Министерство науки и высшего образования
Российской Федерации
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ

В.С. Николаенко

БЕЗУПРЕЧНЫЙ РИСК-МЕНЕДЖМЕНТ

Учебное пособие

Томск
Издательство ТУСУРа
2023

УДК 005.334(075.8)
ББК 65.290-2я73
Н634

Рецензенты:

Никулина И.Е, профессор школы инженерного предпринимательства Томского политехнического университета, д-р экон. наук, профессор;

Калиновский Н.В., Генеральный директор ООО «ИНТЭК»

Печатается по решению научно-методического совета ТУСУРа
(протокол № 5 от 01.06.23)

Николаенко, Валентин Сергеевич

Н634 Безупречный риск-менеджмент: учеб. пособие / В.С. Николаенко. – Томск: Изд-во Томск. гос. ун-та систем управления и радиоэлектроники, 2023. – 140 с.

ISBN 978-5-6050216-0-5

Представлены теоретические и практические аспекты управления различными видами рисков (негативными, позитивными, комплаенс-рисками, проектными, рисками внешней среды и др.). Описан инструментарий оценки, мониторинга и контроля рисков, механизм воздействия на риски и их документальное сопровождение. Рассмотрены основные ментальные ловушки, которые могут препятствовать результативному и эффективному достижению запланированных целей.

Предназначено для риск-менеджеров, руководителей проектов и участников проектных команд, представителей бизнес-сообщества и студентов высших учебных заведений, обучающихся по направлениям подготовки в области управления, экономики и информационных технологий.

УДК 005.334(075.8)
ББК 65.290-2я73

ISBN 978-5-6050216-0-5

Оглавление

Введение

В аналитических докладах The CHAOS Manifesto [1] дается лаконичный ответ на вопрос «Зачем необходимо управлять рисками». Управление рисками снижает вероятность возникновения неблагоприятных событий и сводит к минимуму возможные потери. В частности, проанализировав порядка 50 000 ИТ-проектов, реализуемых в США и странах Европы, представители моноактивной деловой культуры установили, что ущерб от наступления одного негативного риска приблизительно равен $1000. При глубоком изучении причин наступления негативных рисков специалисты обнаружили, что этих материальных потерь можно было избежать, всего лишь предварительно проведя профилактические мероприятия. В The CHAOS Manifesto говорится, что профилактическая мера и превентивное устранение одного негативного риска обходится всего в $1.

Анализ результатов бизнес-деятельности в отечественной практике и судебных решений 495 томских организаций, занятых разработкой компьютерного программного обеспечения (ОКВЭД 62.0), показал, что причиненный материальный ущерб от наступления одного комплаенс-риска[1] превышает 277 тыс. руб. [2]. Изучение причин материализации комплаенс-рисков позволяет сделать вывод о том, что их можно элиминировать посредством заблаговременного внесения в контракты определенных условий (ковенантов[2]). С примерами ковенантов, которые изменяют вероятность материализации комплаенс-рисков и их возможное влияние в случаях наступления, можно ознакомиться в приложении 1.

Кроме того, необходимость управления рисками также подтверждается Федеральной службой по надзору в сфере связи,

---

[1] Комплаенс (от англ. *to comply* — соответствовать) — соответствие внутренним требованиям организации и внешним нормам действующего законодательства. Комплаенс-риск — несоответствие нормативным актам, стандартам и кодексам поведения. Последствия материализации этих рисков проявляются в форме юридических санкций со стороны регулирующих и надзорных органов, отраслевых ассоциаций и лиц, права и интересы которых были нарушены.

[2] Ковенант — обязательство совершить какое-либо действие или воздержаться от его совершения. Ковенанты — условия, нарушение которых должником дает кредитору право на определенные действия (например, требовать досрочного погашения обязательств).

информационных технологий и массовых коммуникаций (Роскомнадзор). В частности, по данным Роскомнадзора за первое полугодие 2021 г. число компьютерных атак на отечественную критическую информационную инфраструктуру (КИИ) выросло на 150 % [3]. Больше всего кибератак было совершено на КИИ научных и образовательных организаций и промышленных предприятий — около 30 % всех компьютерных атак; еще 28 % нападений было направлено на государственные и медицинские учреждения [4].

Приведенные данные показывают, что необходима заблаговременная работа с вероятными негативными событиями, чтобы элиминировать наступление гражданской, дисциплинарной, административной и уголовной ответственности, а также нивелировать возможные материальные потери. Следовательно, прежде чем приступать к процессу достижения целей, нужно выявлять вероятные события, которые могут помешать этому, продумывать наиболее безопасные пути движения, а также запасаться ресурсами на случай материализации непредвиденных событий. Подобный процесс достижения целей называют ***риск-ориентированным***.

В учебном пособии изложены основные теоретические аспекты и представлены практические инструменты риск-ориентированного управления, применение которых дает возможность руководителям организаций, департаментов, отделов и проектов достигать запланированных стратегических, тактических, операционных и проектных целей, нивелируя и ослабляя негативное влияние и усиливая позитивный эффект от наступивших последствий.

В первом разделе рассматриваются основные понятия и теоретические аспекты управления рисками, история развития и становления риск-менеджмента в мире и Российской Федерации, классификация рисков, а также приведены материалы наиболее распространенных национальных[1] и международных[2] стандартов.

---

[1] ГОСТ Р ИСО 31000. Менеджмент риска. Принципы и руководство; ГОСТ Р 31010. Методы оценки риска.

[2] Свод знаний управления рисками (Management of Risk: Guidance for Practitioners — M_o_R®); Свод знаний управления проектами (Project Management Body of Knowledge — PMBOK® Guide); Свод знаний управления проектами (Projects IN Controlled Environments — PRINCE2®); Свод знаний управления рисками организаций (The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management» — COSO ERM).

Во втором разделе анализируются процессы управления рисками и методы оценки, воздействия, мониторинга и контроля рисков. Кроме того, представлен перечень универсальных коммерческих, проектных, комплаенс-рисков и рисков внешней среды, механизм документального сопровождения риск-менеджмента, а также примеры ментальных ловушек, в которые можно угодить в процессе управления рисками.

В третьем разделе пособия описывается механизм внедрения риск-менеджмента и перечень внутренних документов организации, декларирующих управление рисками. Также в разделе формализованы методы оценки результативности и экономической эффективности управления рисками, возможные ментальные ловушки и способы элиминирования[1] комплаенс-рисков.

Автор настоящего учебного пособия желает читателем безрисковых проектов и успешной реализации всех поставленных целей.

[1] Элиминирование рисков (лат. *eliminare* — изгонять, устранять, ликвидировать) — совокупность стратегий, методов и инструментов (способов) минимизации негативных последствий рисков в компании.

Павел, руководитель проекта в области ИТ «e-System», встретился с ведущими специалистами в области ИТ программистом Сергеем и тестировщиком Александром. Все выразили радость по поводу предстоящей совместной работы, но вспомнили о проблемах, с которыми они столкнулись в прошлом проекте под названием «e-Simulator».

«Помните, как мы узнали, что пользователям не понравился интерфейс e-Simulator? — спросил Александр. — У нас ушло четыре недели на то, чтобы переделать интерфейс и заново протестировать его».

Павел согласился: «А ведь пользователи, с которыми мы беседовали, клялись, что им нужно много функций. Помню, мы столкнулись с трудностями при программировании и потратили в три раза больше времени, чем ожидали. Когда все было готово, оказалось, что с этими функциями пользователи не работают».

«Может быть, нам стоит составить список проблем, возникших при работе с «e-Simulator», чтобы попытаться избежать их при разработке «e-System», — предложил Сергей. — Я читал статью по управлению рисками, в которой говорилось, что мы ***должны выявлять риски и не давать им возможности наносить вред нашему проекту****».*

Случай из практики

1. РИСК КАК ОБЪЕКТ УПРАВЛЕНИЯ

1.1. Основные понятия теории управления рисками

Результаты исследований показали, что в литературе нет общепринятого толкования понятия «риск», что создает проблему его интерпретации и использования на практике. Примеры интерпретации понятия риска в литературных источниках представлены в таблице 1.1. Следует отметить, что среди лингвистов также нет единого мнения относительно этимологии понятия «риск». По мнению одних специалистов, слово «risk» имеет французские и итальянские истоки. Например, в итальянском языке «risiko» означает «опасность» [5]. С французского «risdoe» трактуется как «объезжать утес». Другие специалисты предполагают, что слово «риск» имеет греческие корни «ridsikon» и «ridsa», означающие «утес», «скала» и «лавирование между скалами».

Таблица 1.1 – Интерпретация понятия «риск» в литературных источниках

Содержание понятия «риск»	Источник
1. Влияние неопределенности на цели	ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство [6] ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство [7]
2. Угроза и/или опасность	Балабанов И.Т. [8] Машков Д.М. [9]
3. Неопределенность	Филимонов Д.И. [10] Бурков В.Н и др. [11] Мазур И.И. и др. [12]
4. Условие или неопределенное событие, которое в случае наступления оказывает влияние на цели проекта (содержание, длительность, стоимость, качество)	Свод правил проектного управления (версии 4, 5 и 6) (Project Management Body of Knowledge — PMBOK® Guide) [13, 14, 15]
5. Угроза или возможность	Сангхира П. [16]
6. Событие, которое одновременно несет угрозу, опасность, неопределенность и возможность	Price water house Coopers (PwC) [17]
7. Вероятность недополучения доходов и/или вероятность возникновения убытков	Грабовый П.Г. и др. [18]
8. Мера опасности	Шохин Е.И. [19]
9. Совокупность значений возможного ущерба	Королев В.Ю и др. [20]
10. Возможность получения убытков от предпринимательской деятельности	Гражданский кодекс РФ (ст. 926, 933) [21]
11. Действия, сделанные наудачу	Даль В. [22]

Окончание таблицы 1.1

Содержание понятия «риск»	Источник
12. Неопределенное событие или совокупность неопределенных событий	Свод знаний управления рисками (Management of Risk: Guidance for Practitioners — M_o_R®) [23]
13. Неопределенное событие или набор событий, которые в случае наступления, способны оказать влияние на процесс достижения целей	Свод знаний управления проектами (PRojects IN Controlled Environments — PRINCE2®) [24]
14. Искусственная экономическая категория, совокупно отражающая меру реальности нежелательного отклонения от цели хозяйственной деятельности предприятия и размер обусловленного этим отклонением ущерба	Качалов Р.М. [25]
15. Негативная часть неопределенного события, наступление которого может принести организации ущерб и/или выгоду	Свод знаний управления рисками организаций (The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management» — COSO ERM) [17]
16. Вероятный неблагоприятный исход для субъекта	Мадера А.Г. [26, 27]

В азиатской культуре понятие «риск» включает два иероглифа 风 险, которые означают опасность и позитивную возможность.

Современное толкование понятия «риск» закреплено в отечественных и международных стандартах. В частности, в версиях отечественного стандарта «Менеджмент риска. Принципы и руководство» ГОСТ Р ИСО 31000-2010 и ГОСТ Р ИСО 31000-2019 риск характеризуется как влияние неопределенности на запланированные цели [6, 7], его структура представлена на рисунке 1.1.

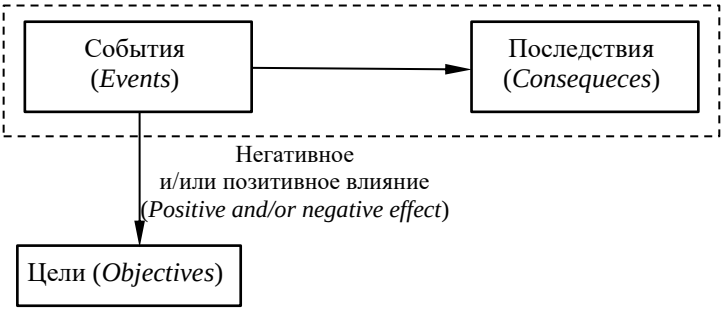


Рисунок 1.1 – Структура риска
согласно ГОСТ Р ИСО 31000-2010

В разных версиях свода знаний управления проектами «Project Management Body of Knowledge» (PMBoK® Guide. Версии: PMBOK-4, PMBOK-5 PMBOK-6) под риском понимается неопределенное событие (ситуация), которое при наступлении оказывает негативное или позитивное влияние на проектные цели, такие как содержание, длительность, стоимость и/или качество проекта [13, 14, 15] (рисунок 1.2).

Свод знаний управления рисками организаций «Управление рисками организации. Интеграция со стратегией и эффективностью деятельности» (The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management» — COSO ERM) опирается на концепцию природы риска, разработанную PricewaterhouseCoopers (PwC). Специалисты PwC считают, что риск — это неопределенное событие, которое несет угрозу, опасность, неопределенность и возможность [17]. Согласно своду правил COSO ERM структура риска представлена на рисунке 1.3.

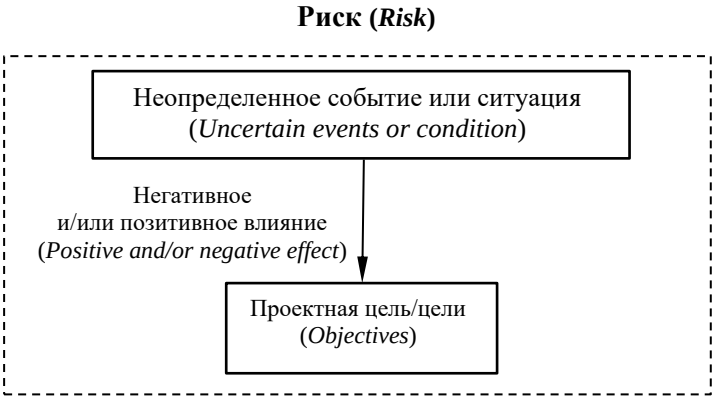


Рисунок 1.2 – Структура риска согласно PMBOK® Guide

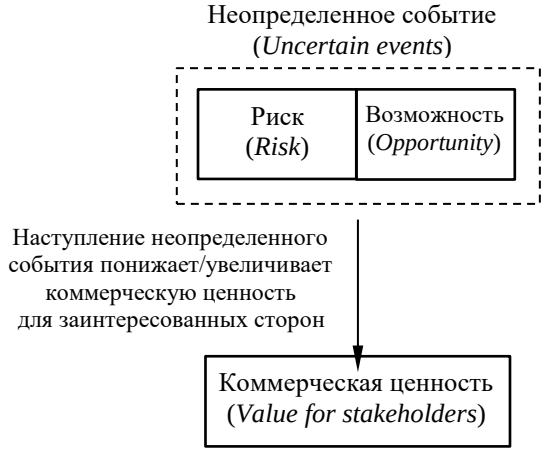


Рисунок 1.3 – Структура риска согласно COSO ERM

В своде знаний управления рисками (Management of Risk: Guidance for Practitioners, M_o_R®) под риском понимается неопределенное событие, состоящее одновременно из угрозы и позитивной возможности, которое при наступлении оказывает влияние на процесс достижения целей организации (рисунок 1.4) [23].

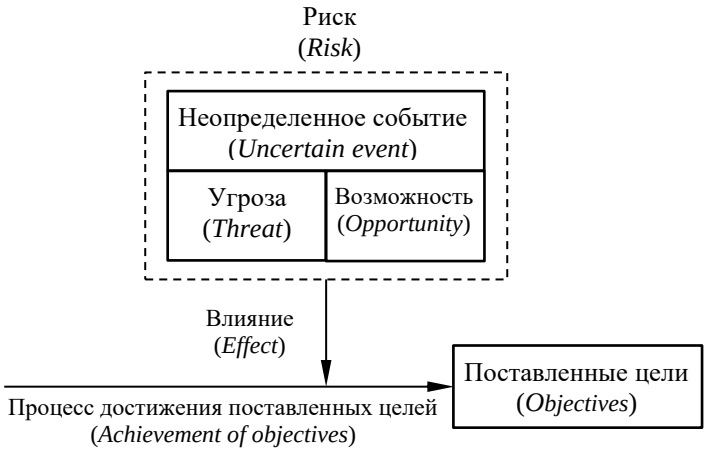


Рисунок 1.4 – Структура риска согласно M_o_R®

В своде знаний управления проектами PRINCE2® риск трактуется как неопределенное событие, которое имеет сложную структуру. В частности, риск состоит из причины риска, угрозы, позитивной возможности и последствия в случае его материализации (рисунок 1.5) [24].

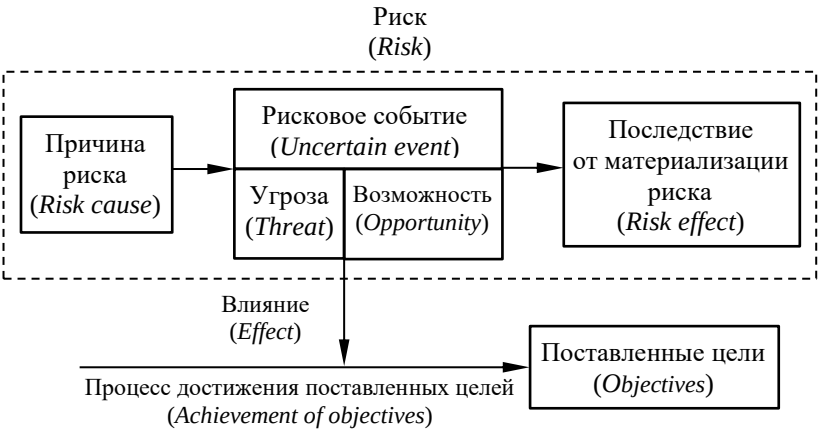


Рисунок 1.5 – Структура риска согласно PRINCE2®

Следует подчеркнуть, что согласно отечественным и международным стандартам понятия «неопределенность» и «риск» часто воспринимаются как синонимы, однако между ними есть существенные различия, в частности:

- неопределенность возникает, когда нет необходимой и достоверной информации. Риск же, напротив, базируется на накопленных предшественниками статистических данных, поэтому материализация риска может быть спрогнозирована;
- неопределенность при недостатке необходимой и достоверной информации опирается на субъективные мнения, например на предыдущий опыт работников и экспертов. Риск же оперирует объективными фактами (причиной, создающей риск, источником риска, последствиями от материализации риска и др.);
- источники неопределенности, как правило, неизвестны. Риск же создают конкретные причины и источники, каждый из которых может быть идентифицирован.

Таким образом, на основе рассмотренных выше точек зрения можно заключить, что **риск** — это вероятное событие, проистекающее из конкретных источников, материализация которого может привести к наступлению благоприятных/проблемных последствий (рисунок 1.6). Под ***причинами, создающими риск,*** понимаются условия, имеющие потенциал создавать события, которые способны оказывать влияние на процесс достижения целей; под ***источниками риска*** — объекты, имеющие потенциал создавать события, способные оказывать влияние на процесс достижения целей; а под ***последствиями от наступления риска*** — новые обстоятельства, возникающие в результате материализации риска.

Стоит отметить, что последствия от наступления рисков являются основанием для дифференциации рисков на ***следующие виды:***

1) ***негативный риск*** — это вероятное событие, которое может привести к наступлению проблемных последствий;

2) ***позитивный риск*** — это вероятное событие, которое может привести к наступлению благоприятных последствий;

3) ***смешанный риск*** — это вероятное событие, наступление которого приводит одновременно к проблемным и благоприятным последствиям;

4) ***нейтральный риск*** — это вероятное событие, которое не приводит к проблемным и/или благоприятным последствиям.

