента не должно менять существующее и устоявшееся управление в ИТ-проекте, то есть управление в проекте должно оставаться неизменным независимо от методологии реализации ИТ-проекта и независимо от используемой модели жизненного цикла (*Waterfall, Agile* и т. п.);
- внедрение риск-менеджмента в ИТ-проект должно способствовать минимальному отклонению фактических результатов от запланированных (не более 5%).

Согласно статистическим данным, представленным в отчетах *The Standish Group International* в 2014 году, среднее отклонение от запланированных бюджетов, сроков выполнения и качества в ИТ-проектах, разрабатываемых в основном в США и в европейских странах, составило 89%[8].

Данное противоречие было устранено путем решения следующих **задач**:

1) анализа методов, используемых для выполнения основных процедур риск-менеджмента (Рисунок 1);

2) разработки организационно-методического обеспечения по внедрению риск-менеджмента в ИТ-проекты;

3) экспериментальной апробации разработанного организационно-методического обеспечения по внедрению риск-менеджмента в ИТ-проекты. Ее результаты показали, что отклонение фактических результатов от запланированных составило 4,5%, то есть перерасход ресурсов по сравнению со средним отклонением 89% был уменьшен в 19 раз.

Рассмотрим решение каждой задачи подробнее.

Разработка организационно-методического обеспечения процесса внедрения риск-менеджмента в ИТ-проектах требует создания комплексного подхода и создания эффективного риск-менеджмента, с помощью которого менеджер ИТ-проекта сможет оперативно идентифицировать, анализировать, контролировать рисковые события и реагировать на них. Таким образом, решение поставленных задач требует анализа и

[8] CHAOS Manifesto 2014 / The Standish Group International, 2014. P. 16.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

адаптации эвристических методов (методов, позволяющих находить идеальное решение) для каждой процедуры риск-менеджмента[9].

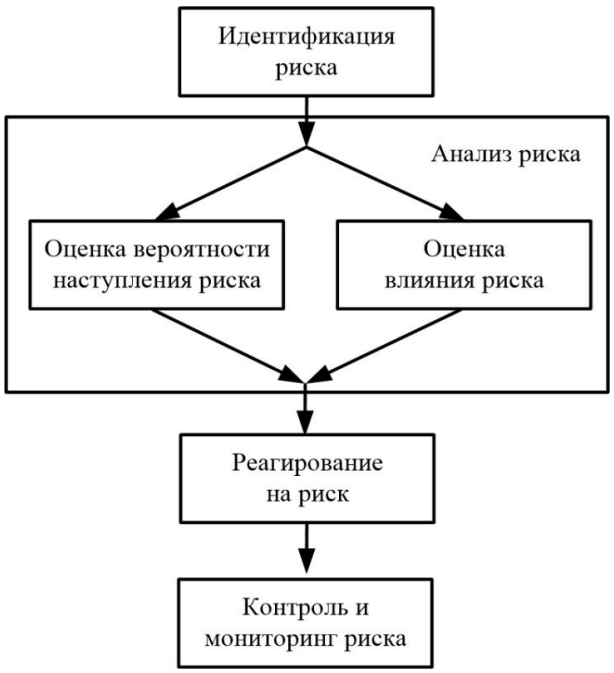

Рисунок 1. Основные процедуры риск-менеджмента

Идентификация рисков ИТ-проекта. Для идентификации рисков в ИТ-проектах автором статьи предлагается последовательно выполнить следующие действия:

1) проанализировать проектную документацию, что позволит выявить риски, связанные с планируемыми результатами, сроками, бюджетом, предъявляемыми требованиями и т. п., а также идентифицировать риски, которые ранее реализовались в других ИТ-проектах;

2) применить метод «блок-схема принятия решения» (*Process Decision Program Chart, PDPC*)[10];

3) использовать опросные листы[11];

4) применить метод «мозговой штурм», усиливая его инновационной игрой *Speed Boat*[12]. В качестве участников «мозгового штурма» рекомендуется задействовать

---

[9] *Краковецкая И.В., Николаенко В.С.* Активация творческого потенциала персонала с помощью эвристических методов при разработке сайта // Креативная экономика. 2013. № 10 (82). С. 37–43.

[10] *Ефимов В.В.* Сборник методов поиска новых идей и решений управления качеством. Ульяновск: УлГТУ, 2011.

[11] *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: Изд-во Томского политехнического университета, 2015. С. 254–257.

[12] Innovation games [Site]. URL: http://www.innovationgames.com/speed-boat (accessed: 05.02.2016).

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

полный состав проектной команды, включая менеджера ИТ-проекта и приглашенных экспертов[13];

5) использовать метод *SWOT*-анализ (*Strengths, Weaknesses, Opportunities, Threats*). Использование данного метода дает возможность одновременно идентифицировать как негативные, так и позитивные рисковые события;

6) провести интервью с экспертами, имеющими опыт реализации аналогичных ИТ-проектов.

Анализ рисков ИТ-проекта. Процедуру анализа предлагается проводить с помощью качественных (экспертных) методов оценки вероятности проявления и влияния рисковых событий вследствие следующих факторов:

- ограниченного времени, отводимого на этап планирования в реальных производственных условиях, тогда как использование количественных методов — это процесс, требующий значительных трудозатрат, временн*ы*х ресурсов, а также соответствующих знаний, умений и навыков у менеджера ИТ-проекта;
- применения *KISS* (*Keep it Short and Simple*) — способа проектирования и разработки ИТ-проектов, при котором простота формулировок декларируется как основная ценность проектной реализации (методы количественной оценки рисков требуют значительной формализации процессов);
- использования основных подходов гибкой разработки, перечисленных в манифесте разработки программного обеспечения *Agile Manifesto*[14]. *Agile* устанавливает приоритеты, согласно которым люди и их взаимодействие важнее, чем процессы и инструменты. Следовательно, применение качественных методов во всех процедурах управления рисками способствует росту взаимодействия, доверия и коммуникации между участниками проектной команды;
- каждый реализуемый ИТ-проект является уникальным, согласно определению проекта, что ограничивает возможность применения информационных данных, полученных от предыдущих ИТ-проектов[15];
- сложность и трудоемкость использования количественных методов для малых проектов (длительность разработки не более двух месяцев) не является целесообразным;

---

[13] *Николаенко В.С.* Пути активизации творческого потенциала проектной команды с помощью эвристических методов // Креативная экономика. 2014. № 01 (85). С. 18−25.
[14] Manifesto for Agile Software Development [Site]. URL: http://agilemanifesto.org (accessed: 05.02.2016).
[15] *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.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

- итеративная реализация ИТ-проекта требует быстрого и гибкого процесса исполнения всех основных процедур управления рисками.

В этой связи для оценки ущерба от проявления негативных рисков или возможного положительного эффекта от проявления позитивных рисков предлагается использовать следующие эвристические методы:

- «галстук-бабочка» — первый этап (*Bow-tie*)[16]. Отметим, что метод «галстук-бабочка» консолидирует особенности методов «дерево событий» (*Event Tree Analysis, ETA*) и «дерево неисправностей» (*Fault Tree Analysis, FTA*)[17];
- причинно-следственная диаграмма Исикавы (*Fishbone Diagram*)[18];
- интервью[19].

Рассмотрим процесс адаптации каждого из вышеперечисленных методов с учетом специфики реализации ИТ-проектов.

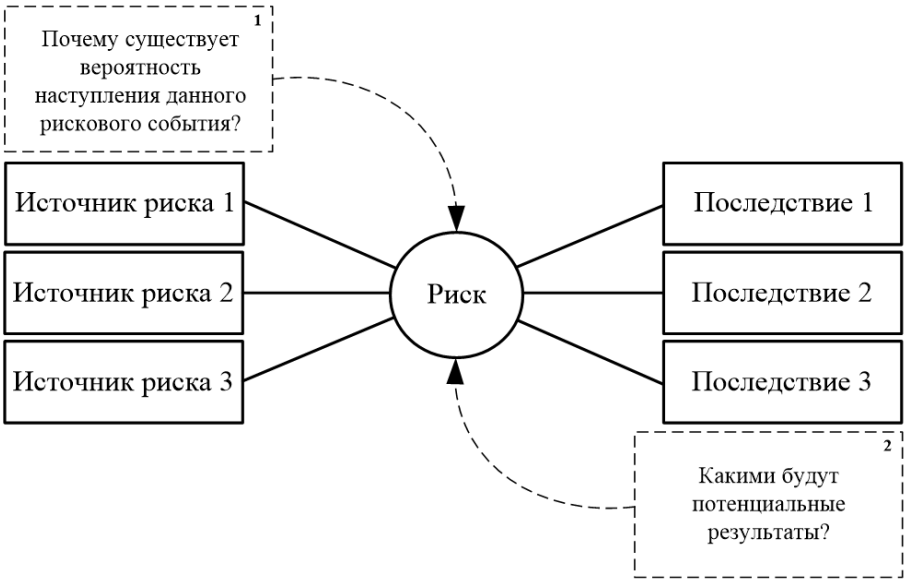

Рисунок 2. Метод «галстук-бабочка» — первый этап[16]

В алгоритме метода «галстук-бабочка» выделяют два основных этапа. На первом этапе проводится анализ риска путем определения основных источников рискового события и установления последствий в случае его наступления (Рисунок 2).

---

[16] *Lewis S., Smith K.* Lessons Learned from Real World Application of the Bow-tie Method / Prepared for Presentation at American Institute of Chemical Engineers 2010 Spring Meeting 6th Global Congress on Process Safety San Antonio, Texas, March 22–24, 2010. Unpublished.
[17] ISO/IEC 31010:2009. Risk management — Risk assessment techniques.
URL: http://www.iso.org/iso/catalogue_detail?csnumber=51073 (accessed: 13.03.2015).
[18] *Ishikawa K.* Guide to Quality Control. Tokyo: Asian Productivity Organization, 1986.
[19] *ДеМарко Т.* Вальсируя с медведями: управление рисками в проектах по разработке программного обеспечения. М.: Компания p.m.Office, 2005.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Подобные действия позволяют менеджеру ИТ-проекта и проектной команде выявлять основные первопричины, порождающие рисковое событие, а также прогнозировать различные сценарии развития ИТ-проекта.

Для идентификации причин и источников негативных рисков предлагается использовать метод «причинно-следственная диаграмма Исикавы» (Рисунок 3). Классический алгоритм применения диаграммы Исикавы включает комплексный анализ проблемы с помощью следующих основных групп:

- персонал — причиной возникновения проблемы является «человеческий фактор»;
- оборудование — причиной возникновения проблемы является используемое оборудование, машины, программное обеспечение и т. п.;
- материалы — причиной возникновения проблемы является используемое сырье;
- внешняя среда — причиной возникновения проблемы является экзогенная среда;
- контроль — причиной возникновения проблемы является некачественная система управления, обеспечивающая контроль;
- технология — причиной возникновения проблемы является технологический процесс.

Классический алгоритм использования причинно-следственной диаграммы Исикавы не в полной мере соответствует требованиям, предъявляемым к процедуре анализа рисков в ИТ-проектах[20]. Например, в процессе реализации ИТ-проектов отсутствует группа «производственное сырье». Однако комплексное исследование рисковых событий требует включения группы, отвечающей за информацию, так как информационные данные являются основным материалом, использующимся при разработке ИТ-продуктов. Таким образом, адаптированный метод «диаграмма Исикавы» будет включать в себя следующие группы:

- персонал — причиной возникновения риска являются участники проектной команды. Источниками рисковых событий могут быть отсутствие необходимых профессиональных навыков или опыта, низкий уровень коммуникации и доверия между участниками, конфликты и т. п.;

[20] *Youssef Z., Mohamed O.* Applying Ishikawa Approach for Modeling ERP Risk-effects // Journal of Theoretical and Applied Information Technology. 2015. Vol. 1. No 1. P. 51−60.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

- оборудование — причиной возникновения риска является, например, используемое программное обеспечение, поломка сервера, отсутствие интернета и т. п.;
- информация — причиной возникновения риска является, в частности, отсутствие проектной документации, необходимой для разработки ИТ-продукта и т. п.;
- внешняя среда — причиной возникновения риска является внешняя среда ИТ-проекта, к которой относятся организация, где реализуется проект, а также субподрядчики и т. п.;
- контроль — причиной возникновения риска является стиль управления менеджера ИТ-проекта (демократический, авторитарный, либеральный);
- технология — причиной возникновения риска является используемая в реализации ИТ-проекта модель жизненного цикла: каскадная модель, V-образная модель, инкрементная модель, спиральная модель, модель быстрой разработки приложений *RAD, Agile.*

Пример графического представления адаптированной диаграммы Исикавы показан на Рисунке 3.

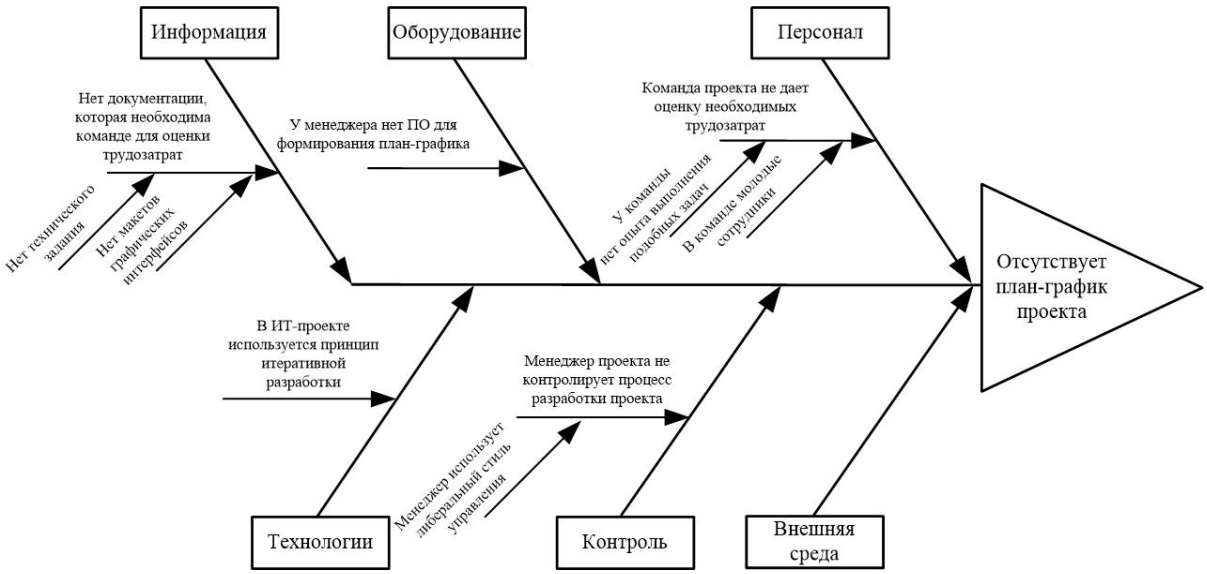

Рисунок 3. Пример адаптированной диаграммы Исикавы для ИТ-проектов[19]

Во время использования методов «галстук-бабочка» и «диаграмма Исикавы» могут быть идентифицированы новые риски.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Для увеличения качества экспертной оценки автор статьи рекомендует использовать вес участников проектной команды (Таблица 2), формулу 1 и вербально-числовую шкалу Харрингтона (Таблица 3, Таблица 4)[21].

$$x = \frac{\sum_{i=1}^{n} x_i k_i}{n}, \qquad (1)$$

где x_i — это оценка вероятности (влияния), данная участником проекта; n — количество участников проекта; k_i — вес участника в проекте.