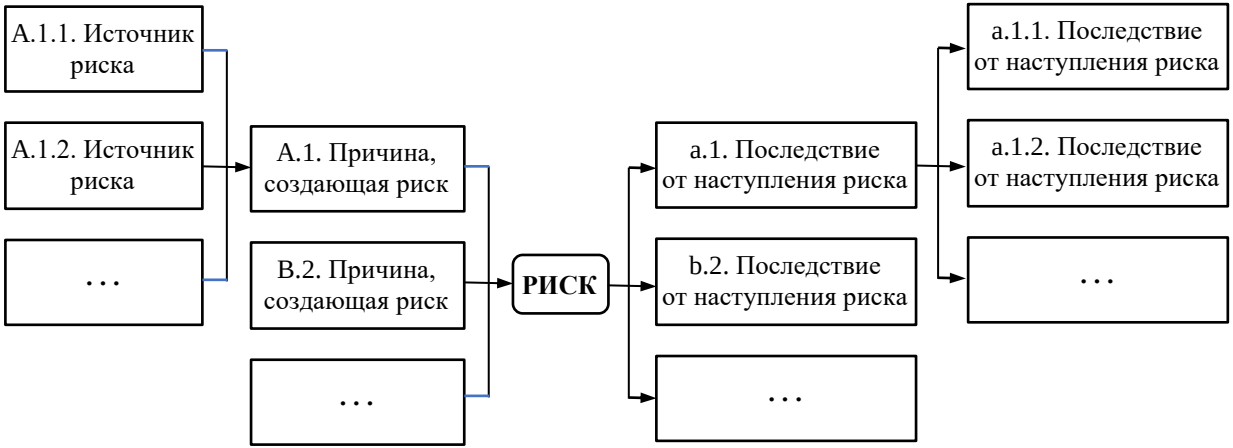


Рисунок 1.6 – Структура риска: причины, создающие риск; источники риска, последствия от наступления риска

Необходимо отметить, что представленная на рисунке 1.6 структура риска позволяет сделать важные практико-ориентированные выводы относительно последствий от наступления риска:

1) если оперативно не локализовать проблемные последствия, то в скором времени они приведут к новым проблемным последствиям. Например, установлено, что спецификация требований к представленной разработчиком программе для ЭВМ является неполной и недостоверной. Если оперативно не устранить данное отклонение, то вскоре последует изменение требований и целей;

2) для нейтральных и смешанных рисков необходимо блокировать наступление проблемных последствий, усиливая при этом возможный благоприятный эффект. Например, при атаке на критическую информационную инфраструктуру необходимо блокировать возможность неправомерного доступа, копирования, предоставления и/или распространения конфиденциальной информации, неправомерного уничтожения и/или модификации конфиденциальной информации, заражения КИИ вредоносным программным обеспечением (ПО), идентифицируя при этом возможные уязвимости КИИ.

В качестве примера воздействия негативного и позитивного рисков на план проекта в случае их материализации рассмотрим рисунок 1.7, где t — это длительность проекта.

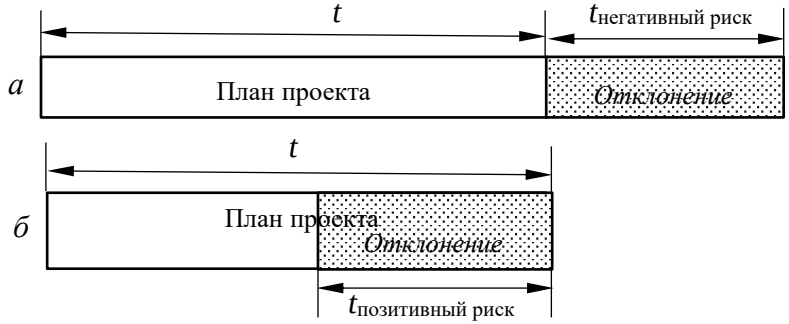


Рисунок 1.7 – Влияние наступившего негативного риска (*а*) и позитивного риска (*б)* на план проекта

В случае материализации негативного риска происходит увеличение длительности проекта на величину $t_{негативный\ риск}$, так как

руководителю и участникам проекта требуется дополнительное время для устранения возникшей проблемы. В случае наступления позитивного риска также происходит отклонение от запланированной длительности. Однако при материализации позитивного риска проект можно завершить быстрее, сократив время выполнения на величину $t_{позитивный\ риск}$.

Влияние материализовавшихся негативного и позитивного рисков можно охарактеризовать следующими формулами:

$$\mathrm{Im}_{neqative} = C_1 + C_2 + C_3 + C_4; \quad (1.1)$$

$$\mathrm{Im}_{positive} = C_5, \quad (1.2)$$

где $\mathrm{Im}_{neqative}$ — влияние (*impact*) в результате наступления негативного риска;

C_1 — прямой материальный ущерб;

C_2 — ресурсы, которые будут направлены на ликвидацию последствий;

C_3 — ресурсы, которые будут направлены на восстановление;

C_4 — материальный ущерб, вызванный отклонением от запланированных целей;

$\mathrm{Im}_{positive}$ — влияние в результате материализации позитивного риска;

C_5 — материальная польза, вызванная отклонением от запланированных целей.

В качестве примера наступившего негативного риска можно рассмотреть ситуацию потери сервера жестких дисков в ИТ-организации в результате пожара (C_1). Для того чтобы ликвидировать полученные последствия, ИТ-организации необходимо приобрести новый сервер (C_2), осуществить пуско-наладочные работы (C_3), а также оплатить простой трудовых ресурсов (C_4), спровоцированный потерей информационных данных.

Наглядным примером влияния наступившего позитивного риска является привлечение в ИТ-проект программиста более высокого квалификационного уровня либо возможность проведения

дополнительного аудита спецификаций требований к программам для ЭВМ. Эмпирические данные показывают, что проведение аудита по обнаружению и исправлению дефектов в спецификации требований обходится ИТ-организациям примерно в $200. Если же аудит не проводится, то исправление дефектов и ошибок, которые будут обнаружены конечным пользователем в созданной программе для ЭВМ, обойдутся ИТ-организации в $4200 [28].

Далее рассмотрим значение понятия «управление рисками» (risk management). Согласно ГОСТ Р ИСО 31000-2010 **управление рисками** — это совокупность принципов, скоординированных действий и процессов по оценке, воздействию, мониторингу и контролю рисков [6, 7] (рисунок 1.8). Следует отметить, что отечественный ГОСТ Р ИСО 31000-2010 является локализованной версией международного стандарта ISO 31000:2009 «Risk Management – Principles and Guidelines».

Принципы управления рисками (*Principle*)

Стандарт ГОСТ Р ИСО 31000-2010 содержит 11 принципов, которых должны придерживаться менеджмент и сотрудники организации для результативного и эффективного управления рисками. К данным принципам относятся:

1) ***направленность не только на достижение целей, но и создание и защиту общепринятых ценностей*** (*creates value*), в частности таких как безопасность жизни и здоровья работников, соответствие законодательным и другим обязательным требованиям, защита окружающей среды, предоставление качественной продукции, сервисов и услуг клиентам и др.;

2) ***принадлежность ко всем организационным процессам.*** Риск-менеджмент — это часть обязанностей руководства и неотъемлемая составляющая всех организационных процессов (*integral part of organizational processes*), включая стратегическое планирование, управление проектами и управление изменениями;

3) ***обязательный элемент процесса принятия решений*** (*part of decision making*), позволяющий работникам, принимающим решения, делать осознанный выбор и определять приоритетность действий;

4) ***безусловный учет фактора неопределенности*** *(explicitly addresses uncertainty)* при организации процессов управления, стремление обеспечить переход к объективным фактам и информации;

5) ***систематический, структурированный и своевременный подход в практическом применении*** (*systematic, structured and timely*) как средство достижения устойчивых и стабильных результатов;

6) ***использование наилучшей доступной информации*** (*based on the best available information*). Входные данные для процесса управления рисками основываются на таких источниках информации, как исторические данные, опыт, обратная связь от заинтересованных сторон, наблюдения, прогнозы и экспертные оценки;

7) ***адаптируемость процессов управления рисками*** (*tailored*) к текущей внешней и внутренней ситуации);

8) ***учет человеческих и культурных факторов*** (*take human and cultural factors into account*);

9) ***прозрачность принимаемых решений с учетом позиции заинтересованных сторон*** (*transparent and inclusive*). Своевременное вовлечение заинтересованных сторон и лиц, принимающих решения, гарантирует, что управление рисками будет отвечать их интересам и требованиям;

10) ***динамичность, итеративность и своевременное реагирование на изменения*** (*dynamic, iterative and responsive to change*). Управление рисками должно быть направлено на непрерывное распознавание изменений, их оценку и превентивное элиминирование. В частности, как только происходит внешнее и/или внутреннее событие, необходимо актуализировать перечень рисков, поскольку могут появиться новые риски и исчезнуть ранее выявленные;

11) ***систематизация и совершенствование приобретенных знаний о рисках*** в целях создания более совершенных стратегий управления рисками (*facilitates continual improvement and enhancement of the organization*).

Инфраструктура управления рисками (*Framework*)

Согласно ГОСТ Р ИСО 31000-2010 реализация перечисленных принципов обеспечивается включением в инфраструктуру управления рисками следующих пяти элементов:

1) полномочия и обязательства;
2) эффективная схема организации;
3) внедрение и применение;
4) мониторинг и анализ;
5) постоянное совершенствование.

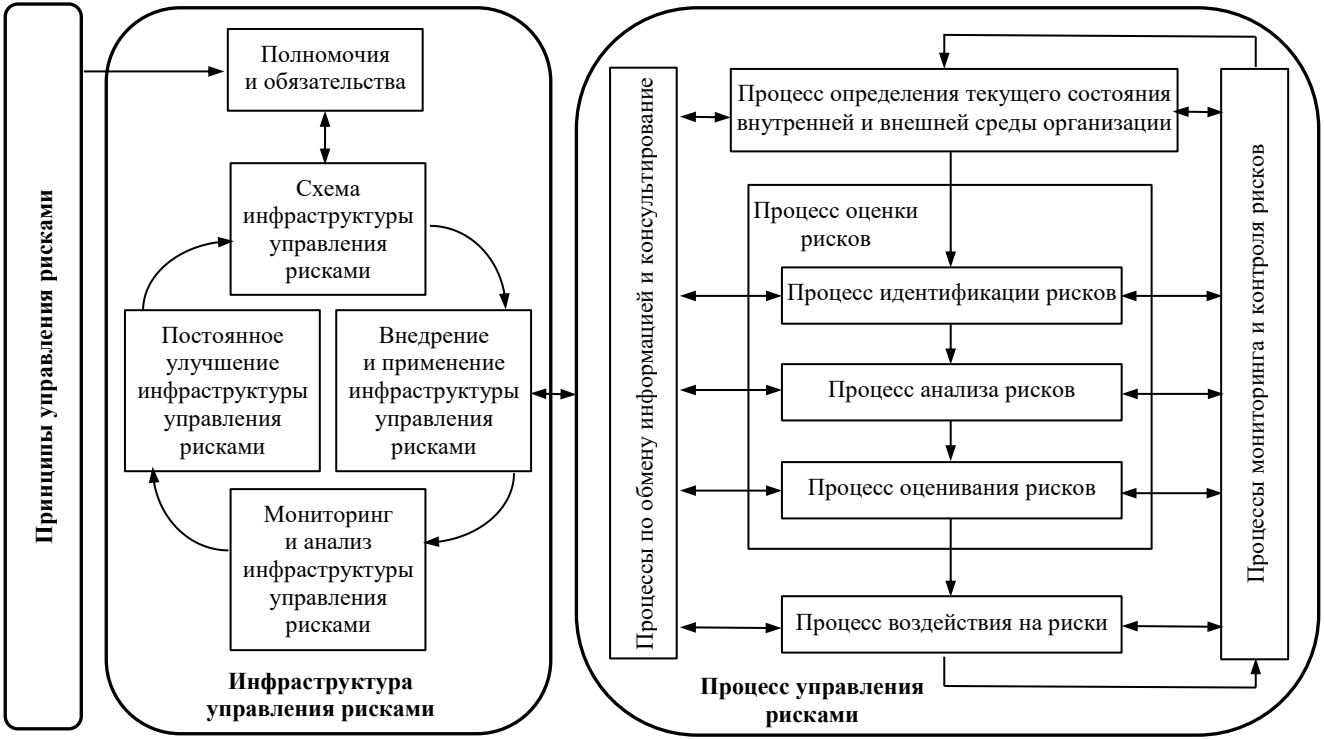


Рисунок 1.8 – Взаимосвязь между принципами, инфраструктурой и процессами управления рисками согласно ГОСТ Р ИСО 31000-2010 (ISO 31000:2009)

1. ***Полномочия и обязательства*** (*mandate and commitment*). Управление рисками — это итеративный и непрерывный процесс, требующий поддержки и внимания со стороны руководства. Полномочия и обязательства в части управления рисками должны быть закреплены во внутренних документах организации (KPI[1], должностные инструкции, стандарты, чек-листы и др.) на всех уровнях организации, включая высшее руководство, средний менеджмент и остальных работников.

2. ***Схема инфраструктуры управления рисками*** (*design of framework for managing risk*). Результативное и эффективное внедрение процессов управления рисками организации возможно лишь при наличии зрелой инфраструктуры организации. Под инфраструктурой организации понимаются работники, ответственные за управление рисками, их трудовые договоры и должностные инструкции, рабочие места, специализированное программное обеспечение и др.

3. ***Внедрение и применение инфраструктуры управления рисками*** (*implementing risk management*). Внедрение инфраструктуры управления рисками прежде всего направлено на интеграцию с ключевыми бизнес-процессами организации, а применение инфраструктуры предусматривает реализацию процессов управления рисками на всех уровнях организации.

4. ***Мониторинг и анализ инфраструктуры управления рисками*** (*monitoring and review of the framework*). Для поддержания инфраструктуры управления рисками в работоспособном состоянии требуется систематически оценивать качество, результативность и эффективность управления рисками, пересматривать политику, внутренние регламенты и должностные инструкции.

5. ***Постоянное улучшение инфраструктуры управления рисками*** (*continual improvement of the framework*). Основываясь на результатах мониторинга, руководству необходимо принимать решения по совершенствованию инфраструктуры управления рисками.

---

[1] KPI (*Key Performance Indicator*, ключевой показатель эффективности) — измеримая величина, позволяющая видеть, насколько продуктивно работники достигают поставленные цели, которые имеют ценность для организации.

Процессы управления рисками

Управление рисками согласно ГОСТ Р ИСО 31000-2010 включают семь процессов (см. подробно во втором разделе):

1) ***обмен информацией и консультирование*** (*communication and consultation*): обмен правдивой, существенной, точной и понятной информацией между заинтересованным сторонами и их консультирование с учетом аспектов конфиденциальности;

2) ***анализ внутренней и внешней среды объектов риска*** (*establishing the context*): формулирование целей посредством установления ситуации (контекста) организации, а также определение внешних и внутренних параметров, которые следует принять во внимание в процессе управления рисками;

3) ***идентификацию рисков*** (*risk identification*): составление всеобъемлющего перечня рисков, которые в случае их наступления могут оказать влияние на процесс достижения целей. Документ, в котором фиксируются выявленные риски, называется *реестром рисков*;

4) ***анализ рисков*** (*risk analyses*): сбор информации об идентифицированных рисках, а именно установление причин, источников и возможных последствий от наступления рисков;

5) ***оценивание рисков*** (*risk evaluation*): количественное измерение вероятности наступления рисков и их возможного влияния в случае материализации. В ГОСТ Р ИСО 31000-2010 *вероятность* понимается как возможность наступления какого-либо события, *влияние* — как отклонение (отрицательное или положительное) от ожидаемого результата. Документ, в котором фиксируются результаты изменения характеристик рисков, называется *матрицей рисков*. Отметим, что процессы идентификации, анализа и оценивания рисков также принято называть *оценкой рисков*;

6) ***воздействие на риски*** (*risk treatment*): разработка мер превентивного воздействия на риски (план А) и мер принятия рисков (план Б). Документ, в котором фиксируются разработанные меры воздействия на риски, называется *планом управления рисками*;

7) ***мониторинг и контроль рисков*** (*monitoring and review*): выявление рисков, которые не были ранее зафиксированы в реестре рисков (неидентифицированные риски), и надзор за рисками, зафиксированными в реестре рисков.

1.2. История развития риск-менеджмента

Считается, что совокупность скоординированных действий и процессов по оценке, воздействию, мониторингу и контролю рисков впервые была закреплена в Базельском соглашении 1988 г., называемом «Базель I» [29]. Однако с уверенностью можно утверждать, что истоки управления рисками берут свое начало в религиозных учениях, философии, математике и теории вероятностей (таблица 1.2) [30].

Первое формальное закрепление риска в документах произошло благодаря азартным играм, в которых активно применялась концепция теории вероятностей. Ведущую роль в развитии данного направления сыграл крупный алгебраист XVI в. Джероламо Кардано, посвятивший анализу игр содержательную монографию «Книга об игре в кости» (1526 г.).

Таблица 1.2 – Хронологическое развитие теории управления рисками

Год издания	Наименования научных трудов, нормативных документов и разработок по управлению рисками
1526	Кардано Дж. «Книга об игре в кости»
1654	Паскаль Б. и Ферма П. «Математическое ожидание и теорема сложения и умножения вероятностей»
1657	Гюйгенс Х. «О расчетах в азартной игре или рассмотренная математически стоимость всех шансов при азартных играх в карты, кости, при заключении пари, при участии в лотерее и т. д.»
1693	Галль Э. и Ллойд Э. «Труды о страховании рисков»
1848	Милль Д. «Основы политической экономии с некоторыми приложениями их к социальной философии»
1850	Фон Тюнен И.Г. «Изолированное государство в его отношении к сельскому хозяйству и национальной экономии. Исследование о влиянии хлебных цен, богатства почвы и налогов на земледелие»
1921	Найт Ф. «Риск, неопределенность и прибыль»
1953	Нейман Дж. и Моргенштерн О. «Теория игр и экономическое поведение»
1988	Соглашение «Базель I»
1992	COSO «International Control – Integrated Framework»
1996	Project Management Body of Knowledge. First Edition
1999	Разработка стандарта управления рисками AS/NZS 4360:1999

Окончание таблицы 1.2

Год издания	Наименования научных трудов, нормативных документов и разработок по управлению рисками
2000	Project Management Body of Knowledge. Second Edition
2002	Разработка стандартов управления рисками FERMA, IRM, AIRMIC и ALARM
2004	Соглашение «Базель II»
2004	Project Management Body of Knowledge. Third Edition
2004	Создание модели «COSO ERM»
2005	Пособие PRMIA
2008	Создание модели организованной зрелости в плате управления рисками RIMS
2008	Project Management Body of Knowledge. Fourth Edition
2008	Руководство по передовым стандартам в области управления рисками. Австралийское правительство
2008	BS 311000:2008 «Свод практик для риск-менеджмента» (Великобритания)
2009	ISO 31000:2009. «Risk Management – Principles and Guidelines»
2010	ГОСТ Р ИСО 31000-2010
2010	Management of Risk: Guidance for Practitioners (M_o_R®)
2011	Федеральный закон № 402-ФЗ «О бухгалтерском учете» от 06.12.2011 г.
2013	Project Management Body of Knowledge. Firth Edition
2017	Усовершенствование модели COSO ERM «Enterprise Risk Management. Integrating with Strategy and Performance»
2017	Project Management Body of Knowledge. Sixth Edition
2017	PRojects IN Controlled Environments (PRINCE2®)
2020	О рекомендациях по организации управления рисками … : информационное письмо Банка России от 01.10.2020 г. № ИН-06-28/143

Следует отметить Паскаля Б. и Ферма П., пришедших в 1654 г. к пониманию математического ожидания и формулированию теоремы сложения и умножения вероятностей, Гюйгенса Х., опубликовавшего в 1657 г. труд «О расчетах в азартной игре или рассмотренная математически стоимость всех шансов при азартных играх в карты, кости, при заключении пари, при участии в лотерее и т. д.» [31].