Таблица 2. Вес участников в ИТ-проекте

Роль в проекте	Опыт работы сотрудника в данной роли более года	Компетенции (образование, повышение квалификации)	Итого, k
Менеджер проекта	0,5	0,5	1
Эксперт	0,5	0,4	0,9
Разработчик	0,5	0,4	0,9
Аналитик	0,5	0,4	0,9
Верстальщик	0,5	0,2	0,7
Проектировщик / дизайнер	0,5	0,4	0,9
Тестировщик	0,5	0,3	0,8
Заказчик	0,4	0,1	0,5

Таблица 3. Вербально-числовая шкала Харрингтона для качественной оценки степени влияния

Степень влияния риска на проект	Коэффициент Харрингтона (согласно PMBoK)	Коэффициент Харрингтона	Ущерб
Очень высокая	0,8-1,0	5	Работы в проекте остановлены
Высокая	0,64-0,8	4	Работы в проекте выполнены с большим опозданием
Средняя	0,37-0,64	3	Есть задержка в выполнении работ
Низкая	0,2-0,37	2	Работы в проекте выполнены с небольшим опозданием
Очень низкая	0,0-0,2	1	Есть незначительные отставания от намеченных планов
Нет влияния	0,0	0	Работы в проекте полностью выполняются с намеченным планом

[21] *Николаенко В.С.* Анализ инструментария по обеспечению функции управления рисками в ИТ-проектах // Государственный управление. Электронный вестник. 2015. № 49. С. 105−120. URL: http://e-journal.spa.msu.ru/vestnik/item/49_2015nikolaenko.htm (дата обращения: 12.02.2016).

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Таблица 4. Вербально-числовая шкала Харрингтона для качественной оценки степени влияния

Степень вероятности наступления риска в проекте	Коэффициент Харрингтона (согласно PMBoK)	Коэффициент Харрингтона	Вероятность
Очень высокая	0,8-1,0	5	Риск неизбежен. Гарантированное наступление риска
Высокая	0,64-0,8	4	Риск вероятен
Средняя	0,37-0,64	3	Нет гарантий, что риск наступит, но все же существует такая возможность
Низкая	0,2-0,37	2	Есть возможность наступления риска
Очень низкая	0,0-0,2	1	Есть потенциальная возможность наступления риска
Нет вероятности	0,0	0	Риск невозможен

Полученные результаты предлагается визуализировать с помощью матрицы вероятности проявления и влияния для негативных и позитивных рисков, показанных на Рисунках 4 и 5.

Рисунок 4. Матрица вероятности проявления и влияния Т. Мерны и Ф. Тхани для негативных рисков[22]

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

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Согласно классификации Т. Мерны и Ф. Тхани (*T. Merna, F. Al-Thani)* негативные риски могут быть распределены по следующим категориям:

- катастрофические риски («тигры») — это риски, которые имеют высокую вероятность наступления и способность оказывать значительное негативное влияние на ИТ-проект. Наступление одного катастрофического риска приводит к остановке всего проекта;
- непредсказуемые риски («аллигаторы») — это риски, которые имеют низкую вероятность наступления, но обладают способностью оказывать значительное негативное влияние на ИТ-проект;
- часто встречающиеся риски («щенки») — это риски, которые имеют высокую вероятность наступления, но при этом не способны оказывать значительное влияние на ИТ-проект;
- несущественные риски («котята») — это риски, которые имеют низкую вероятность наступления и не обладают способностью оказывать значительное влияние на ИТ-проект. Подобными рисками менеджер проекта может пренебречь и не разрабатывать меры реагирования.

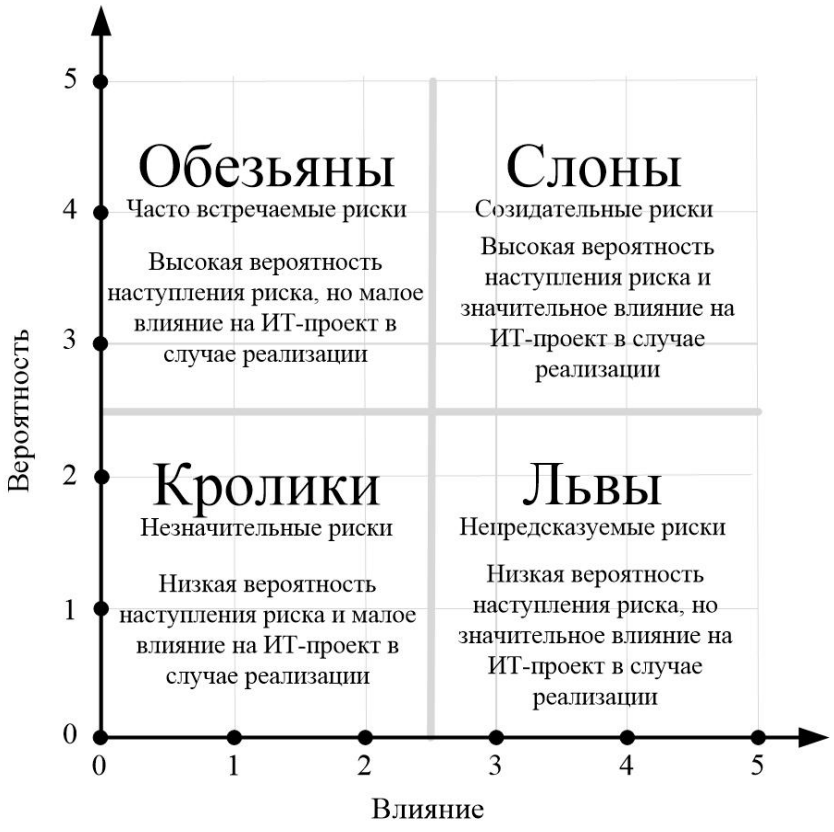

Рисунок 5. Матрица вероятности проявления и влияния для позитивных рисков

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Для выявления наиболее катастрофических негативных рисков в ИТ-проектах ранжирование, предложенное Т. Мерной и Ф. Тхани, является оптимальным, потому что позволяет установить приоритет между всеми негативными рисками. Так, в первую очередь необходимо работать с рисками, которые относятся к категории «тигры», затем с «аллигаторами» и «щенками». Рисками, которые относятся к категории «котята», менеджер ИТ-проекта может пренебречь.

Несмотря на удобство использования данной классификации, Мерна и Тхани не предлагают ранжирование для позитивных рисков. В этой связи автор статьи предлагает классифицировать позитивные риски, используя следующие категории (Рисунок 5):

- созидательные риски («слоны») — это риски, которые имеют высокую вероятность наступления и способность оказывать значительное позитивное влияние на ИТ-проект;
- непредсказуемые риски («львы») — это риски, которые имеют низкую вероятность наступления, но обладают способностью оказывать значительное позитивное влияние на ИТ-проект;
- часто встречаемые риски («обезьяны») — это риски, которые имеют высокую вероятность наступления, но при этом не способны оказывать значительное позитивное влияние на ИТ-проект
- незначительные риски («кролики») — это риски, которые имеют низкую вероятность наступления и не обладают способностью оказывать значительное позитивное влияние на ИТ-проект. Незначительными рисками менеджер ИТ-проекта может пренебречь и не разрабатывать меры по реагированию на них.

Использование матрицы вероятности проявления и влияния для позитивных рисков дает возможность установить приоритетные позитивные рисковые события. В первую очередь необходимо работать с рисками, которые относятся к категории «львы», так как они могут оказать значительный позитивный эффект на ИТ-проект. Затем необходимо работать с рисками, которые относятся к категории «обезьяны». Рисками типа «слоны» и «кролики» менеджер ИТ-проекта может пренебречь, потому что созидательные риски гарантированно наступят в процессе реализации проекта, а незначительные риски не окажут существенного позитивного влияния.

Разработку креативных мероприятий по реагированию на риски предлагается проводить с помощью:

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

- метода «галстук-бабочка» — второй этап;
- метода Уолта Диснея;
- метода «разделение мышления де Боно» (*Six Thinking Hats*)[23];
- метода «мозговой штурм»;
- метода Дельфи.

Причем для разных категорий негативных и позитивных рисков предлагается использовать различные эвристические методы. Например, для рисков, которые были классифицированы как катастрофические, предлагается использовать методы, выявляющие причины возникновения риска, возможные последствия и связи с другими рисками. Подобный детальный анализ катастрофических рисков дает возможность экспертам оценивать их комплексно и более точно определять возможный уровень вероятности проявления и влияния.

В реальных производственных условиях менеджер ИТ-проекта не имеет достаточных ресурсов для обеспечения качественного управления всеми идентифицированными негативными и позитивными рисками. Таким образом, установка приоритетов между различными категориями рисков дает возможность менеджеру ИТ-проекта и проектной команде сконцентрировать ограниченные ресурсы на управление наиболее существенными рисками. Прежде всего необходимо разрабатывать меры «плана А», триггеры и меры «плана Б» для негативных рисков, которые были определены как катастрофические («тигры»). Далее исследуются риски, попавшие в категории непредсказуемых («аллигаторы») и часто встречающихся («щенки»). Самый низкий приоритет у негативных рисков, определенных как незначительные («котята»).

В этой связи для управления рисками с высоким приоритетом («тигры» и «львы») предлагается разработать:

- «план реагирования на риск», или «план А», — план превентивных мер по нивелированию, ослаблению, переносу, принятию для негативных рисков, а также использованию, усилению, разделению, принятию — для позитивных;
- триггеры — показатели наступления риска, то есть признаки, по которым ответственный за риск может понять, что превентивные меры «плана А» не принесли ожидаемого эффекта;

[23] *De Bono E.* Six Thinking Hats. New York: Little, Brown Book Group Limited, 1985.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

- «план отступления», или «план Б», — план мер, который предусматривает действия в случае наступления рискового события.

Для рисков, которые относятся к категориям «аллигаторы», «щенки», «обезьяны», будет достаточно разработки креативных мер «плана А» и триггеров. Рисками же категорий «котята», «слоны» и «кролики» можно будет пренебречь.

Далее рассмотрим адаптацию эвристических методов для разработки креативных мер реагирования на риски для каждой категории более подробно.

Катастрофические риски («тигры»). Так как катастрофические риски оказывают значительное влияние на успешное завершение ИТ-проекта, реализация одного риска типа «тигры» приводит к остановке проекта, поэтому разработку креативных мероприятий «плана А», «плана Б» и триггеров предлагается проводить с использованием:

- метода «галстук-бабочка» — второй этап (Рисунок 6);
- метода Уолта Диснея;
- метода разделения мышления де Боно (*Six Thinking Hats*);
- метода Дельфи, усиленного интервью.

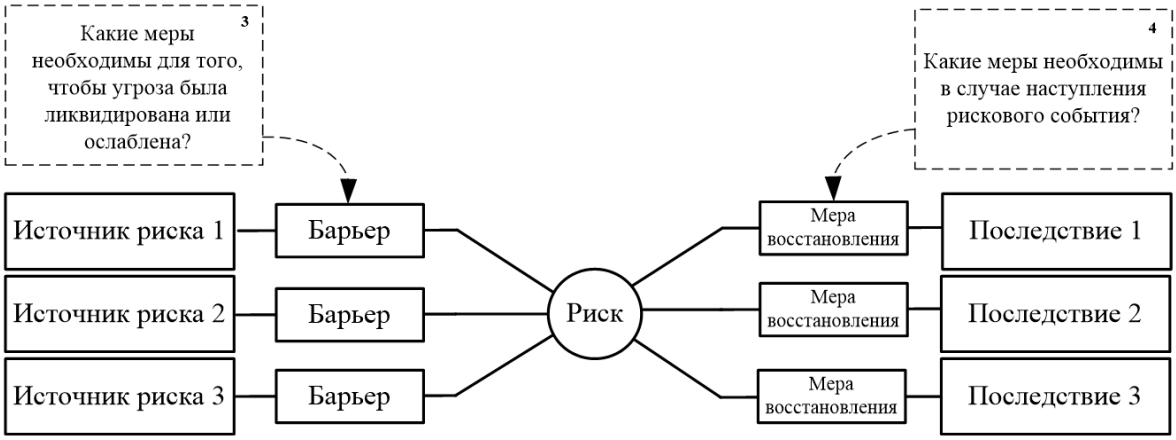

Рисунок 6. Метод «галстук-бабочка» — второй этап[16]

На втором этапе метода «галстук-бабочка» менеджер ИТ-проекта и проектная команда разрабатывают «барьеры» (мероприятия «плана А») и «меры восстановления» (мероприятия «плана Б»). Согласно правилам использования метода, идентифицированные источники риска на первом этапе дают возможность оперативно разработать «барьеры», которые позволят нивелировать, ослабить или перенести риск. Формализованные же последствия в случае наступления риска позволяют менеджеру ИТ-проекта и проектной команде разработать эффективные мероприятия по

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

ликвидации негативных эффектов. Метод «галстук-бабочка» также дает возможность создать триггеры, которые заблаговременно будут сигнализировать о скором наступлении рискового события и о том, что меры «плана А» не принесли ожидаемого положительного эффекта.

Если разработанные мероприятия «плана А» и «плана Б» превысили установленную предельную стоимость мероприятий риск-менеджмента, тогда могут быть использованы метод Уолта Диснея или метод разделения мышления де Боно.

Суть метода Уолта Диснея заключается в жестком разделении направлений мышления участников проектной команды. Так, на этапе «Фантазер» участники проектной команды предлагают различные идеи, в том числе и фантастические, которые могут нивелировать катастрофический риск. Метод Диснея будет более продуктивен в случае привлечения сторонних экспертов, не входящих в состав команды ИТ-проекта. Высказанные ими идеи могут стать основой для разработки более креативных мероприятий. На этапе «Критик» каждое из предложенных мероприятий участники проектной команды подвергают критической оценке и приводят аргументы, обосновывающие неэффективность данных мер. Этап «Реалист» включает в себя проведение оценки предложенных мероприятий, а этап «Исполнитель» — принятие управленческого решения о том, для каких мероприятий необходимо готовить ресурсы.