Конец XVII в. характеризуется новым витком развития управления рисками — выходом в свет первых трудов по статистике. В частности, в 1693 г. были опубликованы научные работы

Галля Э., ставшие основой для последующего страхования рисков, и труды страхового агента Ллойда Э., систематизировавшего информацию о крупных сделках и заключившего первые контракты страхования морских рисков [32].

В XVIII в. активно разрабатываются экономические теории, также оказавшие влияние на понимание природы риска. Например, Смит А. в работе «Исследование о природе и причинах богатства народов» пришел к выводу, что представители рисковых профессий, таких как врач и юрист, получают более высокие вознаграждения, чем представители профессий с низким уровнем риска [33].

Английский экономист Милль Д.С. в работе «Основы политической экономии с некоторыми приложениями их к социальной философии» в 1848 г. ввел в оборот термин «плата за риск» [34]. Тюнен И.Г. в 1850 г. опубликовал труд «Изолированное государство в его отношении к сельскому хозяйству и национальной экономии. Исследование о влиянии хлебных цен, богатства почвы и налогов на земледелие», где впервые описал сущность инновационных рисков [35]. Главной идеей данной работы стала классификация рисков на страхуемые риски, под которые могут быть выделены резервы, и нестрахуемые риски, где предприниматель полностью принимает ущерб на себя.

В 1921 г., развивая идеи Тюнена И. о прибыли и риске, Найт Ф. в книге «Риск, неопределенность и прибыль» впервые разделил понятия «риск» и «неопределенность». По его мнению, риск является «измеримой неопределенностью, которой можно управлять» [36]. Новый взгляд на риск предложил ученый Кейнс Дж. М., добавив в деловой оборот такие понятия, как «риск кредитора», «риск заемщика», «риск обесценивания денег» и др. Кроме того, в своем труде «Трактат о вероятности» Кейнс использует такое понятие, как «издержки рисков» [37].

Важным моментом в понимании природы риска стало осознание того, что неопределенность наступает из-за неизвестных желаний и предпочтений людей. Эта концепция составила основу теории игр и нашла отражение в книге Моргенштерна О. и Неймана Дж. и «Теория игр и экономическое поведение» (1953 г.) [38].

В 1988 г. банковский сектор принял консолидированное решение о необходимости регулирования деятельности финансовых

институтов в части управления рисками. В связи с этим Базельским комитетом по банковскому надзору был издан документ «Базель I», в котором рассматривались вопросы о достаточности капитала банков для покрытия расходов по кредитным рискам [29]. Данный свод правил считается первым документом, в котором зафиксирован механизм по оценке, воздействию, мониторингу и контролю рисков.

Управление рисками получило развитие и в проектной деятельности. Например, Project Management Institute (PMI) в 1996 г. выпустил в свет свод знаний проектного управления PMBoK® Guide [13, 14, 15], который с тех пор каждые 4–6 лет корректируется, обновляется и дополняется новыми знаниями. С первого издания PMI уделяет управлению рисками особое внимание. Это во многом связано с тем, что нивелирование негативных рисков значительно повышает шансы на успешное завершение проектов, в связи с чем «*реестр рисков*» и «*план управления рисками*» стали важнейшими проектными документами наравне с уставом проекта, иерархической структурой работ (ИСР), планом управления стоимостью и др. Следует отметить, что с 1996 г. управление рисками в PMBoK® Guide претерпело значительные изменения. Например, сравнительный анализ процессов управления рисками показал, что в последней версии 2017 г. (рисунок 1.9) на «вход» подается план управления проектом, включающий планы из других областей знаний проекта (план управления содержанием, стоимостью, расписанием, качеством и др.). Кроме того, факторы среды организации стали учитывать информацию о *риск-аппетите* (возможный ущерб, который проект готов принять для достижения запланированных целей) и толерантности к рискам (возможный ущерб, который организация способна принять не обанкротившись).

В 2004 г. частная некоммерческая организация COSO выпустила первую версию собственного стандарта по управлению рисками «Управление рисками организации. Интеграция со стратегией и эффективностью деятельности» (COSO ERM — The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management») [17]. Затем в 2017 г. была опубликована обновленная версия «Enterprise Risk Management. Integrating with Strategy and Performance».

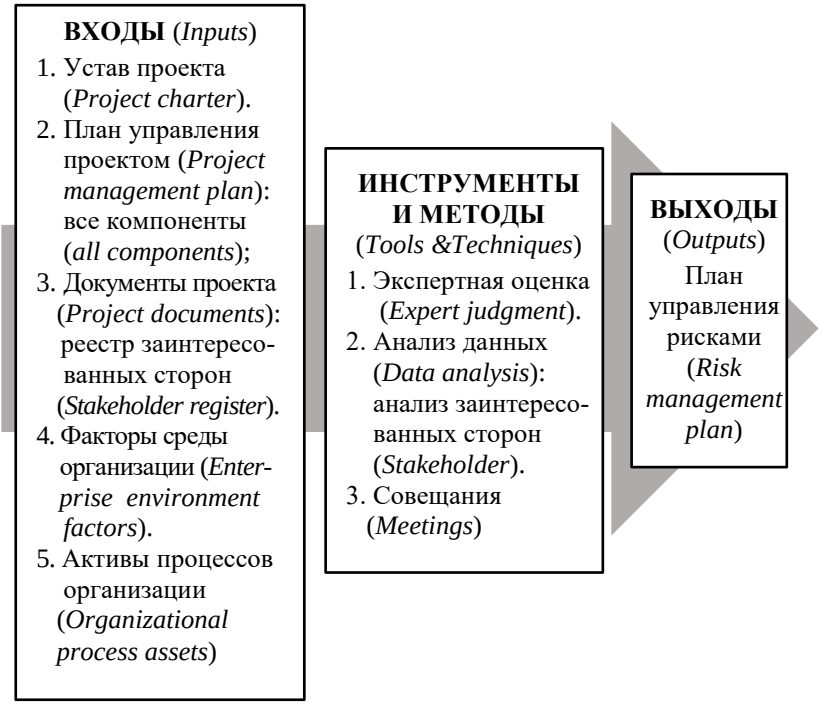


Рисунок 1.9 – Процесс управления рисками
согласно PMBoK® Guide (2017 г.)

1.3. Стандарты управления рисками

Исторически в мире сформировалось несколько школ современной теории управления рисками: американская, австралийская и европейская.

Американская школа управления рисками. Одна из первых ссылок на термин «управление рисками» встречается в американском издании «Harvard Business Review», опубликованном в 1956 г. В этом издании впервые было высказано предположение, что в организациях необходим специальный работник *(риск-менеджер)*, в чьи обязанности должна входить минимизация величины причиненного ущерба [39].

В 1973 г. вслед за нефтяным кризисом стали появляться труды, в которых предлагались первые способы оценки рисков. В частности, опрос промышленников показал, что около 25 % из них создали собственные подразделения по оценке рисков. В банковской сфере в 1975 г. был создан отдельный Комитет по рискам, который стал закреплять лучшие практики оценки рисков.

В конце 1980-х гг. Морган Дж. П. разработал показатель рисковой стоимости для оценки рыночных рисков — Value-at-Risk (VaR).

После серии финансовых скандалов, самым ярким из которых стало банкротство в 2001 г. американской энергетической корпорации Enron Corporation, в 2002 г. был принят закон Sarnabes-Oxey (Сарбейнза-Оксли). Согласно данному закону организации, акции которых размещены на Американском фондовом рынке, обязаны предоставлять Комиссии по ценным бумагам и биржам США (U.S. Securities and Exchange Commission, SEC) подробную информацию о рисках, в том числе в годовых отчетах по форме 10-K [40].

Австралийская школа управления рисками. Первый стандарт по управлению рисками AS/NZS 4360 появился в Австралии в 1995 г. Позднее, в 1999 и 2004 гг., он был обновлен. В 2003 г. Австралийская фондовая биржа опубликовала принципы корпоративного управления, среди которых управление рисками названо одним из восьми важнейших принципов. Затем принципы обновлялись в 2007, 2010 и 2014 гг. В 2009 г. Австралийская фондовая биржа опубликовала отдельное пособие по управлению рисками в рамках программы повышения уровня соответствия принципам корпоративного управления. Тогда же австралийский стандарт по управлению рисками был практически полностью принят за основу международного стандарта ISO 31000:2009.

Европейская школа управления рисками. В 1974 г. была создана ассоциация «European Association of Insureds of Industries», впоследствии переименованная в «Federation of European Risk Management Associations» (FERMA). В 2002 г. был выпущен европейский стандарт по управлению рисками, разработанный The Institute of Risk Management (IRM), The Association of Insurance and Risk Managers (AIRMIC) и ALARM The Nation Forum for Risk Management in the Public Sector.

В 2009 г. был выпущен международный стандарт по управлению рисками ISO 31000:2009. В некоторых европейских странах

(например, в Германии) законодательно закреплено требование о раскрытии в годовых отчетах информации, касающейся системы управления рисками и проведении регулярных независимых аудитов. В 2018 г. стандарт ISO 31000 был обновлен. В рабочую группу вошли представители 63 стран, в том числе представители Российской Федерации. На сегодняшний день ISO 31000 является самым распространенным стандартом по управлению рисками в мире. Стандарт представляет собой обобщенное руководство, призванное обеспечить единообразие управления рисками во всех организациях. Управление рисками в соответствии со стандартом ISO 31000:2018 позволяет организациям:

- повышать вероятность достижения целей;
- совершенствовать процесс выявления возможностей и угроз;
- модернизировать процессы управления;
- соответствовать законодательным и другим обязательным требованиям, международным нормам;
- упорядочивать формирование обязательной и управленческой отчетность;
- укреплять и повышать лояльность заинтересованных сторон;
- эффективно распределять и использовать ресурсы для воздействия на риски;
- повышать безопасность жизни и здоровья работников;
- предотвращать материальные потери и негативные инциденты;
- способствовать повышению устойчивости организации.

Управление рисками в Российской Федерации. В 2010–2012 гг. вышли стандарты по управлению рисками серии ИСО/ГОСТ 31000, включающие методические рекомендации по управлению рисками в малом и среднем бизнесе. В 2013 г. были опубликованы указания о формах, порядке и сроках раскрытия информации о рисках.

Согласно ст. 19 Федерального закона «О бухгалтерском учете» № 402-ФЗ, вступившего в силу с 01.01.2013 г., экономический субъект обязан организовать и осуществлять ***внутренний контроль***, под которым понимается процесс, направленный на получение достаточной уверенности в том, что экономический субъект обеспечивает эффективность и результативность своих действий, в том числе достижение финансовых и операционных показателей,

достоверность и своевременность бухгалтерской (финансовой) отчетности и соблюдение применяемого законодательства, в том числе и в ведении бухгалтерского учета [41].

Основными элементами внутреннего контроля экономического субъекта являются:

- контрольная среда;
- оценка рисков;
- процедуры внутреннего контроля;
- информация и коммуникации;
- оценка внутреннего контроля.

Оценка рисков согласно Федеральному закону «О бухгалтерском учете» № 402-ФЗ представляет собой процесс выявления и анализа рисков. При выявлении рисков экономический субъект обязан принять соответствующее решение по их управлению, в том числе путем создания соответствующей контрольной среды, разработки процедур внутреннего контроля и информирования персонала.

В 2014 г. Банком России был разработан Кодекс корпоративного управления, продекларированными целями которого являются снижение рисков и совершенствование управления рисками. Для достижения этой цели в кодексе закреплен перечень рекомендаций, соблюдение которых позволит выстроить результативную и эффективную систему управления рисками, в частности [42]:

- использование при создании системы общепринятых концепций и практик, в частности COSO и ГОСТ 31000;
- определение советом директоров принципов и подходов организации и утверждение политики в области управления рисками и внутреннего контроля, с последующим использованием утвержденных принципов при принятии решений; определение характера и периодичности пересмотра системы управления рисками и политики в области управления рисками, исходя из целей и задач общества, масштабов его деятельности, принимаемых рисков и изменений в организации деятельности;
- оценивание советом директоров как финансовых, так и нефинансовых рисков, которым подвержено общество, а также определение приемлемой величины рисков для общества;

- обеспечение оптимального баланса между рисками и доходностью с учетом требований законодательства и внутренних документов при утверждении советом директоров политики в области управления рисками, в которой должна быть предусмотрена разумная степень риска для операций и сделок, связанных с повышенным риском.

В 2018 г. Министерство труда и социальной защиты Российской Федерации утвердило Профессиональный стандарт «Специалист по управлению рисками» (Код 08.018).

В 2019 г. Некоммерческим партнерством «Русское Общество Управления Рисками» (НП «РусРиск») опубликован обновленный национальный стандарт ГОСТ Р ИСО 31000-2019 «Принципы и руководство». На сегодняшний день современное семейство национальных стандартов по управлению рисками насчитывает более 20 наименований (таблица 1.3).

Таблица 1.3 – Семейство национальных стандартов по управлению рисками

Код стандарта	Название стандарта
ГОСТ Р 14.09-2005	Экологический менеджмент. Руководство по оценке риска
ГОСТ Р 51901.11-2005	Hazard and operability studies (HAZOP studies) – Application guide
ГОСТ Р 51901.3-2007	Руководство по менеджменту надежности
ГОСТ Р 51901.12-2007	Метод анализа видов последствий отказов
ГОСТ Р 51901.14-2007	Структурная схема надежности и булевы методы
ГОСТ Р ИСО/МЭК 16085-2007	Применение в процессах жизненного цикла систем и программного обеспечения
ГОСТ Р 51901.10-2009	Процедуры управления пожарным риском на предприятии
ГОСТ Р ИСО 31000-2010	Принципы и руководство
ГОСТ Р ИСО/МЭК 31010-2011	Методы оценки риска
ГОСТ Р 51897-2011	Термины и определения
ГОСТ Р 54617.1-2011	Менеджмент риска в наноиндустрии. Общие положения
ГОСТ Р 54617.2-2011	Менеджмент риска в наноиндустрии. Идентификация опасностей

Окончание таблицы 1.3

Код стандарта	Название стандарта
ГОСТ Р 51901.21-2012	Реестр риска. Общие положения
ГОСТ Р 51901.22-2012	Реестр риска. Правила построения
ГОСТ Р 51901.23-2012	Реестр риска. Руководство по оценке риска опасных событий для включения в реестр
ГОСТ Р 55059-2012	Менеджмент риска чрезвычайной ситуации. Термины и определения
ГОСТ Р 55234.2-2013	Менеджмент биориска
ГОСТ Р 55914-2013	Руководство по менеджменту психосоциального риска на рабочем месте
ГОСТ Р ИСО 11231-2013	Вероятностная оценка риска на примере космических систем
ГОСТ Р ИСО 15743-2012	Менеджмент и оценка риска для холодных систем
ГОСТ Р МЭК 62502-2014	Анализ дерева событий
ГОСТ Р МЭК 62508-2014	Анализ влияния на надежность человеческого фактора
ГОСТ Р ИСО 31000-2019	Принципы и руководство

1.4. Классификация рисков

Классификация рисков дает возможность определить место любого риска в общей иерархической структуре рисков. На практике это выражается в оперативном применении наиболее подходящих методов, способов и стратегий управления для конкретной группы рисков. Существуют различные классификации рисков:

1) в зависимости от причин возникновения выделяют:

- ***экономические риски*** — вероятные события, природа которых имеет экономический характер. К экономическим рискам относятся изменение цен на нефть, газ и металлы; дефицит (профицит) консолидированного федерального бюджета Российской Федерации; изменения курса национальной валюты, темпов инфляции, ключевой ставки Банком России, темпов роста экономики, уровня безработицы, уровня жизни населения, фондовых индексов; дефолт; экономический кризис и др.;
- ***общественные риски*** — возможные события, природа которых имеет социально-общественный характер. Яркими примерами

общественных рисков являются отсутствие на рынке труда квалифицированных кадров, социальная напряженность, изменение уровня медицины, преступности, миграции и вероятность наступления голода;

- ***политические риски*** — вероятные события, которые связаны с деятельностью органов государственной власти. К политическим рискам относятся изменение геополитического давления, норм действующего законодательства, возможность террористического акта и др.
- ***природно-естественные риски*** (***экологические риски***) — риски, связанные с силами природы (например, землетрясение, наводнение, ураган, пожар, экстремально высокие или низкие температуры и др.). Кроме того, к природно-естественным рискам можно отнести нехватку природных ресурсов, загрязнение окружающей среды, изменение климата и пандемии;
- ***технологические риски*** — риски внешней среды, природа которых имеет технологический характер. К данным рискам относятся атака искусственного интеллекта (ИИ), отключение электричества и интернета, атака на критическую инфраструктуру и информационную инфраструктуру (КИИ) и др.

В качестве примера атаки на КИИ приведем наиболее опасные хакерские атаки, которые произошли в 2021 г., в частности:

– нападение на компьютерные системы «Colonial Pipeline» (9 мая 2021 г.). Атака поставила под угрозу поставки горючего сразу в нескольких густонаселенных штатах США. В итоге компания была вынуждена отключить часть своих систем и заплатить хакерам выкуп в криптовалюте [43];

– компьютерная атака на одну из крупнейших страховых компаний в США «CNA Financial» (23 мая 2021 г.). Компания была вынуждена заплатить $40 млн хакерам за восстановление доступа к своим системам. По мнению экспертов, это был самый крупный выкуп из известных [44];

– масштабная компьютерная атака на информационные сети МВД Бельгии (26 мая 2021 г.) [45];

– многочисленные кибератаки на североамериканские и австралийские филиалы предприятия по производству мяса «JBS S.A.» (3 июня 2021 г.). В итоге компания была вынуждена заплатить $11 млн выкупа [46];

– хакерской атака на американская сеть «McDonald's» (12 июня 2021 г.), в ходе которой были похищены данные клиентов ее ресторанов в Южной Корее и на Тайване [47];

– хакерская атака на компьютерные сети округа Анхальт-Биттерфельд (Германия) (11 июля 2021 г.), повлекшая введение режима чрезвычайной ситуации. Администрация округа была вынуждена приостановить работу почти на две недели. Вследствие отключения критических информационных систем от сети 157 тыс. чел. временно не смогли получить социальные пособия [48];

2) по масштабу воздействия выделяются:

- ***макориски*** — глобальные риски, последствия от материализации которых отражаются на всех экономических агентах. Например, экономический кризис 2007–2009 гг., начавшийся с ипотечного кризиса в США отразился в итоге на экономике РФ вызвав одно их самых глубоких падений ВВП (–7,8 % в 2009 г.);
- ***мезориски*** — риски, последствия от наступления которых влияют на определенный регион или отрасль экономики;
- ***микориски*** *(предпринимательские риски*) — вероятные события, наступление которых оказывает влияние на экономическую деятельность конкретных экономических агентов. Например, алмазодобывающий холдинг «Алроса» 26 июня 2022 г. не смог выплатить купонный доход по еврооблигациям на сумму $7,75 млн из-за рестрикций США, ЕС и Великобритании [49];

3) по функциональной области организации различают:

- ***внутренние и внешние риски*** — риски, находящиеся внутри либо за пределами организации.;
- ***коммерческие риски*** — непредвиденные расходы (доходы), которые могут быть получены во время ведения финансово-хозяйственной деятельности организаций;
- ***имущественные риски*** — вероятность потери имущества по причине пожара, кражи, диверсии, халатности и др.;
- ***производственные риски*** — возможный ущерб от остановки производства, гибели или повреждения оборудования, полученного брака продукции и др.;
- ***торговые риски*** — возможные убытки из-за задержки или отказа от оплаты товара, непоставки товара, потери имущества во время транспортировки и др.;

- ***транспортные риски*** — вероятность повреждения или потери товара во время перевозки автомобильным, морским, речным, железнодорожным и/или воздушным транспортом;
- ***финансовые риски*** — вероятность получения убытков (прибыли);
- ***инвестиционные риски*** — вероятность неполучения (получения) ожидаемого коммерческого эффекта. При рассмотрении инвестиционных рисков в негативном ключе выявляются следующие их подвиды:

– *риски упущенной выгоды* — возможность получения финансового ущерба в результате неосуществления какой-либо превентивной меры, например страхования, хеджирования др.;

– *риски снижения доходности*, возникающие в результате снижения размера дивидендов по портфельным инвестициям и/или вкладам.

– *риски прямых финансовых потерь*.

– *кредитный риск* — вероятность неуплаты заемщиком основного долга и процентов, причитающихся кредитору. К данному риску относится ситуация, при которой эмитент, выпускающий долговые ценные бумаги, окажется не в состоянии выплачивать процент по ним или основную сумму долга;

- ***комплаенс-риски***. Термин «комплаенс» (от англ. *to comply* — соответствовать) означает соответствие внутренним требованиям организации и внешним нормам действующего законодательства. Возможное несоответствие нормативным актам, правилам, стандартам и кодексам поведения называется комплаенс-рисками. Последствия от наступления этих рисков проявляется в форме юридических санкций со стороны регулирующих и надзорных органов, отраслевых ассоциаций, а также лиц, права и интересы которых были нарушены. Подробная информация о комплаенс рисках и способах их нивелирования приведена в разделе 3;
- ***проектные риски*** — вероятные события, наступление которых оказывает влияние на одну цель проекта либо на их совокупность (содержание, длительность, стоимость и качество проекта). Проектные риски, как правило, возникают из-за действий/бездействий руководителей проектов, участников проектных команд, а также применяемых технологий и оборудования;

4) к рискам, связанным с покупательной способностью денег, относятся:

- ***рыночные риски*** — это риски снижения денежной стоимости капитала, ценных бумаг или портфеля вследствие изменения цен и ставок на рынке;
- ***инфляционные риски*** — вероятность обесценивания реальной покупательной способности денег;
- ***дефляционные риски*** — вероятность усиления реальной покупательной способности денег;
- ***валютные риски*** — вероятность денежных потерь при конвертации одной валюты на другую валюту;
- ***риски ликвидности*** — вероятность неисполнения денежных обязательств в установленном объеме и в согласованный срок;

5) по степени контролируемости риски классифицируются на следующие виды:

- ***неконтролируемые*;**
- ***частично контролируемые*;**
- ***контролируемые*;**

6) в зависимости от наступивших последствий риски могут быть:

- ***негативными*;**
- ***позитивными*;**
- ***смешанными*;**
- ***нейтральными*.**

7) по характеру последствий наступления рисковых событий, в частности, выделяют:

- ***чистые риски*** — вероятные события, которые могут привести к наступлению проблемных последствий;
- ***спекулятивные риски*** — вероятные события, которые могут привести к наступлению как проблемных, так и благоприятных последствий;

8) в зависимости от частоты наступлений в ранее заключенных сделках и завершенных проектах различают:

- ***универсальные риски*** — вероятные события, которые актуальны для любой сделки и проекта независимо от его масштаба, сложности, длительности, типа, способов управления и численности участников команды;

- ***специальные риски*** — вероятные индивидуальные события, которые актуальны для частной сделки или проекта;

9) в зависимости от времени актуализации (наступления) рисков относительно фаз жизненного цикла проекта выделяют:

- ***постоянные риски*** — вероятные события, которые имеют потенциал материализоваться в любой временной период выполнения проекта;
- ***риски, связанные с фазой жизненного цикла,*** — вероятные события, которые могут материализоваться только во время определенной фазы жизненного цикла проекта.

Руководители проектов в области ИТ Артем и Михаил во время обеденного перерыва обсуждали текущее положение дел в их проектах. Артем сообщил Михаилу: «Я пришел к выводу, что план мне в проекте не нужен. Все равно не получается следовать ему. Стоит только согласовать с заказчиком сроки, так на следующий день происходит какое-нибудь событие, которое все меняет. В пятницу будет видеоконференция с заказчиком. Придется снова краснеть».

Михаил уточнил: «О каких событиях идет речь?». – «Например, вчера моего ведущего программиста вдруг привлекли на другой проект, – ответил Артем. – На прошлой неделе выяснилось, что на этапе сбора требований мы не выявили очень важный бизнес-процесс, из-за чего теперь часть работ мы не можем выполнить, пока не обновим техническое задание. И это еще не все.

*Над техническим заданием сейчас никто не работает, потому что наш штатный аналитик Алексей занят более приоритетными задачами и, по его словам, он сможет приступить к спецификации только через две недели». Михаил задумался и потом спросил: «**Когда ты разрабатываешь свои планы, ты учитываешь риски**?».*

Случай из практики

2. ПРОЦЕССЫ УПРАВЛЕНИЯ РИСКАМИ

2.1. Анализ внутренней и внешней среды объектов риска

Эффективное и результативное управление рисками возможно, когда ясны и понятны цели организации (проекта), которые требуется достичь. Например, главной целью коммерческих организаций в соответствии с условиями ст. 50 ГК РФ является извлечение прибыли [21]. Согласно PMBOK® Guide целями проекта являются объем и стоимость запланированных работ, срок их выполнения, а также качество создаваемого результата, оказываемой услуги и/или поставляемого товара [13, 14, 15].

Рассмотрим пример достижения цели. Предположим, что субъект желает совершить переход из состояния A в состояние B.

Достичь желаемого состояния субъект планирует спустя время T_1. Желаемое состояние B является для субъекта его целью (рисунок 2.1).

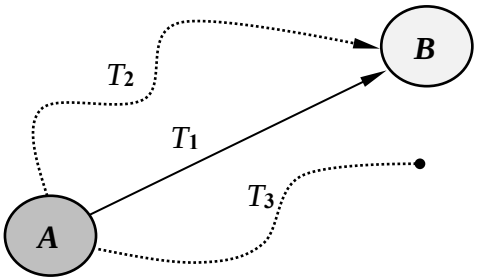


Рисунок 2.1 – Переход субъекта
из состояния *A* в состояние *B*

После того как субъект начнет движение к поставленной цели, для него будут актуальны следующие сценарии развития событий:

- **сценарий 1**. При достижении цели ничего не произойдет и субъект благополучно спустя запланированное время T_1 ее достигнет. Этот сценарий маловероятен, потому что на процесс достижения цели будут влиять различные штатные и нештатные ситуации. Например, цель изменится, будут отсутствовать необходимые компетенции, ключевой сотрудник будет занят на других проектах и др. Если эти ситуации наступят, тогда для субъекта будут актуальны иные сценарии;
- **сценарий 2**. При достижении цели наступили события, которые повлияли на процесс достижения целей и запланированное время. В результате субъект достигнет цели через T_2. Если наступившие события были негативными, то $T_2 > T_1$, если позитивными — $T_2 < T_1$. Подобный сценарий может считаться допустимым, если риск-аппетит и толерантность к риску приемлемы для субъекта. Однако если материализовавшиеся события окажут значительный материальный ущерб, то субъект не достигнет запланированной цели;
- **сценарий 3.** При достижении цели наступили события, не позволившие субъекту достичь запланированной цели. Для субъекта подобный сценарий является неприемлемым и недопустимым. В связи с этим логично предположить, что прежде чем приступить к достижению цели, субъекту необходимо заранее выявить события, которые могут оказать воздействие на данный процесс;

- **сценарий 4**. Прежде чем приступать к достижению цели субъект продумал наиболее безопасное движение и заблаговременно выявил события, которые могут повлиять на данный процесс. Кроме того, для повышения шансов на успех субъект запасся дополнительными ресурсами на случай, если наступят непредвиденные события (рисунок 2.2). Возможно, достижение цели в рамках сценария 4 потребует б*о*льших временных затрат T_4, однако субъект гарантированно достигнет желаемой цели. Подобный процесс достижения целей называют ***риск-ориентированным***.

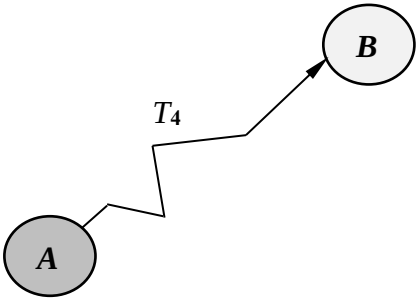


Рисунок 2.2 – Риск-ориентированный переход
субъекта из состояния A в состояние B

На основании рассмотренного примера можно заключить, что при управлении рисками для имплементации[1] процесса «Анализ внутренней и внешней среды объектов риска» необходимо вначале определить цели субъекта, которые он собирается достичь.

Далее требуется провести анализ внутренней среды. Для проектов и организаций этот процесс различен. В частности, для того чтобы провести анализ внутренней среды проекта, достаточно сравнить текущий статус выполненных работ (оказанных услуг) с запланированным и установить, все ли идет по графику и есть ли отклонения. Организация, являясь структурно сложным объектом, требует иного подхода. Чтобы определить текущее внутреннее

[1] Имплементация (от англ. от англ. *implementation* — осуществление, выполнение) — это реализация на практике, т. е. претворение в жизнь какой-либо теории, договора, закона или идеи.

состояние организации, необходимо определить долю рынка, объемы сбыта, качество рекламы, размер прибыли, уровень компетентность работников и др. Инструментом, позволяющим провести анализ внутренней среды организации, является ***комплексное управленческое обследование,*** предполагающее анализ 11 областей деятельности организации, к которым относятся:

1) доля рынка и конкурентоспособность;
2) разнообразие и качество ассортимента;
3) предпродажное и послепродажное обслуживание клиентов;
4) эффективный сбыт, реклама и продвижение товара;
5) прибыль;
6) финансовое состояние;
7) капитал (офисы, оборудование, интеллектуальная собственность и др.);
8) технологии;
9) управление;
10) персонал;
11) корпоративная культура.

Одним из способов, позволяющих определить текущее состояние внутренней среды, является анализ жизненного цикла организации (проекта). Ж**изненный циклом (ЖЦ)** — это набор фаз, через которые проходит организация (проект) с момента ее (его) открытия до момента закрытия. ***Фаза*** — совокупность операций, задач, действий и событий, завершающихся достижением одного или нескольких запланированных результатов. Определение фазы жизненного цикла позволяет идентифицировать этап развития организации (проекта) и оценить перспективы. Жизненные циклы для проектов и организаций также отличаются.

В **жизненном цикле организации** выделяют пять фаз, для каждой из которых характерны собственные цели (рисунок 2.3):

1) ***становление*** — выход на рынок и выживание;
2) ***развитие*** — формирование индивидуального бренда, захват части рынка, увеличение заработной платы сотрудников, стабилизация трудового коллектива. Эта фаза характеризуется устойчивым ростом доходов и расширением географии сбыта;
3) ***зрелость*** — расширение рынка по разным направлениям. Как правило, организация входит в фазу зрелости, когда доходы ее становятся стабильными и могут быть спрогнозированы;

4) **упадок** — сохранение и поддержание достигнутого ранее уровня;

5) ***закат*** — реинжиниринг основных направлений деятельности. Считается, что организация входит в фазу заказа, когда ее расходы начинают превышать доходы.

Рисунок 2.3 – Модель жизненного цикла организации

Согласно PMBOK® Guide универсальными фазами проекта считаются: *начало проекта; организация и подготовка проекта; выполнение работ по проекту; окончание проекта* [13, 14, 15].

Исследования 11 ИТ-проектов позволили установить, что на разных фазах жизненного цикла может материализоваться различное количество рисков (рисунок 2.4) [50]. Общее количество универсальных рисков, актуальных для данных ИТ-проектов, составило 99 рисковых событий. По итогам анализа было установлено, что фаза «Организация и подготовка проекта», в которой могут наступить порядка 64 рисков, является самой опасной фазой проекта. Кроме того, была выявлена группа ***постоянных рисков***, которые могут материализоваться в любой временной период выполнения проекта. Подробнее с результатами исследования можно ознакомиться в работе «Негативные и позитивные риски в ИТ-проектах» [50].

После того как определены цели, установлено текущее внутреннее состояние и фаза жизненного цикла, необходимо провести анализ внешней среды.

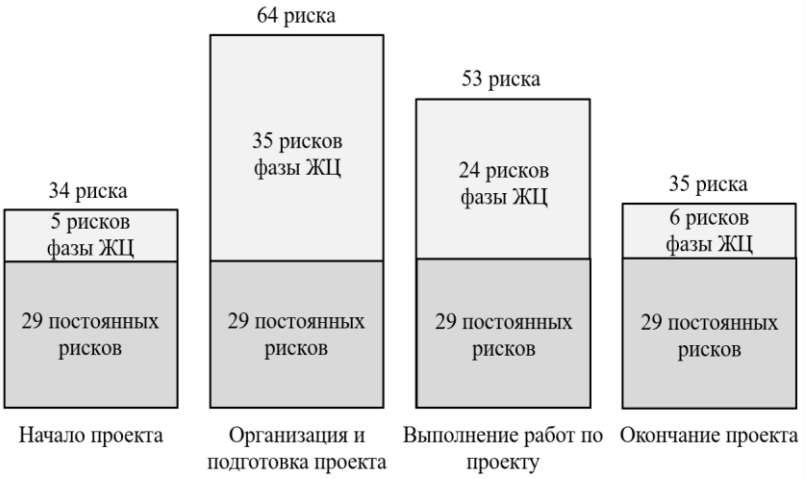


Рисунок 2.4 – Распределение рисков
относительно фаз жизненного цикла проекта

Внешние среды для проекта и организации различны. Например, для проведения анализа внешней среды проекта достаточно оценить текущие интересы, цели и ожидания внешних заинтересованных сторон. Согласно международному своду лучших практик управления проектами PMBOK Guide®, под ***заинтересованными сторонами проекта*** понимаются физические и/или юридические лица, которые активно участвуют в проекте либо интересы которых могут быть затронуты в ходе выполнения проекта или по его завершению.

Определение текущего состояния внешней среды организации является более трудоемким, так как требует выявления и анализа экономических, политических, социально-общественных, природно-естественных и технологических факторов, которые способны влиять на ее деятельность (рисунок 2.5). Прямое и косвенное воздействие факторов внешней среды на деятельность организации создают ***внешние риски*** (риски изменения действующего законодательства, темпов инфляции, ключевой ставки ЦБ, курса национальной валюты, рестрикции, риск отсутствия на рынке труда квалифицированных кадров и др. Примеры внешних рисков представлены в приложении 2.

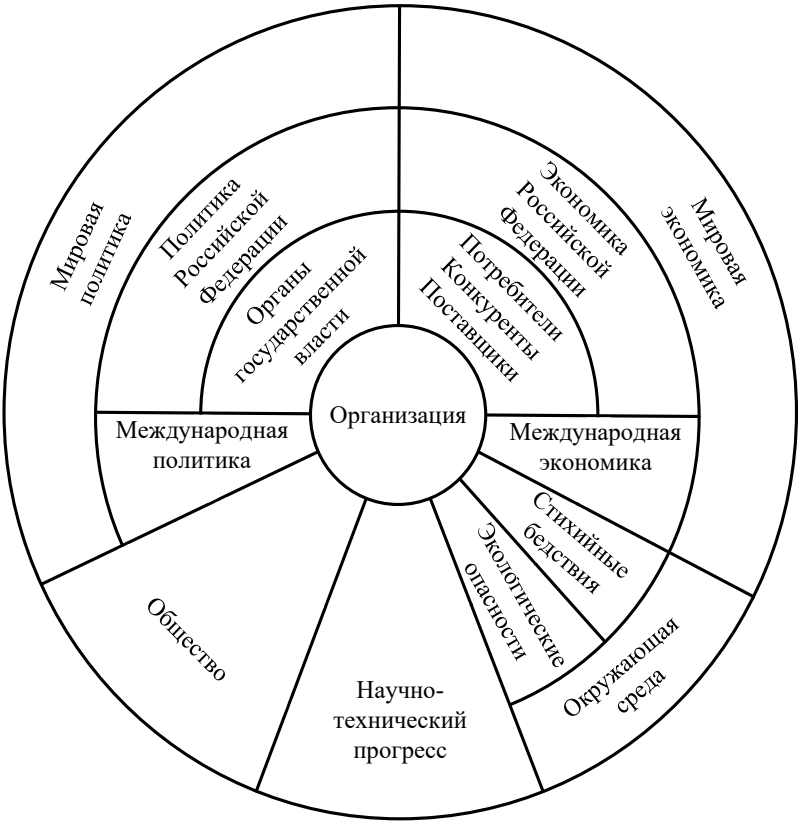


Рисунок 2.5 – Модель влияния факторов внешней среды на деятельность организации

2.2. Идентификация рисков

Одним из наиболее кропотливых процессов управления рисками считается идентификация рисков. По мнению Ключникова В.О., сложность выявления рисков вызвана уникальностью бизнес-процессов [51, 52, 53]. Ученый в своих трудах отмечает, что время, затраченное на выявление рисков, представляет собой инвестицию в успех, так как неучтенные риски при материализации помешают достижению запланированных целей. Для выявления

рисков отечественные и зарубежные ученые рекомендуют применять различные методы и их комбинации в зависимости от специфики бизнес-процессов.

Примеры методов идентификации рисков представлены в таблице 2.1.

Таблица 2.1 – Методы идентификации рисков

Название метода		Разработчики
на английском языке	в переводе на русский	
1. Retrospective	Ретроспективный анализ документов	Никонов В.А. [54]
2. Brainstorming	Мозговой штурм	Осборн А. [55]
3. Delhi	Метод «Дельфи»	Хелмер О. [55]
4. SWOT matrix	SWOT-анализ	Эндрюс К. [55]
5. STEEP matrix (PEST matrix)	STEEP-анализ / PEST-анализ	Портер М. [55]
6. Hazard and Operability Study (HAZOP)/Control Hazards and Operability Analysis или Computer Hazard and Operability Analysis (CHAZOP)	Исследование компьютерной опасности и работоспособности систем	Клетз Т. [56]
7. Structured What-If Technique (SWIFT)	Структурированный анализ сценариев методом «Что, если?»	Лавли Ф. [57]
8. Preliminary Hazard Analysis (PHA)	Предварительный анализ опасностей для систем	Хенкли Э. Дж., Кумамото Х. [55]

Рассмотрим методы, представленные в таблице 2.1, подробнее.

Ретроспективный анализ документов (Retrospective). Анализ документов, например договоров и реестров рисков ранее заключенных сделок и завершенных проектов, позволяет оперативно выявить уже наступившие риски, которые материализовались и оказали влияние на достижение запланированных целей. Пример реестра 170 универсальных рисков, выявленных при анализе 192 судебных решений и изучении бизнес-деятельности 495 ИТ-организаций Томской области (ОКВЭД: 62.0), представлен в приложении 3.

Метод «Мозговой штурм» (Brainstorming) является коллективным и творческим. Основные преимущества метода — выявление специальных рисков, легкость применения, коллаборация (сотрудничество) участников (рисунок 2.6). В числе недостатков можно отметить низкое качество процесса идентификации рисков.