Метод Уолта Диснея рекомендуется использовать при ограниченных временн*ы*х ресурсах, поскольку четыре основных этапа позволяют оперативно разрабатывать креативные мероприятия «плана А» и «плана Б». Если же менеджер ИТ-проекта и проектная команда располагают большим временн*ы*м ресурсом, то вместо метода Диснея может быть использован метод разделения мышления де Боно.

Суть метода «Разделение мышления де Боно», так же как и метода Уолта Диснея, связана с разделением направления мышления, однако в методе де Боно выделяют следующие этапы:

- этап II («Красная шляпа») — этап, на котором участники проектной команды могут выразить свое эмоциональное отношение к предложенному креативному мероприятию, не прибегая к логике или аргументированным ответам. Данный этап может быть использован в качестве фильтра, благодаря которому участники проектной команды будут работать только с теми решениями, которые им понравились;

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

- этап III («Желтая шляпа») — этап, на котором участники проектной команды высказывают только положительные аргументы в пользу предложенных мероприятий;
- этап V («Белая шляпа») — этап, на котором участники проектной команды используют в качестве аргументов только цифры и факты. Также на этом этапе принимается окончательное управленческое решение относительно того, какие мероприятия необходимо включить в план реагирования на риски;
- «Синяя шляпа». Эдвард де Боно эмпирически установил, что метод разделения мышления работает более результативно, если в проектной команде есть специалист, который независимо от этапов метода выполняет следующие функции: фиксирует результаты, предложенные командой; стимулирует творческий потенциал команды; отвечает за строгое соблюдение алгоритма метода.

Использование метода Дельфи также может помочь в поиске креативных мероприятий «плана А» и «плана Б». Указанный метод может быть использован как в классическом варианте, то есть посредством коммуникаций с экспертами через электронную почту, так и будучи усиленным методом «интервью», то есть проведением интервью с приглашенными экспертами.

Для **непредсказуемых рисков («аллигаторов»)** автор статьи предлагает использовать метод «галстук-бабочка» — второй этап и метод Уолта Диснея.

Разработка мероприятий по реагированию на **часто встречающиеся риски («щенки»)**, не оказывающие значительного негативного влияния на успешное завершение ИТ-проекта, может быть осуществлена методом «галстук-бабочка» — второй этап.

Незначительными рисками («котятами») менеджер ИТ-проекта может пренебречь. Однако для разработки профилактических мероприятий (в случае если мероприятия «плана А» и «плана Б» не превысили предельную стоимость мероприятий реагирования риск-менеджмента) предлагается использовать метод «мозговой штурм», при котором респондентами могут быть менеджеры других ИТ-проектов, старшие разработчики, старшие специалисты по тестированию, старшие аналитики и т. п.

Созидательные риски («слоны»). Данными позитивными рисками менеджер ИТ-проекта и проектная команда может пренебречь. Однако для гарантированного наступления позитивного рискового события категории «слоны» участниками

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

проектной команды все же могут быть разработаны профилактические мероприятия с помощью метода «мозговой штурм».

Разработка мероприятий для **непредсказуемых рисков («львов»)** может быть осуществлена с помощью метода «галстук-бабочка» — второй этап, метода Уолта Диснея и метода Дельфи.

Согласно правилам использования, метод «галстук-бабочка» ориентирован на разработку мероприятий «плана А» и «плана Б» для негативных рисков, которые представляют угрозу для успешного завершения ИТ-проекта. В этой связи автором статьи предлагается адаптировать второй этап метода разработки мер реагирования для позитивных рисков путем изменения смыслов ключевых понятий метода, то есть понятие «барьер» должно быть заменено на понятие «стимулирующая мера», а «мера восстановления» — на «мера усиления» (Рисунок 7).

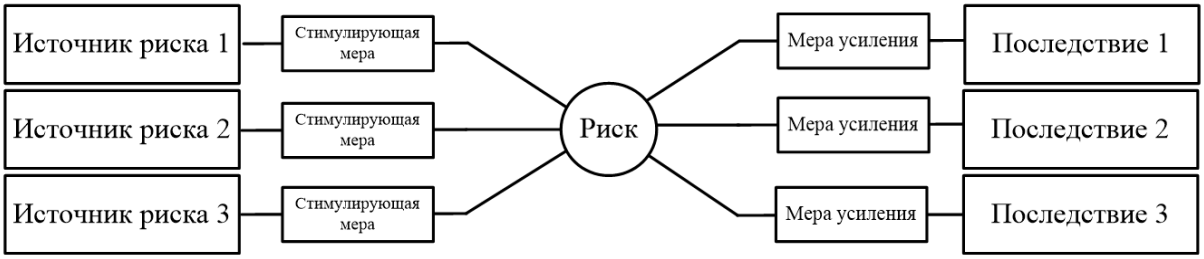

Рисунок 7. Схема метода «галстук-бабочка» для позитивных рисков[16]

Для **часто встречающихся рисков («обезьян»)** предлагается использовать только метод «галстук-бабочка» — второй этап.

Разработкой мероприятий для позитивных **незначительных рисков («кроликов»)** менеджер ИТ-проекта и проектная команда могут пренебречь.

Мониторинг и контроль рисков ИТ-проекта. Оптимальным мероприятием, обеспечивающим контроль триггеров идентифицированных рисковых событий, является распределение ответственности между участниками проектной команды ИТ-проекта, то есть формирование личной ответственности за риск. Подобное делегирование процедуры контроля может быть объяснено тем, что триггеры рисковых событий не являются универсальными и могут быть замечены только определенными специалистами. Так, триггер «во время тестирования была обнаружена ошибка в программном коде (*bug*)» для риска «запланированная на итерацию функциональность не завершится в срок» должен контролировать разработчик программного кода, который раньше менеджера ИТ-проекта заметит признаки наступления рискового события.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Кроме того, процедура мониторинга и контроля может быть обусловлена выбранной моделью жизненного цикла разработки ИТ-проекта[24]. Например: если выбрана итеративная модель жизненного цикла, то предлагается на обсуждение проектной команды выносить следующие вопросы:

- Все ли функциональности и задачи, запланированные на итерацию, завершены. Если нет, то в чем причины?
- Были ли идентифицированы новые рисковые события, которые могут оказать влияние на успешное завершение ИТ-проекта? Если да, то необходимо:

  – проведение оценки вероятности проявления и влияния для выявленного риска;

  – если риск был определен как незначительный, то им можно пренебречь;

  – если риск был определен как катастрофический, непредсказуемый или часто встречающийся, то необходимо разрабатывать меры по реагированию.
- Были ли замечены триггеры идентифицированных рисковых событий? Если да, то принимаются к исполнению меры «плана Б».