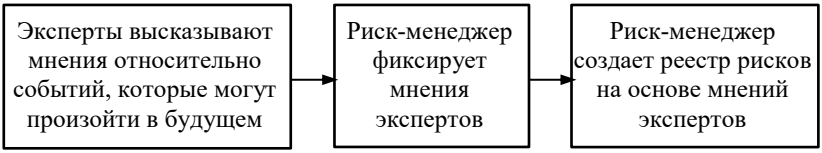


Рисунок 2.6 – Идентификация рисков
с помощью метода «Мозговой штурм»

Метод «Дельфи» (Delhi), созданный в 60-е гг. XX в. сотрудниками RAND Corporation, изначально разрабатывался как метод прогнозирования трендов развития технологий. Однако по прошествии времени метод показал свою результативность во время выявления рисков. Особенность метода заключается в том, что эксперты могут индивидуально и анонимно выражать свое мнение, имея при этом возможность узнавать мнения и идеи друг друга, что позволяет выявлять специальные риски, которые обычно не принято озвучивать (рисунок 2.7).

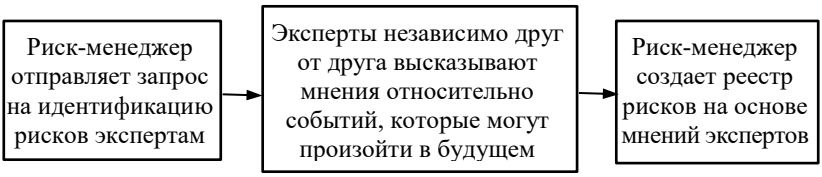


Рисунок 2.7 – Идентификация рисков
с помощью метода «Дельфи»

SWOT-анализ. Данный метод позволяет выявлять не только сильные и слабые стороны, но и возможности (позитивные риски) и угрозы (негативные риски). На практике SWOT-анализ усиливают **STEEP-анализом**, который предоставляет возможность исследовать в том числе социальные, технологические, экономические, экологические и политические риски.

Hazard and Operability Study (HAZOP). Клетз Т. при разработке HAZOP [56] в первую очередь стремился избежать промышленных инцидентов, таких как пожары, выбросы вредных веществ и утечки химикатов. Пример идентификации рисков с помощью CHAZOP представлен в таблице 2.2.

Таблица 2.2 – Идентификация рисков с помощью CHAZOP

Тип отклонения	Управляющее слово	Примеры отклонений для ИТ-проекта
1. Отрицательный	НЕТ	НЕТ информации, которая необходима для реализации ИТ-продукта
2. Количественные изменения	БОЛЬШЕ	Источников, в которых хранится актуальная информация о проекте, БОЛЬШЕ, чем необходимо
	МЕНЬШЕ	Сотрудников в проекте МЕНЬШЕ, чем необходимо
3. Качественные изменения	ТАК ЖЕ, КАК	Ожидается отклонение от запланированных сроков ТАК ЖЕ, КАК и в проекте, который был завершен ранее
	ЧАСТЬ	Доступна только ЧАСТЬ актуальной информации, необходимой для создания ИТ-продукта
4. Замена	ПЕРЕМЕНА	В процессе реализации ожидается ПЕРЕМЕНА запланированных требований
	ДРУГОЙ	Проектом будет управлять ДРУГОЙ руководитель
5. Время	РАНО	Реализация проекта будет начата слишком РАНО
	ПОЗДНО	Реализация проекта будет начата слишком ПОЗДНО
6. Порядок (последовательность)	ПРЕЖДЕ, ЧЕМ	Заказчик будет знакомиться с разработанным инкрементом программного кода ПРЕЖДЕ, ЧЕМ завершится тестирование
	ПОСЛЕ	Актуальная информация поступит ПОСЛЕ разработанных функций

Со временем метод доказал свою работоспособность, и в 1974 г. HAZOP вошел в состав обязательных методов, применяемых для идентификации рисков. Позднее метод был адаптирован и для разработки программ для ЭВМ, получив название «Computer Hazard and Operability Analysis (CHAZOP)».

Structured What-If Technique (SWIFT). Анализ сценариев развития последствий в результате наступления рисков с помощью метода SWIFT является упрощенной версией CHAZOP. Такие фразы, как «Что, если … ?» «К чему это приведет … ?», «Что случится, если … ?», «Может ли кто-либо … ?», «Может ли что-либо … ?», помогают выявить возможные последствия в случае наступления риска.

Идентификация возможных последствий для риска «На стороне Заказчика будут отсутствовать ключевые и квалифицированные специалисты» с помощью метода SWIFT представлена на рисунке 2.8.

Рисунок 2.8 – Идентификация последствий
в результате наступления риска с помощью метода SWIFT

Главными достоинствами метода SWIFT является простота использования, так как метод не требует предварительной подготовки, а также его графическое исполнение, что стимулирует творческий процесс.

Preliminary Hazard Analysis (PHA). Метод PHA направлен на выявление угроз, способных причинить вред используемому оборудованию или разрабатываемой программе для ЭВМ. Благодаря определению критических контрольных точек с помощью метода определяются стадии, требующие создания дополнительных профилактических мер, нивелирующих угрозу наступления катастрофических рисков. Согласно методу PHA выделяется три класса рисков:

1) безопасные вероятные события, которые не могут оказать негативное влияние;

2) пограничные вероятные события, которые, например, не вызывают поломки оборудования, но сказываются на качестве выполненной работы;

3) критические вероятные события (поломка оборудования, уход ключевого сотрудника, отсутствие финансирования и др.)

Пример использования метода PHA представлен в таблице 2.3.

Таблица 2.3 – Идентификация рисков с помощью метода PHA

Опасный элемент	Событие, вызывающее опасное состояние	Последствия	Класс опасности
Персонал	Уход ключевого сотрудника в процессе выполнения работ	Остановка выполнения работ	Третий
Оборудование	Поломка оборудования	Остановка выполнения работ	Второй
Оборудование	Отключение интернета	Потеря связи с сервером. Потеря связи с Заказчиком	Первый
Заказчик	Отказ от оплаты	Остановка выполнения работ. Судебный спор	Третий
Руководитель проекта	Руководитель проекта занят на других проектах	Отставание от запланированных сроков	Второй

Каждый из представленных методов идентификации рисков направлен на выявление определенных рисковых событий. При решении проблемы применимости методов для выявления акту-

альных для организации и/или проекта рисков рекомендуется использовать различные методы и привлекать сторонних экспертов [58, 59, 60].

Выявленные риски рекомендуется заносить в раздел «Идентификация» в реестре рисков, фиксируя при этом тип, название, описание, класс и дату идентификации риска (таблица 2.4).

Таблица 2.4 – Пример раздела «Идентификация» реестра рисков

Тип / Название риска	Описание риска	Класс риска	Дата идентификации риска
1. Негативный / Риск изменения условий контрактов сотрудников	Профсоюз работников кафетериев может потребовать пересмотра контрактов сотрудников кафетерия для того, чтобы они отражали новое распределение обязанностей и графиков работы кафетерия	Комплаенс-риск	хх.хх.хххх
2. Негативный / Риск того, что выполненная работа (оказанная услуга) не принесет ожидаемого коммерческого эффекта	Слишком мало работников могут сразу принять новую программу для ЭВМ, что уменьшит прибыль от инвестиций в разработку этой программы	Коммерческий риск	хх.хх.хххх
3. Негативный / Риск того, что партнеры откажутся от сотрудничества	Близлежащие рестораны могут не согласится предоставить скидки, что уменьшит удовлетворенность работников программой для ЭВМ	Коммерческий риск	хх.хх.хххх
4. Негативный / Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям конечного пользователя	Имеющихся возможностей программы для ЭВМ может оказаться недостаточно, из-за чего сотрудники не всегда смогут получать свои заказы и заказывать доставку в нужное время	Коммерческий риск	хх.хх.хххх

2.3. Анализ рисков

Процесс анализа рисков направлен на установление источников рисков, причин, создающих риски, и возможных последствий в случае их наступления. Оптимальными методами для проведения анализа считаются «Галстук-бабочка» (первый этап) и «Почему-почему» (таблица 2.5) [61, 62], что отмечается в ГОСТ Р 31010-2011 «Методы оценки риска» [63].

Таблица 2.5 – Методы, применяемые для анализа рисков

Название метода		Разработчики
Оригинал (англ.)	В переводе на русский	
Bow-tie	«Галстук-бабочка» (первый этап)	Лангминд Б. [61]
5Why	«Почему-почему»	Тоеда С. [62]

Метод «Галстук-бабочка» (Bow-tie) состоит из двух этапов:

1) анализ рисков — определение причин, создающих риски, и источников рисков; прогнозирование возможных последствий в случае их наступления;

2) разработка «барьеров», направленных на локализацию источников рисков, и «мер восстановления (усиления)», призванных оперативно локализовать причиненный ущерб (усилить благоприятный эффект). Второй этап метода применяется в процессе воздействия на риски во время разработки мер плана А и плана Б.

Пример анализа риска «Изменение требований в процессе выполнения работ (оказания услуг)» с помощью метода «Галстук-бабочка» (первый этап) представлен на рисунке 2.9.

Метод «Почему-почему» (5Why) был предложен Тоёда С. с целью повышения качества продукции фирмы «Тойота». Впоследствии метод стал применяться и в других сферах. Суть метода заключается в последовательном задавании вопроса «Почему есть вероятность наступления этого риска?» для того, чтобы определить источник риска. Если источник риска во время первой итерации не устанавливается, тогда процедура повторяется.

Пример анализа риска «По факту проектные работы окажутся значительно сложнее, чем предполагалось изначально» представлен в таблице 2.6.

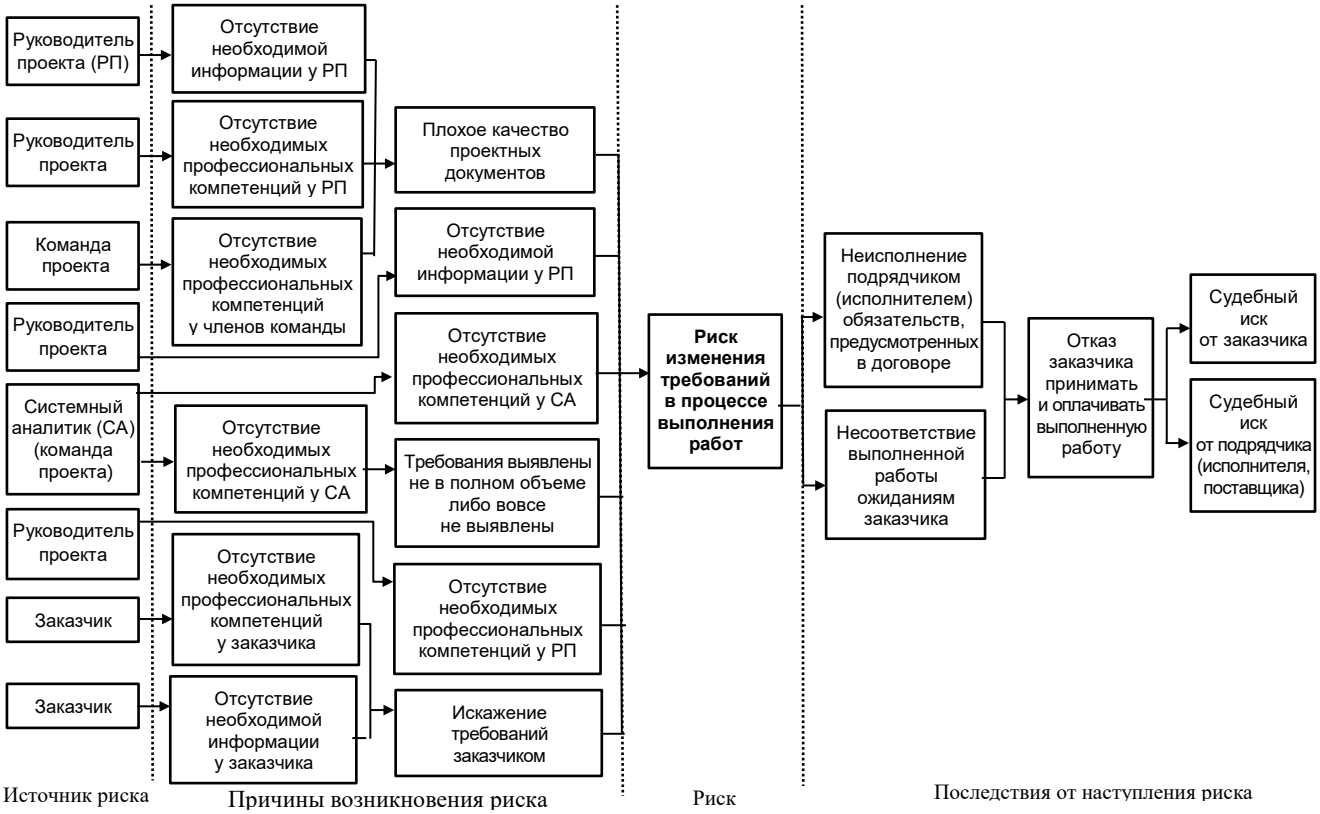


Рисунок 2.9 – Анализ риска с помощью Bow-tie (первый этап)

Таблица 2.6 – Анализ риска с помощью метода «5Why»

Название риска	Почему есть вероятность наступления этого риска?	Повторный вопрос: Почему есть вероятность наступления этого риска?	Источник риска
Риск того, что по факту проектные работы окажутся значительно сложнее, чем предполагалось изначально	Руководитель проекта может не иметь необходимых профессиональных компетенций	Нет ответа	Руководитель проекта
	У руководителя проекта не будет необходимой информации	Нет ответа	Руководитель проекта
	Требования могут быть выявлены не в полном объеме либо вовсе не выявлены	Системный аналитик не будет иметь необходимых профессиональных компетенций	Системный аналитик (команда проекта)
	Проектные документы могут быть плохого качества	У руководителя проекта не будет необходимой информации	Руководитель проекта
		Руководитель проекта может не иметь необходимых профессиональных компетенций	Руководитель проекта
		Команда проекта может не иметь необходимых профессиональных компетенций	Команда проекта

Анализ коммерческих, комплаенс-рисков и проектных универсальных рисков (приложение 3**)** методом «Почему-почему» позволил установить, что источниками рисков являются заинтересованные стороны проекта (рисунок 2.10), а именно:

- конечный пользователь;
- заказчик;
- руководитель проекта;
- команда проекта;
- субподрядчик;
- конкурент.

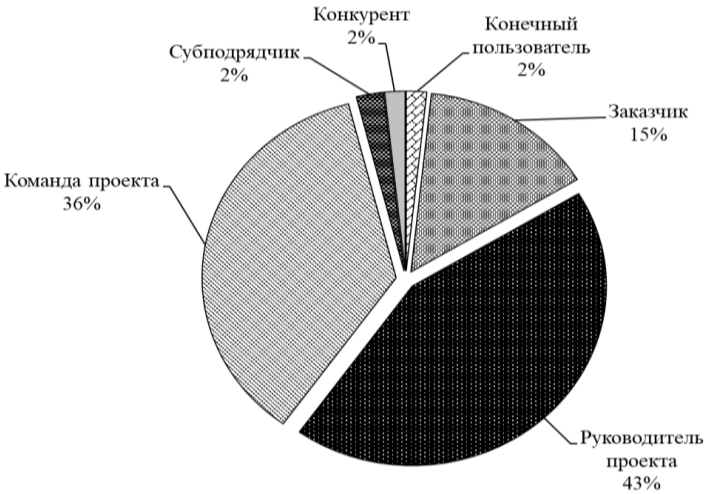


Рисунок 2.10 – Источники универсальных рисков, актуальных для проектов

Результаты анализа рекомендуется заносить в раздел «Анализ» реестра рисков, фиксируя следующую информацию:

- тип риска,
- название риска,
- причины, создающие риск,
- источники риска,
- последствия от наступления риска.

Пример раздела «Анализ» реестра рисков представлен в таблице 2.7.

Таблица 2.7 – Пример раздела «Анализ» реестра рисков

Тип риска / Название риска	Причины, создающие риск	Источники риска	Последствия от наступления риска
1. Негативный / Риск изменения условий контрактов сотрудников	Влияние конкурентов	Конкурент	Изменение лояльности работников
	Изменение бизнес-контекста	Рынок	Изменение лояльности работников
	Профсоюз защищает интересы и права работников	Профсоюз	Пересмотр контрактов, отражающий новое распределение обязанностей и графиков работы кафетерия
2. Негативный / Риск того, что выполненная работа (оказанная услуга) не принесет ожидаемый коммерческий эффект	У работников недостаточно профессиональных компетенций	Работники	Уменьшение прибыли от инвестиций в разработку программы для ЭВМ
3. Негативный / Риск того, что партнеры откажутся от сотрудничества	Партнерам будет невыгодно предоставлять скидки	Партнеры	Уменьшение удовлетворенности работников программой для ЭВМ
4. Негативный / Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям конечного пользователя	Нет необходимого функционала в программе для ЭВМ	Программа для ЭВМ	Работники не всегда смогут получать свои заказы и заказывать доставку в нужное время

2.4. Оценивание рисков

Представим, что в процессе идентификации рисков было выявлено большое количество рисков и что после проведения анализа стало очевидно, что не все они одинаково важны. Например, риск возможного ухода ключевого сотрудника будет представлять для нас б*о*льший интерес, нежели отключение электричества или интернета. В связи с этим логично предположить, что выявленные риски следует определенным образом сгруппировать для того, чтобы выделить среди них группу наиболее опасных рисков, группу рисков, требующих постоянного управленческого внимания, группу незначительных рисков, которые можно не учитывать и др. Для решения данной проблемы применяют оценивание рисков.

Согласно ГОСТ Р 31010-2011 оцениваются две основные характеристики риска [63]:

1) **вероятность материализации риска**;

2) **возможное влияние в случае его наступления**.

Измерение степени вероятности и влияния риска осуществляется с помощью специальных количественных и качественных методов.

Количественные методы — это методы, использующие математический аппарат для прогнозирования вероятности материализации рисков и возможного влияния в случае их наступления. В частности, количественные методы оценивания рисков представляют вероятность материализации рисков как величину, которая рассчитывается по формуле

$$P(A) = \frac{m}{n}, \qquad (2.1)$$

где $P(A)$ — вероятность наступления события A;

m — число исходов испытания, благоприятствующих событию A;

n — число всех равновозможных несовместных исходов испытания, образующих полную группу.

Примерами количественных методов являются:

- математическое ожидание;
- дисперсия и среднеквадратическое отклонение;

- полудисперсия;
- Value-at-Risk (VaR).

Качественные методы — это методы, в которых используются экспертные мнения для оценивания характеристик вероятностей и влияний рисков. Как правило, качественные методы применяются в случаях, когда наблюдается большая неопределенность, отсутствует необходимая информация и/или нет накопленных статистических данных о ранее наступивших рисках.

При работе с качественными методами оценивания рисков используют весовые коэффициенты, базирующиеся на вербально-числовой шкале Харрингтона. Примеры коэффициентов Харрингтона для оценок степени вероятности и влияния представлены в таблицах 2.8 и 2.9.

Таблица 2.8 – Коэффициенты оценивания вероятности материализации риска

Вероятность наступления риска	Коэффициент Харрингтона		Комментарии
	PMBOK® Guide	Merna T. и Al-Thani F. [64]	
Очень высокая	0,8–1,0	5	Гарантированное наступление риска
Высокая	0,64–0,8	4	Высокая вероятность наступления риска
Средняя	0,37–0,64	3	Нет гарантий, что риск наступил, но все же такая возможность остается
Низкая	0,2–0,37	2	Остается возможность наступления риска
Очень низкая	0,1–0,2	1	Остается малая возможность наступления риска
Нет вероятности	0,0–0,1	0	Вероятность наступления риска отсутствует

Для увеличения точности рекомендуется получение трех видов экспертных оценок:

1) оптимистической;
2) наиболее вероятной (реалистической);
3) пессимистической.

Таблица 2.9 – Коэффициенты оценивания возможного влияния в случае наступления риска

Влияние риска в случае наступления	Коэффициент Харрингтона		Комментарии
	PMBOK ® Guide	Merna T., Al-Thani F. [64]	
Очень высокая	0,8–1,0	5	Работы полностью остановлены. Причинен катастрофический материальный ущерб
Высокая	0,64–0,8	4	Работы выполнены, но с большим опозданием. Причинен значительный материальный ущерб
Средняя	0,37–0,64	3	Есть задержка в выполнении работ. Причинен материальный ущерб
Низкая	0,2–0,37	2	Работы выполнены с небольшим опозданием. Ущерб незначительный
Очень низкая	0,1–0,2	1	Есть незначительные отставания от намеченного расписания и бюджета
Нет влияния	0,0–0,1	0	Материальный ущерб отсутствует

Полученные оценки необходимы для применения формулы расчета вероятности и влияния PERT (Project Evaluation and Review Technique):

$$A_{ij} = \frac{a_i^o + 4a_i^r + a_i^p}{6} \quad (2.2)$$

$$B_{ij} = \frac{b_i^o + 4b_i^r + b_i^p}{6} \quad (2.3)$$

где a_i^o, a_i^r и a_i^p — оптимистическая, реалистическая и пессимистическая оценка вероятности материализации риска;

b_i^o, b_i^r и b_i^p — оптимистическая, реалистическая и пессимистическая оценка возможного влияния в случае наступления риска;

A_{ij} — расчетное значение вероятности материализации i-го риска по мнению j-го эксперта;

B_{ij} — расчетное значение возможного влияния в случае наступления i-го риска по мнению j-го эксперта;

i и j — номер риска и номер эксперта соответственно.

Далее для каждого риска рассчитывается среднее арифметическое значение вероятности материализации риска и возможного влияния в случае его наступления:

$$A_i = \frac{\sum_{j=1}^{n} A_{ij}}{n}, \tag{2.4}$$

$$B_i = \frac{\sum_{j=1}^{n} B_{ij}}{n} \tag{2.5}$$

где n — количество экспертных мнений.

Для визуализации полученных оценок используется специальный инструмент — ***матрица рисков***, которая применяется Министерством обороны США (The Department of Defense United States of America — DoD) в виде, представленном на рисунке 2.11 [65].

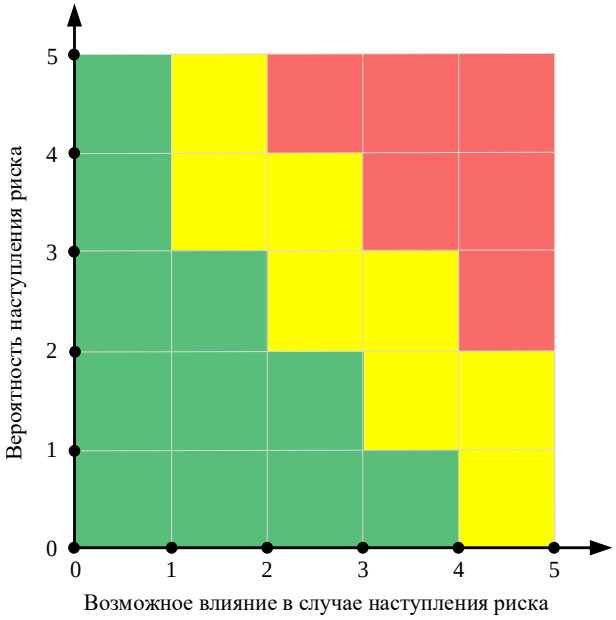


Рисунок 2.11 – Матрица рисков Министерства обороны США

Следует отметить, что DoD рассматривает риск только в негативном ключе, поэтому матрица рисков имеет три группы:

1) ***красная***. Риски «красной» группы самые опасные, способные нанести катастрофический ущерб;

2) ***желтая***. Риски «желтой» группы умеренные, способные нанести приемлемый ущерб;

3) ***зеленая***. Риски «зеленой» группы безопасны.

Merna T. и Al-Thani F. предлагают распределять негативные риски на четыре группы [64]:

1) ***катастрофические риски, или «тигры»*** (tiger), — негативные риски, которые имеет высокую вероятность материализации и способны оказать значительное негативное влияние в случае их наступления. По мнению Merna T. и Al-Thani F, материализация одного «тигра», например «Проект покинул руководитель проекта», способна привести к полной остановке работ (оказания услуг, поставке товаров);

2) ***непредсказуемые риски, или «аллигаторы»*** (alligator), — негативные риски, имеющие низкую вероятность материализации, но обладающие способностью оказывать значительное негативное влияние. Как правило, к «аллигаторам» относятся комплаенс-риски. Например, организация, реализующая проект, может получить штраф в связи с нарушением императивных норм (ч. 1, ст. 9.5 КоАП РФ; ч. 3, ст. 14.1 КоАП РФ и ст. 15.33.2 КоАП РФ) [66] и др.;

3) ***часто встречаемые риски, или «щеночки»*** (puppy), — негативные риски, которые имеют высокую вероятность материализации, но при этом не способны оказывать какое-либо значительное влияние. Примерами часто встречаемых рисков могут быть риски, связанные с социально-психологической атмосферой в команде проекта, внутренней мотивацией, конфликтами и др.;

4) ***несущественные риски, или «котята»*** (kitten), — это негативные риски, которые имеют низкую вероятность материализации и при этом не обладает способностью оказывать какое-либо значительное влияние. По мнению Merna T. и Al-Thani F., «котята» не способны хоть как-то навредить проекту, поэтому данными негативными рисками можно пренебречь [64].

Матрица вероятности и влияния Merna T. и Al-Thani F. представлена на рисунке 2.12.

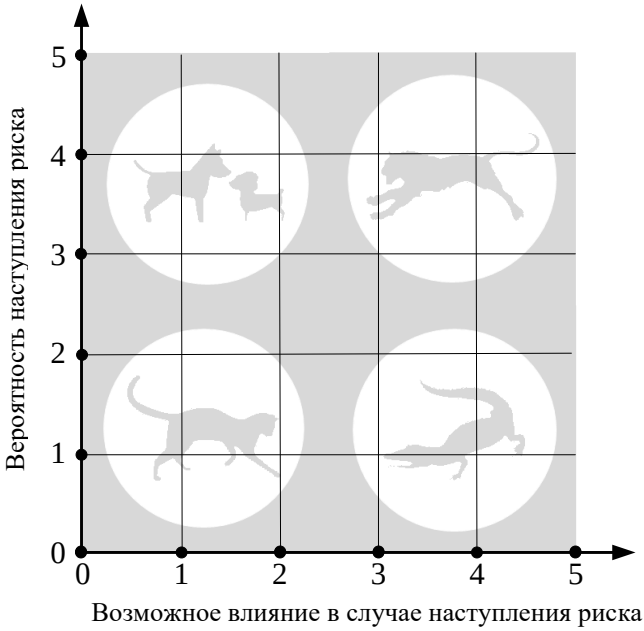


Рисунок 2.12 – Матрица негативных рисков

Отдельно следует выделить группу маловероятных, но очень опасных рисков, таких как промышленные катастрофы, потрясения, природные катаклизмы, пандемии и эпидемии. Талеб Н.Н. называет подобные риски **«*черные лебеди*»** [67]**.**

Позитивные риски автор настоящего пособия рекомендует распределять на четыре группы [68]:

1) ***созидательные риски, или «слоны»***, — позитивные риски, которые имеют высокую вероятность материализации и способны оказывать значительное влияние. Зачастую «слоны» наступают независимо от превентивных мер воздействия на риски, поэтому для них не рекомендуется проводить какие-либо дополнительные меры воздействия;

2) ***непредсказуемые риски, или «львы»,*** — позитивные риски, которые имеют низкую вероятность материализации, но обладают способностью оказывать значительное влияние. Исходя

из вышесказанного можно заключить, что «львы» имеют большой практический интерес. Например, если заблаговременного будут проведены стимулирующие меры, то в проект могут быть привлечены ведущие программисты, что позитивно повлияет на процесс достижения целей;

3) ***часто встречаемые риски, или «обезьяны»,*** — позитивные риски, имеющие высокую вероятность материализации, но не способные оказывать значительное влияние. Отделение данных позитивных рисков от остальных имеет большую практическую ценность, так как «дразня» заинтересованные стороны, «обезьяна» вынуждает расходовать ограниченные ресурсы, не оказывая при этом какое-либо значительное влияние на процесс достижения целей;

4) ***незначительные риски, или «кролики»,*** — позитивные риски, которые имеют низкую вероятность материализации и не обладают способностью оказывать значительное позитивное влияние. Рисками данной группы можно пренебречь.

Матрица вероятности и влияния позитивных рисков представлена на рисунке 2.13 [68].

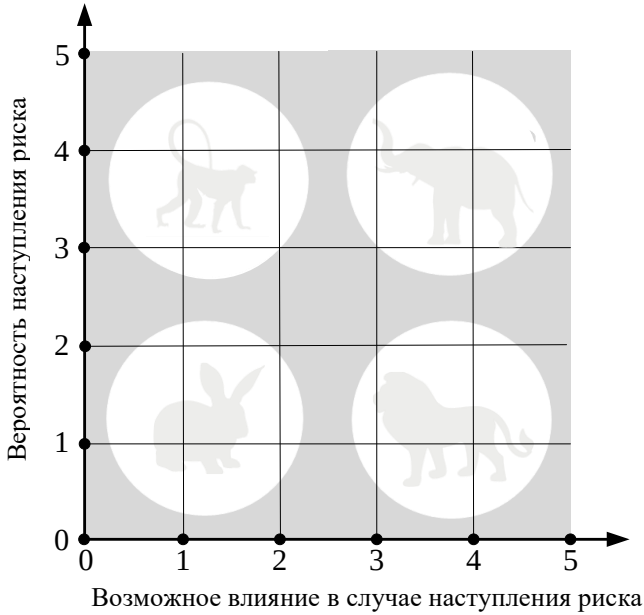


Рисунок 2.13 – Матрица позитивных рисков

Рассмотрим примеры позитивных рисков в проектах.

Риск того, что численность участников проекта будет менее 6 человек. В аналитических докладах The CHAOS Manifesto приводятся статистические данные, которые показывают, что проекты, в состав которых входило менее 6 участников, были гораздо успешнее, чем проекты, в которых принимало участие более 6 человек (таблица 2.10) [1].

Таблица 2.10 – Проекты, в состав которых входило менее 6 участников (50 000 проектов)

Статус проекта	Распределение, %
Успешные проекты	67
Незавершенные проекты	5
Проекты, в которых проблемы повлекли изменение целей	28

Риск привлечения в проект высококвалифицированного работника. Результаты исследований показывают, что материализация данного позитивного риска повышает вероятность успешного достижения запланированных целей проекта до 70 % [69].

Риск привлечения в проект руководителя проекта, имеющего профессиональное образование в области управления проектами (опыт управления проектами более 2-х лет). В аналитических отчетах The CHAOS Manifesto утверждается, что на успешное завершение проекта значительно влияют профессиональные и личные качества руководителя проекта. В частности, если руководитель проекта имеет профессиональное образование в области управления проектами, то проекты выполняется согласно общепринятым нормам, что нивелирует значительную часть негативных рисков.

Кроме того, результаты исследования Гаги В.А., Козловой С.А., Тютюшева А.П. и Ярославцевой Е.Н. показали, что на эффективность и результативность рабочих групп значительно влияет эмоциональный интеллект руководителя [70]. Например, негативные эмоции руководителя проекта быстро передаются участникам проекта, что отражается на их координации, мотивации и энтузиазме.

Риск декомпозиции большого проекта на малые проекты (длительностью не более 4-х месяцев). Согласно статистическим данным The CHAOS Manifesto доля краткосрочных проектов, трудоемкость которых составляет не более 700 чел./ч равна 76 %, в то время как доля среднесрочных (700–2500 чел./ч) — 14 %, долгосрочных ИТ-проектов (более 2 500 чел.ч) — 10 % [1].

Помимо вероятности материализации рисков и возможного влияния в случае их наступления, могут оцениваться и другие характеристики риска:

- ***время актуализации*** — время, в течение которого следует ожидать наступление риска;
- ***близость*** — насколько быстро риск станет оказывать влияние на одну или несколько стратегических, тактических, операционных или проектных целей;
- ***выявляемость*** — насколько просто можно выявить и опознать приближение риска. Для представления близости, выявляемости и величины влияния может быть использована пузырьковая диаграмма (bubble chart);
- ***срочность*** — период, в течение которого должны быть проведены меры воздействия на риск;
- ***латентность*** — период, в течение которого будут обнаружены последствия от наступления риска.
- ***управляемость*** — уровень (степень) сложности управления риском для его владельца;
- ***смешанность*** — степень влияния проблемных и благоприятных последствий от наступлений рисков, с которыми связан анализируемый риск. Графическое представление смешанности может быть представлено с помощью диаграммы «торнадо».

Результаты оценивания рекомендуется заносить в раздел «Оценивание» реестра рисков, при этом фиксируется следующая информация:

- тип риска;
- название риска;
- вероятность наступления риска;
- влияние в случае наступление риска;
- группа риска. Например, указывается «красная», «желтая» или «зеленая» группа, если применяется группировка рисков DoD.

Пример раздела «Оценивание» реестра рисков представлен в таблице 2.11.

Таблица 2.11 – Пример раздела «Оценивание» реестра рисков

Тип риска / Название риска	Вероятность наступления риска, (0÷1)	Влияние в случае наступления риска, (0÷10)	Группа риска
1. Негативный / Риск изменения условий контрактов сотрудников	0,6	3	Зеленая
2. Негативный / Риск того, что выполненная работа (оказанная услуга) не принесет ожидаемого коммерческого эффекта	0,3	9	Желтая
3. Негативный / Риск того, что партнеры откажутся от сотрудничества	0,3	3	Зеленая
4. Негативный / Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям конечного пользователя	0,5	6	Желтая

2.5. Воздействие на риски

После того как среди выявленных рисков установлены наиболее важные и наиболее опасные риски, требующие постоянного управленческого внимания, и риски, которыми можно пренебречь, необходимо разработать точечные меры воздействия на данные риски. Процесс разработки мер **воздействия на риски** включает имплементацию мер превентивного воздействия и мер принятия рисков.

Меры превентивного воздействия на риски (план А) — это перечень профилактических мер упреждающего управления. Например, если будет идентифицирован риск, связанный с отсутствием знаний, навыков и опыта у участников проекта, то превентивной мерой будет организация курсов повышения квалификации и привлечение в проект сторонних экспертов.

Меры принятия рисков (план Б) — это резервы и инструкции по локализации последствий в случае наступления риска. План Б необходим, если произойдет наступление вторичных рисков и рисков-невидимок. ***Вторичные риски*** — это вероятные события, которые могут наступить несмотря на проведение профилактических мер плана А. ***Риски-невидимки*** — это скрытые риски, которые не были обнаружены во время идентификации. Опасность данных рисков заключается в их неожиданном наступлении.

В качестве примера мер плана Б можно рассмотреть возможный уход ключевого сотрудника. Наступление этого риска, как правило, оказывает значительное негативное влияние на процесс достижения целей, поэтому для уменьшения возможного ущерба рекомендуется заблаговременно формировать денежные, временные, кадровые и управленческие резервы.

Яркие примеры применения мер плана Б можно часто встретить В в производстве фильмов. Например, в картине 1994 года «Побег из Шоушенка» главный герой Энди Дюфрейн смог уйти в побег только потому, что он заблаговременно подготовил «тайный ход» и спрятал на счетах $370 000.

В проектах резервы мер плана Б входят в общий бюджет проекта. Более того, специалисты PMBOK® Guide утверждают, что успех проекта во многом зависит от правильно запланированных резервов (трудовых, материальных резервов, резервов на покрытие инфляции, средств на возможные потери и др.) [13, 14, 15]. На рисунке 2.14 представлена структура бюджета проекта с учетом управленческих резервов и резервов на возможные потери.

Рисунок 2.14 – Структура бюджета проекта с учетом управленческих резервов и резервов на возможные потери согласно PMBOK® Guide

Отдельно стоит отметить управленческий резерв, который, как правило, не входит в базовый план по стоимости. ***Управленческий резерв*** — это сумма в бюджете проекта или временной промежуток в расписании проекта, которые зарезервированы для управленческого контроля, выполнения какой-либо непредвиденной работы либо принятия ранее неидентифицированных рисков (рисков-невидимок).

Для увеличения качества разрабатываемых мер плана А и мер плана Б рекомендуется вести их имплементацию, придерживаясь определенной стратегии воздействия на риски. Под **стратегией воздействия на риски** понимается совокупность разрабатываемых мер, направленных на изменение вероятности наступления риска и возможного влияния в случае их материализации, а также иных мер, которые смогут обеспечить наиболее результативную и эффективную работу с данными рисками. Виды стратегий воздействия на риски представлены в таблице 2.12.

Таблица 2.12 – Характеристика стратегий воздействия на риски

Тип риска	Стратегия Воздействия	Описание стратегии воздействия
Негативный риск	Нивелирование	Выявляются источники риска с их последующей ликвидацией
	Ослабление	Изменяются вероятность материализации риска и/или возможное влияние в случае его наступления
	Передача (страхование и хеджирование)	Риск передается третьему лицу
	Эскалация	Риск передается компетентному лицу
	Наблюдение	Активных действий в отношении риска не ведется, но осуществляется процесс мониторинга
	Принятие	Активных действий в отношении риска не ведется
Позитивный риск	Масштабирование	Увеличивается масштаб возможного благоприятного эффекта
	Усиление	Изменяются вероятность материализации риска и/или возможное влияние в случае его наступления

Окончание таблицы 2.12

Тип риска	Стратегия воздействия	Описание стратегии воздействия
Позитивный риск	Передача	Риск передается третьему лицу
	Эскалация	Риск передается компетентному лицу
	Наблюдение	Активных действий в отношении риска не ведется, но осуществляется процесс мониторинга
	Принятие	Активных действий в отношении риска не ведется

Отметим, что по мнению Селиховкина И., самой результативной стратегией воздействия на негативные риски является ***стратегия нивелирования***, суть которой заключается в ликвидации источников рисков [71]. Если не будет источника риска, то не будет и самого риска. Для позитивных рисков Селиховкин рекомендует использовать ***стратегии масштабирования*** **и** ***усиления*****.**

В банковской и страховой сферах встречаются специальные виды стратегий, такие как диверсификация и хеджирование. Под ***стратегией диверсификации рисков*** понимается перераспределение капитала между несколькими, не связанными между собой инвестиционными инструментами: акциями, облигациями, валютой, недвижимостью, криптовалютой и др. Под ***стратегией хеджирования рисков*** понимается перенос рисковых событий на субъектов, готовых их принять. Перенос рисков осуществляется посредством заключения фьючерсных и форвардных контрактов, свопов и опционов.

Когда для каждого идентифицированного риска определена стратегия воздействия, далее с помощью специальных методов непосредственно разрабатываются меры плана А и плана Б. Методы, применяемые для разработки мер воздействия на риски, представлены в таблице 2.13.

Ретроспективный анализ документов (Retrospective). Договоры, реестры рисков, планы управления рисками ранее завершенных проектов и заключенных сделок позволяют оперативно установить наиболее результативные и эффективные меры воздействия на риски.