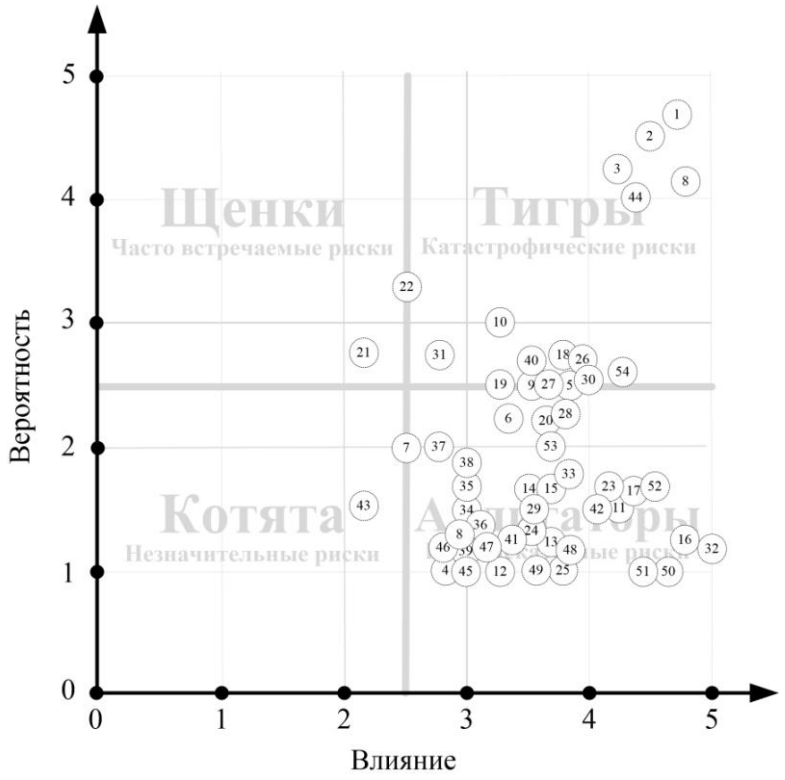

Рисунок 8. Идентифицированные негативные риски проекта

[24] *Lopez C., Salmeron J.L.* Monitoring Software Maintenance Project Risks // Procedia Technology. 2012. No 5. P. 363–368.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Согласно разработанному организационно-методическому обеспечению была проведена экспериментальная апробация по внедрению риск-менеджмента в малый ИТ-проект (длительность разработки не более двух месяцев).

На этапе идентификации была изучена сопроводительная проектная документация и проведены интервью с каждым участником проектной команды. В результате был создан раздел реестра рисковых событий «Идентификация рисков», в которых описаны 54 негативных и 14 позитивных рисковых события.

Используя методы анализа рисков, а также вербально-цифровой шкалы Харрингтона, участники проектной команды провели экспертную оценку негативных и позитивных рисков.

В результате экспертных оценок вероятности проявления и влияния рисковых событий было установлено, что из 54 (100%) негативных рисков 17 (31,4%) являются катастрофическими, 35 (64,8%) — непредсказуемыми; 1 (1,9%) — часто встречающимися и 1 (1,9%) — незначительным (Рисунок 8). Среди 14 (100%) позитивных рисковых событий 10 (71,4%) — созидательные, 4 (28,6%) — непредсказуемые.

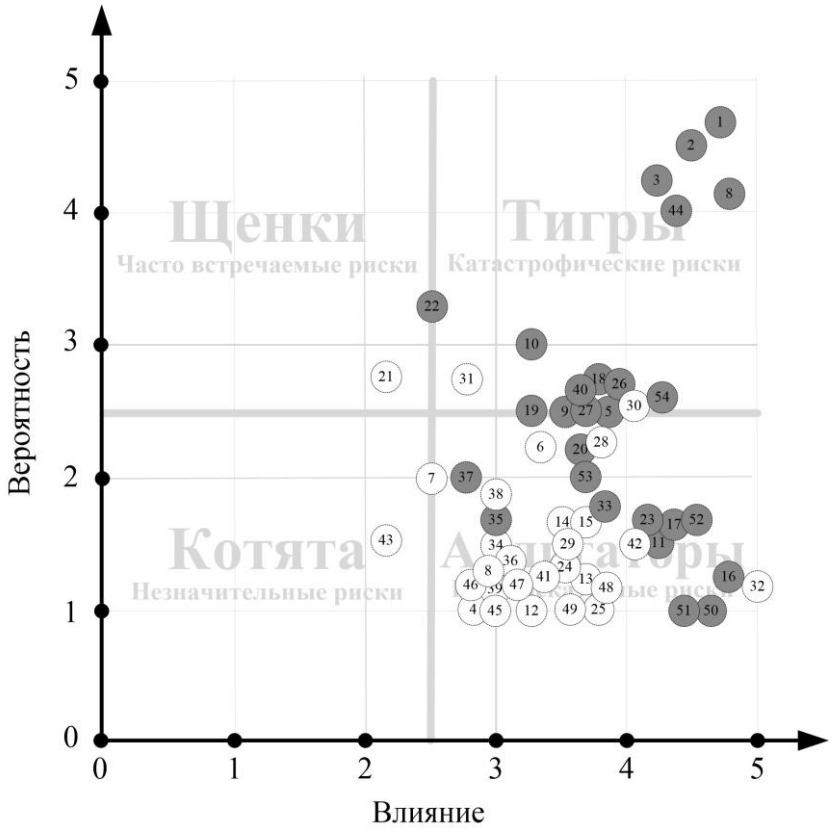

Рисунок 9. Негативные риски,
для которых были разработаны мероприятия «план А»

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Так как более 70% позитивных рисков были определены как «слоны», то есть риски, которые могут наступить в проекте независимо от усилий участников проектной команды, менеджер проекта принял решение не разрабатывать мероприятия, повышающие вероятность наступления, для четырех рисков типа «львы». Таким образом, концентрация ресурсов была сосредоточена на управлении катастрофическими («тиграми») и непредсказуемыми («аллигаторами») негативными рисками.

Перед реализацией ИТ-проекта участники проектной команды разработали мероприятия «плана А», триггеры и мероприятия «плана Б» для 27 идентифицированных негативных рисков (Рисунок 9).

В первую очередь участники проектной команды сосредоточили свое внимание на рисках категории «тигры». Однако не для всех рисков удалось разработать креативные меры реагирования. Например, риски «Участники проекта могут заболеть» и «У участников проекта могут быть форс-мажорные обстоятельства» были определены как рисковые события, которыми нельзя управлять. В этой связи из 17 рисков типа «тигры» были разработаны и проведены превентивные мероприятия только для 15.

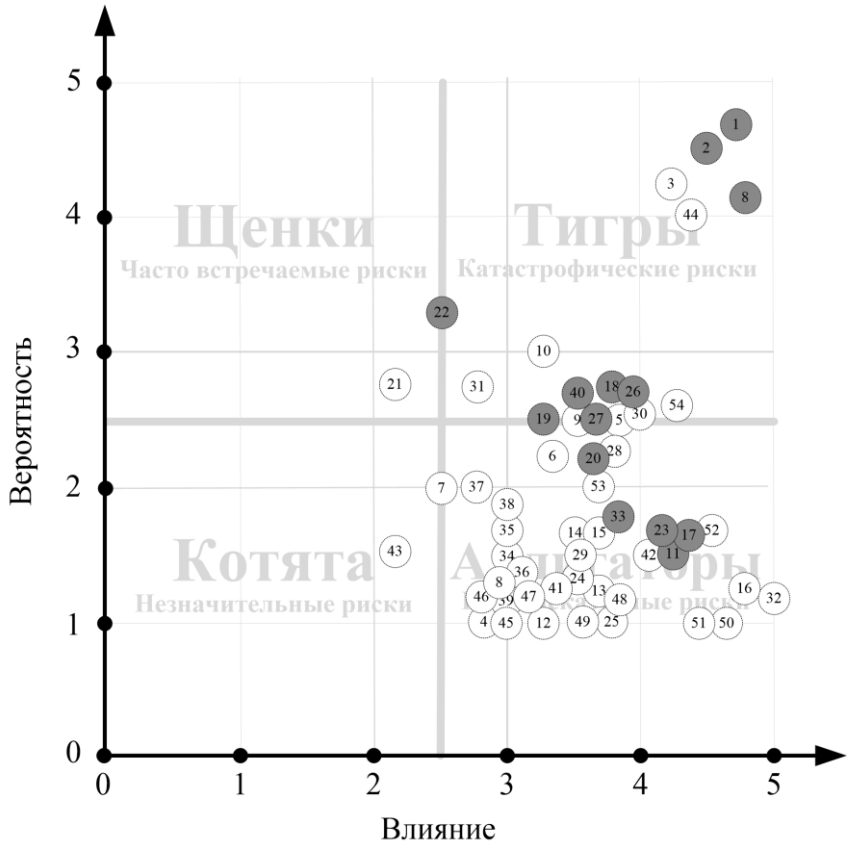

Рисунок 10. Негативные риски,
для которых были разработаны триггеры мероприятия «План Б»