Таблица 2.13 – Методы, применяемые для разработки мер воздействия на риски

Название	Название (перевод на русский)	Разработчики
Retrospective	Ретроспективный анализ документов	Никонов В.А. [54], Поляков А.А. и др. [72, 73]
Delhi	Метод «Дельфи»	Хелмер О. и др. [55]
Brainstorming	Метод «Мозговой штурм»	Осборн А. [55]
Bow-tie	Метод «Галстук-бабочка» (2-й этап)	Лангминд Б. [61]
Method of Walt Disney	Метод Уолта Диснея	Дисней У. [55]

Метод «Дельфи» (Delhi). Как было отмечено ранее, риски условно могут быть универсальными и специальными. Для универсальных рисков применимы стандартные меры воздействия, которые могут быть установлены, например, во время проведения ретроспективного анализа документов. Так как эти меры показали свою надежность в ранее заключенных сделках и завершенных проектах, то нет необходимости создавать для них какой-либо иной механизм воздействия. Для специальных рисков ввиду их индивидуальности, напротив, требуется использование творческого подхода в процессе создания мер плана А и плана Б. Одним из методов, который использует творческое мышление экспертов, является метод «Дельфи» (рисунок 2.15).

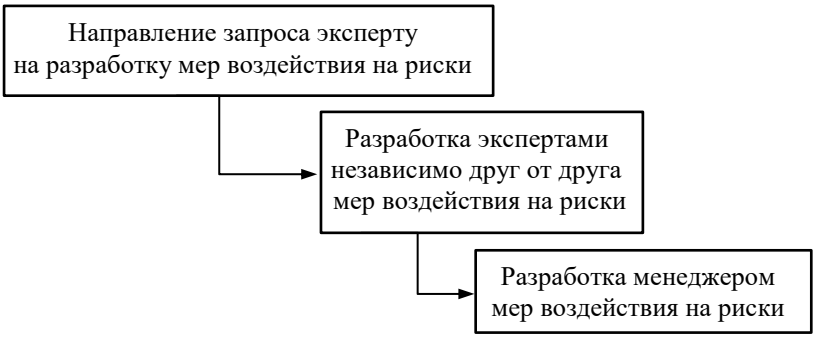


Рисунок 2.15 – Разработка мер воздействия на риски с помощью метода «Дельфи»

Метод «Мозговой штурм» (Brainstorming). Результативно данный метод проявляет себя при работе в малых группах до 6 человек (рисунок 2.16).

Рисунок 2.16 – Разработка мер воздействия на риски с помощью метода «Мозговой штурм»

Творческая свобода и отсутствие критики дают возможность экспертам создать большое количество разнообразных мер воздействия не только для специальных рисков, но и пересмотреть механизм воздействия для универсальных рисков.

Метод «Галстук-бабочка» (Bow-tie). Как отмечено ранее, на втором этапе метода «Галстук-бабочка» разрабатываются «барьеры», направленные на локализацию источников рисков, и «меры восстановления (усиления)», которые призваны оперативно локализовать причиненный ущерб (усилить благоприятный эффект).

Метод Уолта Диснея (Method of Walt Disney). Суть метода заключается в условном выделении ролей для каждого участника разработки мер воздействия на риски:

1) «фантазер», отвечающий за поиск творческих идей, включая фантастические и волшебные;

2) «критик», занимающийся поиском слабых мест в предложенных мерах;

3) «реалист», оценивающий достижимость и целесообразность разработанных мер воздействия на риски.

Помимо разработки мер плана А и плана Б в процессе воздействия на риски, рекомендуется выявлять триггерные условия.

Триггерные условия (триггеры) в управлении рисками — это условия, события или ситуации, которые указывают на скорую

материализацию рисков. Например, если в процессе общения заказчик произнес такую фразу, как «Мне это не нравится» или «Чего-то тут не хватает», то эта фраза будет являться триггерным условием, которое предупреждает о том, что скоро наступит риск изменения требований.

Результаты разработки мер превентивного воздействия на риски и мер принятия рисков необходимо фиксировать в ***плане управления рисками***, в котором указывают:

- тип риска;
- название риска;
- стратегию воздействия.
- меры превентивного воздействия.
- владельца риска (конкретное лицо/группа лиц, которое будут управлять риском;
- триггерные условия;
- меры принятия рисков.

Пример плана управления рисками представлен в таблице 2.14.

2.6. Мониторинг и контроль рисков

Мониторинг рисков — это процесс, направленный на выявление ранее неидентифицированных рисков, т. е. рисков, которые не были ранее зафиксированы в реестре рисков. **Контроль рисков** — это процесс наблюдения за уже идентифицированными рисками, т. е. рисками, которые были ранее зафиксированы в реестре рисков и плане управления рисками. Оптимальным механизмом, обеспечивающим контроль рисков, являются триггерные условия. Именно благодаря триггерам владельцы рисков могут понять, что меры плана А не принесли ожидаемого результата и поэтому необходимо готовиться к наступлению рисков. Процесс контроля триггерных условий индивидуален, потому что риски закрепляются за конкретным ответственным лицом. Во многом это связано с тем, что некоторые риски и их триггеры могут быть замечены только определенными работниками. Например, триггерное условие «Во время тестирования была обнаружена ошибка в программном коде» риска, связанного с изменением длительности проекта, может выявить только работник, ответственный за тестирование программного кода.

Таблица 2.14 – Пример плана управления рисками

Тип/Название риска	Стратегия воздействия	Меры превентивного воздействия	Владелец риска	Триггерные условия	Меры принятия рисков
1. Негативный/Риск изменения условий контрактов сотрудников	Ослабление	Провести переговоры с представителями профсоюза для того, чтобы выявить их цели и интересы	ФИО	Требования от профсоюза пересмотреть контракты сотрудников кафетерия	Привлечь юриста
2. Риск того, что выполненная работа (оказанная услуга) не принесет ожидаемый коммерческий эффект	Ослабление	Провести обучение сотрудников	ФИО	Обратная связь от работников	Подготовить руководство пользователя программы для ЭВМ
3. Риск того, что партнеры откажутся от сотрудничества	Ослабление	Заключение контрактов с партнерами	ФИО	Непредоставление скидки	Привлечь юриста
Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям конечного пользователя	Ослабление	Подготовить спецификацию требований к программе для ЭВМ	ФИО	Обратная связь от работников	Доработать программу для ЭВМ

Рынок предлагает обширный выбор программного обеспечения по оценке рисков и автоматизации процессов мониторинга и контроля рисков:

- ***@RISK for Project Management*** — программный продукт (ПП), выполняющий количественную оценку вероятности завершения проектов и оценку возможного перерасхода бюджетов;
- ***RiskTrack, RiskRadar, Risk Register*** — ПП, которые представляют собой электронную версию реестра рисков;
- ***OpenPlanProfessional*** — ПП, который оценивает вероятность завершения проекта с помощью метода «Монте-Карло»;
- ***RiskGap*** — отечественный ПП, консолидирующий информацию о рисках. Главным его преимуществом является возможность привлечения к управлению рисками участников проектной команды. Оценивание вероятности наступления рисков и возможного влияния в случаях наступления осуществляется посредством вербально-числовой шкалы Харрингтона.

В качестве инструмента по определению текущего статуса риска рекомендуется использовать модель «Жизненный цикл риска», которая наглядно показывает, как меняется статус риска от неидентифицированного до управляемого (рисунок 2.17). Сопровождение процессов мониторинга и контроля рисков посредством модели ЖЦ риска заключается в получении ответов на следующие вопросы:

- выявлены ли новые ранее не идентифицированные риски;
- замечены ли триггерные условия для ранее идентифицированных рисков;
- все ли запланированные цели достигнуты. Если нет, то в чем причины;
- верно ли были выбраны стратегии воздействия на риски;
- оказались ли меры превентивного воздействия на риски достаточно эффективными и результативными;
- оказались ли меры принятия рисков достаточно эффективными и результативными;
- есть ли замечания по управлению рисками от его владельцев;
- имеются ли замечания у заинтересованных сторон в части управления рисками.

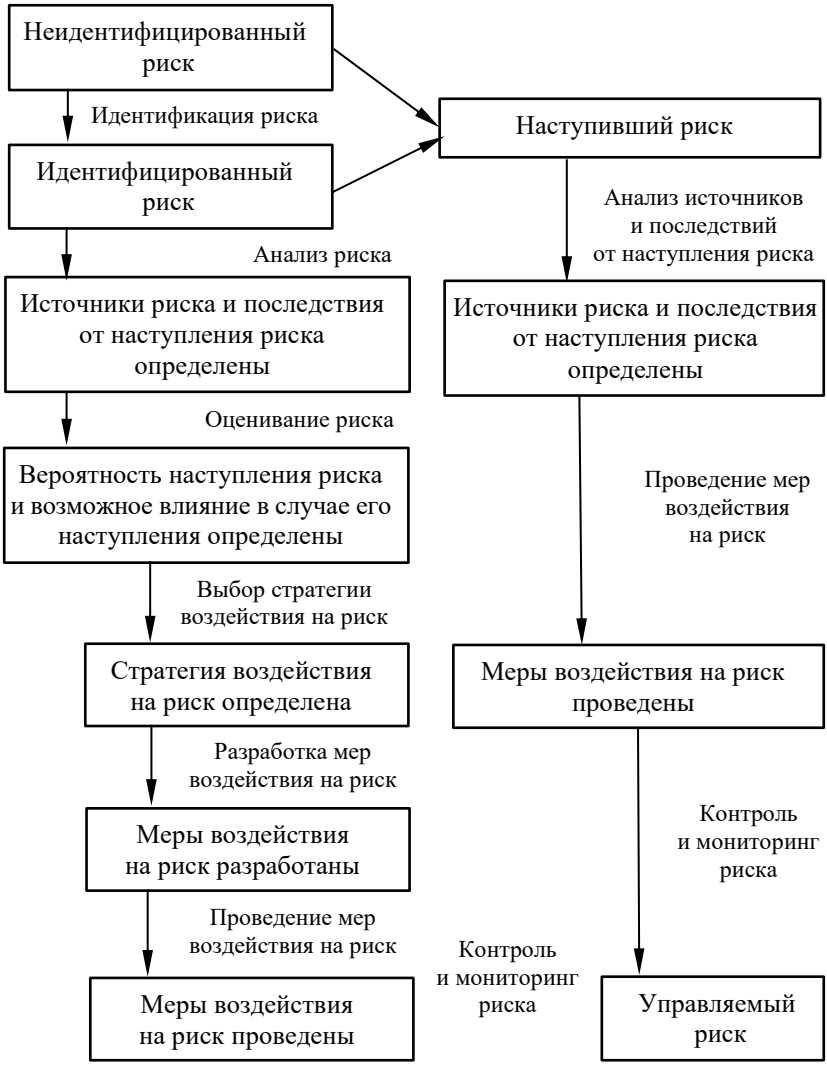


Рисунок 2.17 – Модель «Жизненный цикл риска»

Несколько лет назад Роман решил разработать коммерчески перспективную программу для ЭВМ «Мед-архив», для чего нанял опытных программистов Бориса и Максима, заключил с ними трудовой договор и выдал задание на разработку. И все получилось. Программа действительно оказалась востребованной на рынке. Когда работы над «Медархив» были завершены, Борис и Максим написали заявление на увольнение и ушли из организации Романа.

Спустя месяц на рынке появилась программа «Medsenger», по своей сути являющаяся аналогом программы «Медархив». Обратившись в Единый государственный реестр юридических лиц, Роман с удивлением обнаружил, что его бывшие работники являются собственниками организации, которой принадлежат исключительные права на программу «Medsenger». Роман решил обратиться в суд.

В ходе судебного разбирательства было установлено, что программа «Medsenger» зарегистрирована в Роспатенте, на нее выдано Свидетельство о государственной регистрации, Борис и Максим являются авторами данной программы и ее правообладателями. Зачитывая решение, судья отметил, что «само по себе наличие трудовых отношений с Борисом и Максимом не является основанием признания разработанной программы «Медархив» служебным произведением. В материалах дела отсутствуют документы, подтверждающие наличие служебного задания — доказательства создания программы в определенный период времени определенными субъектами, актов приемки-передачи служебного произведения и каких бы то ни было иных документов, свидетельствующих о создании данной программы в рамках исполнения трудовых обязанностей. В то же время именно с наличием подобных документов суды связывают доказанность факта ***создания произведения как служебного****».*

Случай из практики

3. ВНЕДРЕНИЕ РИСК-МЕНЕДЖМЕНТА

3.1. Структура управления рисками

Отечественное семейство национальных стандартов управления рисками, как было отмечено в первом разделе пособия, не является оригинальным. Например, стандарт ГОСТ Р ИСО 31000:2010 «Менеджмент риска. Принципы и руководство» — это локализованная версия международного стандарта ISO 31000:2009 «Risk

management – Principles and guidelines». ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска» является локализованной версией стандарта IEC 31010:2009 «Risk management − Risk assessment techniques» и др. Подобная ориентация на Международную организацию по стандартизации International Organization for Standardization (ISO) создает ряд проблем, которые препятствуют активному развитию управления рисками в Российской Федерации.

1. Утрата актуальности знаний, закрепленных в ГОСТ Р ИСО 31000. В 2017 г. PMI опубликовал обновленный свод лучших управленческих практик в области управления проектами, в котором представлен усовершенствованный инструментарий управления рисками. В 2017 г. COSO ERM и PRINCE2® презентовали новые своды знаний по управлению проектами и рисками в них. В 2018 г. ISO опубликовал новый стандарт менеджмента риска ISO 31000:2018 «Risk management – Guidelines», пересматривающий основные положения управления рисками. В 2019 г. вышел обновленный стандарт IEC 31010:2019 «Risk management – Risk asses-sment techniques», закрепляющий новый механизм оценки рисков.

2. Отсутствие инструментария управления позитивными рисками. В первом разделе пособия были представлены позиции ученых относительно толкования понятия «риск», где большинство склоняется к тому, что риск несет в себе негативную коннотацию. Однако последние результаты исследований показывают, что природа риска дуальна, так как его наступление может привести как к проблемным последствиям, так и к благоприятным.

3. Отсутствие системного подхода по выявлению лучших отечественных практик в области управления рисками. Логично предположить, что для решения вышеобозначенных проблем необходимо определение общей структуры управления рисками, которая бы удовлетворяла всем требованиям национальных и международных стандартов. На основании проведенного анализа было установлено, что общая структура управления рисками включает три взаимосвязанных компонента (рисунок 3.1) [74]:

1) механизм управления рисками;
2) процессы управления рисками;
3) корпоративную культуру управления рисками.

Рисунок 3.1 – Общая структура управления рисками

Механизм управления рисками является системообразующим компонентом управления рисками и создается исключительно руководством организации, поскольку только управляющие органы обладают необходимыми полномочиями для создания инфраструктуры управления рисками, к которым относятся:

- разработка и декларирование применения должностных инструкций, корпоративных стандартов, чек-листов и других внутренних документов, закрепляющих управление рисками;
- приобретение и эксплуатация оборудования и специализированного программного обеспечения;
- утверждение бюджета на систематическое осуществление профилактических мер превентивного воздействия на риски и формирование денежных, временных, кадровых и управленческих резервов;
- назначение ответственных лиц за управление рисками.

Процессы управления рисками. Эффективное и результативное управление рисками возможно только при итеративном применении, поэтому процессы управления рисками должны быть представлены в виде цикла (рисунок 3.2).

Рисунок 3.2 – Процессы управления рисками

Необходимо отметить, что в центре цикла находится процесс «Оценка эффективности и результативности управления рисками», целью которого является определение лучших практик управления рисками для закрепления во внутренних стандартах организации и дальнейшего тиражирования.

Корпоративная культура управления рисками

Корпоративная культура — это модель поведения работников в штатных и нештатных ситуациях. ***Риск-ориентированная корпоративная культура*** — это модель поведения работников, направленная на заблаговременное воздействие на риски и достойное принятие рисков в случае их наступления.

Корпоративная культура управления рисками формируется и развивается только при системной оценке результатов, поэтому

оценка эффективности и результативности управления рисками является важнейшим процессом, который дает возможность выявлять лучшие практики и закреплять их во внутренних стандартах организации.

3.2. Документальное сопровождение риск-менеджмента

Механизм управления рисками должен опираться на твердые и надежные источники, такие как профессиональные стандарты, должностные инструкции и корпоративные стандарты.

Профессиональный стандарт — это характеристика квалификации, которая необходима для осуществления определенного вида профессиональной деятельности. Профессиональный стандарт закрепляет необходимый уровень квалификации работника, которому он должен соответствовать, для того чтобы эффективно и результативно выполнять свои профессиональные обязанности.

В 2018 г. Министерство труда и социальной защиты РФ утвердило Профессиональный стандарт «Специалист по управлению рисками» (Код 08.018). В данном профстандарте подробно описываются цель, задачи, профессиональные компетенции работника, ответственного за управление рисками, а также его трудовые функции [75]. В частности, если работник имеет среднее либо начальное профессиональное образование, то он обязан:

- определять текущее состояние внутренней и внешней среды организации (проекта);
- проводить идентификацию рисков;
- собирать и обрабатывать информацию, необходимую для последующего анализа и оценивания рисков.

Работник, получивший высшее образование по программе бакалавриата, имеет право осуществлять следующие функции:

- разработку мер по воздействию на риски;
- документирование процессов управления рисками;
- корректировку реестра рисков;
- создание методических и нормативных баз управления рисками в рамках отдельных бизнес-процессов и функциональных направлений организации.

Профессиональный стандарт 08.018 является основой для создания должностной инструкции риск-менеджера. **Должностная инструкция** — это внутренний локальный документ организации, регламентирующий производственные полномочия и обязанности работника. Согласно принятым нормам оформления должностная инструкция должна включать следующие разделы [76]:

- ***общие положения***. В данном разделе указывается наименование должности, согласно штатному расписанию, структурное подразделение и подчиненность;
- ***основная цель и трудовые функции профессиональной деятельности***. Данный раздел формализует ясную, лаконичную и конкретную цель, а также описание трудовых функций, которые необходимо выполнять для ее достижения. Основной целью риск-менеджера является предоставление разумной гарантии успешного достижения стратегических, тактических, операционных, проектных и других целей организации;
- ***должностные обязанности.*** В разделе указываются конкретные действия, которые должен выполнять работник для исполнения своих трудовых функций.

Корпоративный стандарт — локальный документ организации, в котором фиксируются модели поведения работника в штатных и нештатных ситуациях. Корпоративные стандарты, как правило, уникальны для каждой организации, так как они вырабатываются на основании собственных лучших практик.

3.3. Оценка результативности и эффективности управления рисками

Процесс оценки эффективности и результативности управления рисками включает в себя оценку эффективности и результативности идентификации рисков и экономического эффекта от использования управления рисками.

Согласно ГОСТ Р ИСО/МЭК 33001-2017 под **результативностью** *(effectiveness)* понимается степень реализации запланированных мероприятий и достижения запланированных результатов [77]. В соответствии с ГОСТ ISO 9000-2011 под **эффективностью** *(efficiency)* понимается связь между достигнутым результатом и использованными ресурсами [78].

Оценка эффективности и результативности идентификации рисков. Качество процесса идентификации рисков оценивается с помощью формулы

$$k = \frac{n_2}{n_1 + n_2}, \tag{3.1}$$

где k — показатель качества идентификации рисков;

n_1 — число наступивших неидентифицированных рисков;

n_2 — число наступивших идентифицированных рисков.

Показатель качества идентификации рисков k дает возможность оценить, насколько качественно была проведена идентификации рисков. Если показатель k равен 1, то это означает, что в процессе достижения целей не материализовался ни один риск. Следовательно, выявление рисков было осуществлено качественно, несмотря на то что это один из наиболее кропотливых процессов управления рисками.