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Далее участники проектной команды ИТ-проекта для 11 из 35 рисков типа «аллигаторы» разработали креативные меры реагирования. Разработка «плана А» и «плана Б» для рисков типа «аллигаторы» велась до тех пор, пока не была достигнута предельная стоимость ресурсов, выделяемых на риск-менеджмент (Рисунок 10).

По окончании работ в проекте фактическая длительность этапа программной реализации проекта составила 69 рабочих дней, что на 3 дня больше утвержденного базового плана. Данное отклонение может быть объяснено двумя наступившими неидентифицированными рисками: «Результаты разработки были рассмотрены заказчиком несвоевременно» и «В результате ребрендинга организации заказчика изменился дизайн сайта». Эти риски были перенесены на заказчика, так как по его вине произошла временная задержка, повлиявшая на длительность проекта.

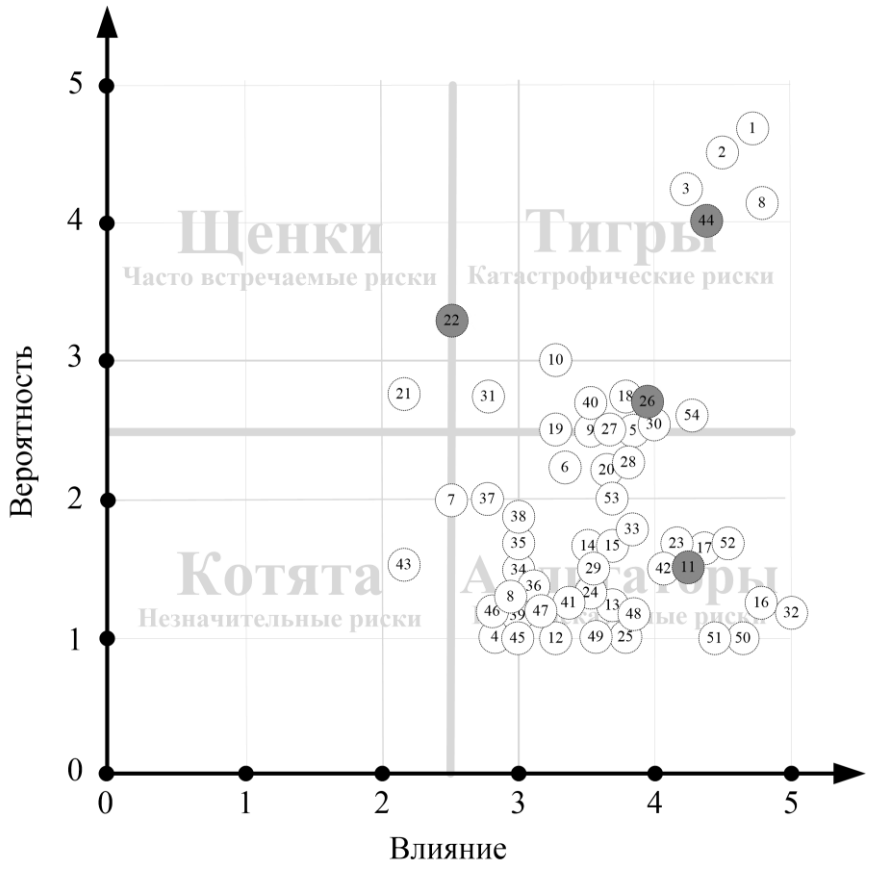

Рисунок 11. Негативные риски, которые наступили в процессе реализации ИТ-проекта

Согласно план-графику, длительность ИТ-проекта была равна 66 рабочим дням. Фактическая длительность ИТ-проекта составила 69 рабочих дней. Таким образом, отклонение от запланированных планов равно 4,5%. По сравнению со

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

статистическими данными, предоставленными *The Standish Group International* за 2014 год, отклонение для ИТ-проекта было уменьшено в 19 раз (с 89% до 4,5%)[25].

На основании проведенного исследования и экспериментальной апробации дано решение актуальной научно-практической задачи, связанной с внедрением риск-менеджмента в ИТ-проекты. Таким образом, снято противоречие между требованиями, предъявляемыми к риск-менеджменту в ИТ-проектах, а именно:

- внедрение риск-менеджмента не изменило существующее управление в ИТ-проекте (*Waterfall*);
- в результате внедрения риск-менеджмента, согласно организационно-методическому обеспечению, отклонение от плана составило 4,5%.

Список литературы:

1. *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.
2. *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: Изд-во Томского политехнического университета, 2015. С. 254−257.
3. *ДеМарко Т.* Вальсируя с медведями: управление рисками в проектах по разработке программного обеспечения. М.: Компания p.m.Office, 2005.
4. *Ефимов В.В.* Сборник методов поиска новых идей и решений управления качеством. Ульяновск: УлГТУ, 2011.
5. *Краковецкая И.В., Николаенко В.С.* Активация творческого потенциала персонала с помощью эвристических методов при разработке сайта // Креативная экономика. 2013. № 10 (82). С. 37−43.
6. *Николаенко В.С.* Анализ инструментария по обеспечению функции управления рисками в ИТ-проектах // Государственный управление. Электронный вестник. 2015. № 49. С. 105−120. URL: http://e-journal.spa.msu.ru/vestnik/item/49_2015nikolaenko.htm (дата обращения: 12.02.2016).

[25] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 16-36-00031 мол_а.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

7. *Николаенко В.С.* Пути активизации творческого потенциала проектной команды с помощью эвристических методов // Креативная экономика. 2014. № 01 (85). С. 18−25.

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

9. *Никулина И.Е., Тухватулина Л.Р., Черепанова Н.В.* Основы современного менеджмента. Томск: Изд-во Томского политехнического университета, 2009.

10. *Стрелец И.А.* Сетевая экономика: учебник. М.: Эксмо, 2006.

11. CHAOS Manifesto 2013 / The Standish Group International, 2013.

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

13. *De Bakker K., Boonstra A., Wortmann H.* Does Risk Management Contribute to IT Project Success? A Meta-Analysis of Empirical Evidence // International Journal of Project Management. 2010. No 28. P. 1–23.

14. *De Bono E.* Six Thinking Hats. New York: Little, Brown Book Group Limited, 1985.

15. Innovation games [Site]. URL: http://www.innovationgames.com/speed-boat (accessed: 05.02.2016).

16. *Ishikawa K.* Guide to Quality Control. Tokyo: Asian Productivity Organization, 1986.

17. ISO/IEC 31010:2009. Risk management — Risk assessment techniques. URL: http://www.iso.org/iso/catalogue_detail?csnumber=51073 (accessed: 13.03.2015).

18. *Lee O.-K. D., Baby D.V.* Managing Dynamic Risks in Global IT Projects: Agile Risk-management Using the Principles of Service-oriented Architecture // International Journal of Information Technology & Decision Making. 2013. Vol. 12. No 6. P. 1121–1150.

19. *Lewis S., Smith K.* Lessons Learned from Real World Application of the Bow-tie Method / Prepared for Presentation at American Institute of Chemical Engineers 2010 Spring Meeting 6th Global Congress on Process Safety San Antonio, Texas, March 22–24, 2010. Unpublished.

20. *Lopez C., Salmeron J.L.* Monitoring Software Maintenance Project Risks // Procedia Technology. 2012. No 5. P. 363–368.

21. Manifesto for Agile Software Development [Site]. URL: http://agilemanifesto.org (accessed: 05.02.2016).

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

23. *Petukhov O.N., Nikolaenko V.S.* Network Projects As a New Paradigm in e-Learning // International Multidisciplinary Scientific Conferences on Social Sciences and Arts,

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

SGEM 2014. September 1-9, 2014. Book 1 Vol. 3. P. 579-586. URL: http://sgemsocial.org/ssgemlib/spip.php?article460 (accessed: 05.02.2016).

24. *Youssef Z., Mohamed O.* Applying Ishikawa Approach for Modeling ERP Risk-effects // Journal of Theoretical and Applied Information Technology. 2015. Vol. 1. No 1. P. 51−60.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

Nikolaenko V.S.

Risk Management in IT-projects

Valentin S. Nikolaenko — Teaching Assistant, Management Department, Tomsk Polytechnic University; graduate student, Tomsk State University, Tomsk, Russian Federation.
E-mail: nikolaenkovs@tpu.ru

Annotation
The article describes the organizational methods of the process of introduction of risk management in IT-projects. These methods make it possible to eliminate the contradiction that arises among the requirements addressed to the risk management executives of IT-organizations, IT-project managers (PM) and other practitioners. The essence of the contradiction lies in the fact that risk management should provide maximum convergence of the actual and planned results (a variation of less than 5%), but it should not change the existing model of management in IT-projects. In connection therewith, the purpose of the article is to resolve contradictions which may occur among requirements imposed on risk management in IT-projects, namely: introduction of risk management should not change existing and established IT-project management, i. e. project management should remain unchanged (Waterfall, Agile, etc.); introduction of risk management should contribute to minimize variation between actual and planned results.

Keywords
Risk, risk management, IT-project, organizational methods.

References:

1. Gaga V.A., Nikolaenko V.S. Sozdanie sistemy upravleniia proektami v organizatsii s primeneniem evristicheskikh metodov. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2013, 374, pp. 137−140.
2. Daibova K.E., Nikolaenko V.S. Razrabotka instrumentariia operativnoi identifikatsii riskov v IT-proektakh. *Resursoeffektivnym tekhnologiiam — energiiu i entuziazm molodykh: sbornik nauchnykh trudov VI Vserossiiskoi konferentsii*. Tomsk: Izd-vo Tomskogo politekhnicheskogo universiteta, 2015. Pp. 254−257.
3. DeMarko T. *Valsiruia s medvediami: upravlenie riskami v proektakh po razrabotke programmnogo obespecheniia*. Moscow: Kompaniia p.m.Office, 2005.
4. Efimov V.V. *Sbornik metodov poiska novykh idei i reshenii upravleniia kachestvom*. Ul'ianovsk: UlGTU, 2011.
5. Krakovetskaia I.V., Nikolaenko V.S. Aktivatsiia tvorcheskogo potentsiala personala s pomoshch'iu evristicheskikh metodov pri razrabotke saita. *Kreativnaia ekonomika*, 2013, 10 (82), pp. 37−43.
6. Nikolaenko V.S. Analiz instrumentariia po obespecheniiu funktsii upravleniia riskami v IT-proektakh. *Gosudarstvennyi upravlenie. Elektronnyi vestnik*, 2015, 49, pp. 105−120. URL: http://e-journal.spa.msu.ru/vestnik/item/49_2015nikolaenko.htm (data obrashcheniia: 12.02.2016).
7. Nikolaenko V.S. Puti aktivizatsii tvorcheskogo potentsiala proektnoi komandy s pomoshch'iu evristicheskikh metodov. *Kreativnaia ekonomika*, 2014, 01 (85), pp. 18−25.
8. Nikolaenko V.S. Razrabotka printsipov upravleniia IT-proektom. *Vestnik Tomskogo gosudarstvennogo universiteta*, 2015, 390, pp. 155−160.
9. Nikulina I.E., Tukhvatulina L.R., Cherepanova N.V. *Osnovy sovremennogo menedzhmenta*. Tomsk: Izd-vo Tomskogo politekhnicheskogo universiteta, 2009.
10. Strelets I.A. *Setevaia ekonomika: uchebnik*. Moscow: Eksmo, 2006.
11. *CHAOS Manifesto 2013* / The Standish Group International, 2013.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016

12. *CHAOS Manifesto 2014* / The Standish Group International, 2014.

13. De Bakker K., Boonstra A., Wortmann H. Does Risk Management Contribute to IT Project Success? A Meta-Analysis of Empirical Evidence. *International Journal of Project Management*, 2010, 28, pp. 1–23.

14. De Bono E. *Six Thinking Hats*. New York: Little, Brown Book Group Limited, 1985.

15. *Innovation games* [Site]. URL: http://www.innovationgames.com/speed-boat (accessed: 05.02.2016).

16. Ishikawa K. *Guide to Quality Control*. Tokyo: Asian Productivity Organization, 1986.

17. *ISO/IEC 31010:2009. Risk management — Risk assessment techniques*. URL: http://www.iso.org/iso/catalogue_detail?csnumber=51073 (accessed: 13.03.2015).

18. Lee O.-K. D., Baby D.V. Managing Dynamic Risks in Global IT Projects: Agile Risk-management Using the Principles of Service-oriented Architecture. *International Journal of Information Technology & Decision Making*, 2013, vol. 12, no 6, pp. 1121–1150.

19. Lewis S., Smith K. *Lessons Learned from Real World Application of the Bow-tie Method* / Prepared for Presentation at American Institute of Chemical Engineers 2010 Spring Meeting 6th Global Congress on Process Safety San Antonio, Texas, March 22–24, 2010. Unpublished.

20. Lopez C., Salmeron J.L. Monitoring Software Maintenance Project Risks. Procedia *Technology*, 2012, 5, pp. 363–368.

21. *Manifesto for Agile Software Development* [Site]. URL: http://agilemanifesto.org (accessed: 05.02.2016).

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

23. Petukhov O.N., Nikolaenko V.S. Network Projects As a New Paradigm in e-Learning. *International Multidisciplinary Scientific Conferences on Social Sciences and Arts, SGEM 2014*. September 1–9, 2014. Book 1. Vol. 3. Pp. 579–586. URL: http://sgemsocial.org/ssgemlib/spip.php?article460 (accessed: 05.02.2016).

24. Youssef Z., Mohamed O. Applying Ishikawa Approach for Modeling ERP Risk-effects. *Journal of Theoretical and Applied Information Technology*, 2015, vol. 1, no 1, pp. 51−60.

© Факультет государственного управления МГУ имени М.В.Ломоносова, 2016