Время, затраченное на выявление рисков, представляет собой инвестицию в успех, так как неучтенные риски, которые могли быть идентифицированы при более тщательной работе, при наступлении препятствуют достижению запланированных целей.

Оценка экономического эффекта от использования управления рисками. Оценка экономического эффекта от использования управления рисками рассчитывается по формуле

$$E_{\text{р}} = R_{\text{р}} - C_{\text{р}}, \tag{3.2}$$

где $E_{\text{р}}$ — экономический эффект от использования управления рисками;

$R_{\text{р}}$ — результаты от управления рисками;

$C_{\text{р}}$ — затраты на управление рисками.

Результаты, полученные от управления рисками, выражаются разностью между вероятными потерями от наступления идентифицированных рисков без проведения мер воздействия и после проведения мер воздействия:

$$R_{\text{р}} = \sum_{i=1}^{N} M_{\text{o}_i} - \sum_{i=1}^{N} M_i, \tag{3.3}$$

где M_{o_i} — вероятные потери от наступления *i*-го идентифицированного риска без проведения мер воздействия на риски;

M_i — вероятные потери от наступления *i*-го идентифицированного риска после проведения мер воздействия на риски;

N — количество идентифицированных рисков.

Понесенные затраты на управление рисками $C_р$ определяются по формуле

$$C_р = \left(\sum_{i=1}^{N} L_i + \sum_{i=1}^{N} H_i \right) + \left(\sum_{j=1}^{K} L_j + \sum_{j=1}^{K} H_j \right), \qquad (3.4)$$

где L_i — фактические убытки от наступления *i*-го идентифицированного риска;

H_i — фактические расходы на обработку *i*-го идентифицированного риска;

L_j — фактические убытки от наступления *j*-го неидентифицированного риска;

H_j — фактические расходы на обработку *j*-го неидентифицированного риска;

Позитивный экономический эффект характеризуется превышением результатов управления рисками над затратами: $R_р > C_р$. Если затраты на управление рисками $C_р$ превышают результаты от использования риск-менеджмента $R_р$, то можно говорить о том, что управление рисками является экономически неоправданным.

3.4. Ментальные ловушки

Под **ментальной ловушкой** понимают определенную форму мышления, которая может приносить вред субъекту, при этом данный субъект этого может даже не осознавать. **В процессе идентификации рисков** начинающий риск-менеджер может угодить в различные ментальные ловушки, а именно:

- ***формируемая риск-менеджером картина мира***. Опыт, образование и привычки формируют нашу картину мира, в кото-

рой «белые пятна» могут скрывать множество рисков. Объясняется это тем, что люди склонны пропускать информацию через призму собственного опыта, что часто мешает ясно оценивать реальную обстановку и текущее положение дел. Лучшим способом борьбы с подобной ловушкой является идентификация рисков в группе, например, с использованием метода мозгового штурма или метода «Дельфи»;

- ***уверенность в надежности доверенного лица***. Делегирование обязанностей по идентификации рисков доверенному лицу не гарантирует выявления наиболее опасных и важных рисков. Доверенное лицо может запросто угодить в ментальную ловушку «картина мира» и не заметить риски, которые будут находиться в его «серой зоне». Для решения данной проблемы рекомендуется привлекать сторонних экспертов и консультантов;
- ***иллюзия понимания (распознавания) мыслей и потребностей других людей***. Исследования показывают, что один из часто встречаемых рисков в проектной деятельности — это риск невостребованности потребителем разрабатываемого продукта;
- ***иллюзия контроля (контролируемости) ситуации***. Человек часто думает, что обладает всей необходимой информацией, однако это далеко не так. Мир постоянно меняется. И если человек считает, что в настоящий момент все хорошо, то это не значит, что сейчас действительно все хорошо, это говорит только о том, что человек не знает реальной ситуации.

Внешняя и внутренняя среда постоянно меняются: принимаются новые законы, вносятся поправки в налоговый режим, корректируются нормы гражданских правоотношений, появляются новые технологии и выходят на рынок продукты-субституты, меняется лояльность и интерес клиентов и т. д.;

- ***глубокая убежденность в наличии более важной работы***. Уверенность в том, что есть более важная работа, снижает значимость процесса идентификации. Подобное отношение к одному из наиболее трудоемких процессов управления рисками может привести к проблемам в будущем. Неучтенные риски, которые могли бы быть идентифицированы при их наступлении, помешают достижению запланированных целей (см. раздел 2);
- ***толерантность к плохой работе***. Исследования показывают, что люди очень быстро привыкают работать плохо;

- ***привычка убеждать***. Человек, как правило, убеждает себя и других в том, что ранее принятое решение остается единственно верным, несмотря на то что новая информация противоречит этому утверждению;
- ***привычка принимать информацию «на веру».*** Отсутствие верификации информации может привести к негативным последствиям, поэтому лучшим способом борьбы с данной ментальной ловушкой является сбор информации из разных источников;
- ***убежденность в невозможности наступления негативного события.*** Некоторые риски воспринимаются человеком как нечто отдаленное и нереальное. Показательным примером является распространение пандемии в 2020 г.: нельзя игнорировать риски, даже если они и находятся где-то «за горизонтом»;
- ***распространенность ретроспективных оценок***. Опытные риск-менеджеры подвержены иллюзии, что ранее идентифицированные риски в проверке уже не нуждаются.

В процессе оценивания рисков также можно угодить в специальные ментальные ловушки, каковыми являются:

- ***чрезмерный и необоснованный оптимизм***. В данном случае уместно вспомнить о статье Смита Д. и др. «Оптимизм руководителя проекта, управление стрессом и успех ИТ-проекта», в которой он приводит следующий вывод: люди склонны убеждать себя в том, что «чему быть, того не миновать», надеясь при этом, что «все самое плохое их непременно обойдет стороной» [79]. Из этого следует, что качественное оценивание вероятностей материализации рисков и их возможного влияния подвержено инстинктивному отрицанию неприемлемых для экспертов последствий;
- ***иллюзия в отношении возможности решения множества проблем посредством выявления позитивных рисков.*** Это не всегда так. Негативным рискам необходимо уделять должное внимание. В качестве примера можно рассмотреть кейс внедрения риск-ориентированного управления в одном из крупнейших томских вузов. В процессе идентификации были выявлены 42 негативных и 2 позитивных риска. Подробно с особенностями внедрения риск-менеджмента в высшие учебные заведения можно ознакомиться в работе «Адаптация инструментария риск-менеджмента для высших учебных заведений Российской Федерации» [80].

Несмотря на значительное благоприятное влияние от наступления позитивных рисков, вероятный суммарный ущерб показал, что нельзя пренебрегать управлением и негативными рисками. Даже если материализация позитивных рисков ослабляет возможный негативный эффект, шанс получения ущерба все-таки остается;

- ***убежденность в необязательности анализа рисков.*** Отметим, что если анализ рисков не будет осуществлен, то риск-менеджер может воспринять определенные риски как незначительные и проигнорировать их.

Во время разработки мер воздействия на риски риск-менеджер может угодить в следующие ментальные ловушки:

- ***иллюзия идеального будущего.*** Человек склонен фокусироваться на будущих событиях и идеализировать разработанные прогнозы;
- ***убежденность в существовании механизмов регулирования очевидными рисками.*** Люди часто думают, что если риск очевиден для всех, то им вероятно уже кто-то управляет;
- ***отрешенность от мирского и ожидание чуда***. Иногда человек склонен верить в высшие силы, частично снимая с себя ответственность за конечный результат — «Авось пронесет!». Риск-менеджер никогда не полагается на «авось». Он знает, что «чудо требует кропотливой и тщательной подготовки».

3.5. Влияние деловой культуры на управление рисками

В трудах известного во всем мире специалиста в области межкультурного взаимодействия Ричарда Льюиса отмечается, что деловые культуры различных стран не являются однородными [81]. Деловые культуры обладают своими особенностями, которые проявляются в различном отношении к жизни, времени, деньгам, а также и риску. На основе своих наблюдений Р. Льюис предлагает классифицировать деловые культуры различных стран по следующим группам (рисунок 3.3):

- моноактивные деловые культуры;
- реактивные деловые культуры;
- полиактивные деловые культуры.

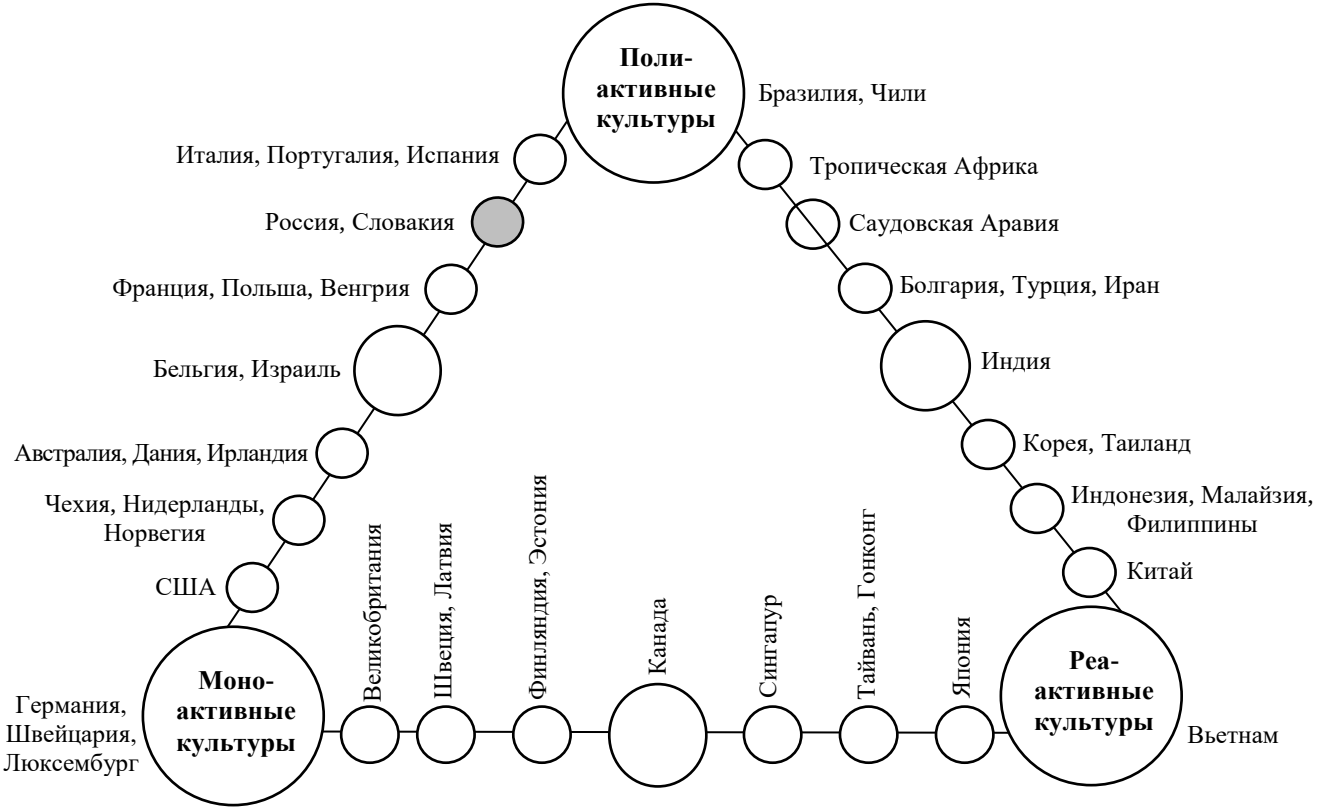


Рисунок 3.3 – Классификация деловых культур по Р. Льюису

Моноактивные (монохромные) деловые культуры очень сильно ориентированы «на дело», т. е. на конечный результат — достижение поставленной цели. Основой организации человеческой деятельности в этих культурах является время, которое рассматривается как стоимостной ресурс. Для представителей монохромной деловой культуры характерно тщательное поэтапное планирование своей деятельности, составление расписаний, точность и пунктуальность, четкое разделение профессиональной и личной сферы жизни, последовательность и сосредоточенность на одном деле в каждый данный момент времени. Для них управление рисками — один из важнейших навыков, ежедневно применяемый в деловой жизни. К типичным представителям моноактивных деловых культур относятся Швейцария, страны Скандинавии, Англия, Германия, США, Канада и др.

Ярким примером использования представителями моноактивных деловых культур основных положений теории управления рисками является доклад Национального совета по разведке США «Глобальные тренды 2040», в котором подробно описаны сценарии развития США в ближайшие 20 лет. Среди основных рисков авторы выделяют риски глобальной кибербезопасности, пандемии, изменения климата на планете Земля, исчерпания и нехватки природных ресурсов и риск мирового экономического кризиса.

Реактивные деловые культуры — это культуры, ориентированные на традиции, процедуры и правила. Представителями реактивных деловых культур являются вьетнамцы, китайцы и японцы. Соблюдение традиций накладывает специфический отпечаток на управление рисками. Например, если цель поставлена, то представители реактивных деловых культур не будут спешить с ее достижением и оценивать риски. Для начала они не торопясь будут обдумывать все свои действия, так как в их культуре не принято решать задачи быстро и последовательно. Они уверены, что спустя время некоторые задачи уже будут кем-то решены. Кроме того, они полагают, что есть задачи значительно важнее, просто сейчас они пока незаметны. Подобный подход, характерный для реактивных деловых культур, негативно влияет на управление рисками, так как если наступит непредвиденный риск, то представители данной культуры не смогут оперативно предпринять необходимые меры.

Полиактивные деловые культуры. Яркими представителями полиактивных деловых культур являются итальянцы, латиноамериканцы и португальцы. Для данных деловых культур характерна ориентация на человека. Представители полиактивных деловых культур обычно подвижны и общительны. Они предпочитают делать много дел сразу. К сожалению, управлять рисками в полиактивных деловых культурах не принято. В частности, когда американцы начинают работать с латиноамериканцами, они испытывают «культурный шок», наблюдая, как пренебрежительно их партнеры относятся к рискам. Моноактивные американцы обычно расценивают это как отсутствие профессионализма.

Что касается представителей российской деловой культуры, то согласно классификации Льюиса Р. россияне находятся между полиактивными и моноактивными деловыми культурами. Данное обстоятельство накладывает определенные ограничения на деятельность отечественных риск-менеджеров. В частности, в процессе формирования и развития риск-ориентированной корпоративной культуры при определении ключевых показателей эффективности (англ. *key performance indicators* — KPI), разработке корпоративных стандартов, должностных инструкций и других внутренних документов риск-менеджеру необходимо понимать, что высокий уровень стандартизации управления рисками может быть саботирован работниками организации. Однако справедливости ради следует отметить, что пограничные состояния деловой культуры дают нам большое преимущество в борьбе с материализованными неидентифицированными рисками, позволяя находить незаурядные решения в условиях ограниченных ресурсов.

3.6. Элиминирование универсальных комплаенс-рисков

Несмотря на устоявшуюся деловую практику и закрепленные нормы права, регулирующие ход реализации проектов, необходимо отметить, что не все участники обладают достаточной управленческой зрелостью, что подтверждается многочисленными примерами материализованных комплаенс-рисков. В частности, для 495 томских организаций, занятых разработкой компьютерного программного обеспечения (ОКВЭД 62.0), примерный совокупный

ущерб от наступления 192 комплаенс-рисков составил более 53 млн руб., т. е. причиненный средний материальный ущерб одного комплаенс-риска превысил 277 тыс. руб.

Merna T. и Al-Thani F. отмечают, что наступление комплаенс-рисков достаточно редкое явление, однако материализация одного подобного риска — уже достаточное условие для причинения существенного материального ущерба [64]. Например, в рамках судебного разбирательства по делу № А81-9472/2019 томская ИТ-организация проиграла спор на общую сумму, равную 1 744 615,65 руб. [82]:

по делу № А67-1623/2017 — 2 850 107,39 руб. [83];

по делу № А40-248300/21-5-1672 — 2 000 000,00 руб. [84];

по делу № А40-32033/19-47-287 — 15 830 400,00 руб. [85] и др.).

В настоящем разделе рассмотрим способы элиминирования универсальных комплаенс-рисков, представленных в приложении 3.

Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям Заказчика. В качестве примера наступления данного комплаенс-риска можно рассмотреть дело № А67-1623/2017, в котором, несмотря на то что истец создал программу для ЭВМ по разработке системы управления проектно-изыскательскими работами на сумму 2 850 107,39 руб., ответчик все же отказался от оплаты, потому что полученный результат не соответствовал его ожиданиям [83].

Согласно PMBOK Guide® сторона Заказчика ожидает, что проектные работы будут выполнены в полном объеме, к определенной дате, в объеме согласованного бюджета и на требуемом уровне качества. Логично предположить, что для того, чтобы получить релевантный результат работ (оказанных услуг), который ожидает Заказчик, в тексте договора должны быть точно сформулированы и корректно формализованы объем, дата окончания, цена, а также и качество выполняемых проектных работ. Однако необходимо отметить, что согласно действующему гражданскому законодательству существенными условиями договора подряда являются предмет договора, дата начала и дата окончания работ, в связи с чем ожидания Заказчика по цене работ могут быть сформированы как до, так и после выполнения работ (оказания услуг). В силу ст. 708 ГК РФ цена в тексте договора может быть твердой (Fixed Price) либо приблизительной (Time & Mate-rials / T&M) [21].

Риск того, что Заказчик откажется принимать выполненную работу (оказанную услугу). Для уменьшения вероятности наступления комплаенс-риска рекомендуется в тексте договора ***зафиксировать процедуру сдачи-приемки результата выполненных работ (оказанных услуг)***. Например, в договоре могут быть зафиксированы следующие условия:

1) подрядчик с помощью средств электронной почты указывает в теме письма, что программа для ЭВМ готова к сдаче, и извещает Заказчика о дате и времени сдачи (ст. 720 ГК РФ);

2) при отсутствии обоснованных претензий и замечаний Заказчик после сдачи выполненной работы (оказанной услуги, поставленного товара) сообщает об этом электронным письмом Подрядчику, указывая в теме письма, что программа для ЭВМ принята;

3) при наличии обоснованных претензий и замечаний Заказчик сообщает об этом электронным письмом Подрядчику, указывая в теме письма «*Мотивированный отказ от принятия программы для ЭВМ*» и в тексте письма излагает имеющиеся у него претензии и замечания. Подрядчик обязан в течение 10 рабочих дней со дня получения мотивированного отказа безвозмездно устранить претензии и замечания;

4) после устранения указанных претензий и замечаний Подрядчик повторно извещает Заказчика о дате и времени сдачи программы для ЭВМ. В случае отсутствия ответа Заказчика и/или отсутствия мотивированных претензий и возражений в течение 2-х рабочих дней программа для ЭВМ считается принятой Заказчиком без претензий на 3-й рабочий день с даты получения Заказчиком уведомления, что программа для ЭВМ готова к сдаче.

Риск того, что Заказчик откажется от оплаты выполненной работы (оказанной услуги). Согласно ст. 702 ГК РФ Заказчик обязуется принять результат выполненных работ и оплатить его [21]. Следовательно, основанием для оплаты выполненных работ является факт приемки работ без претензий и замечаний. Таким образом, для нивелирования комплаенс-риска рекомендуется зафиксировать в тексте договора следующие условия:

1) Подрядчик обязан в течение 2-х рабочих дней с даты принятия Заказчиком результата работ направить Заказчику оригинал подписанного со своей стороны Акта сдачи-приемки работ в 2-х экземплярах;

2) Заказчик обязан в течение 5-ти рабочих дней после получения от Подрядчика оригинала Акта сдачи-приемки работ направить Подрядчику подписанный Заказчиком оригинал и сканированную копию Акта сдачи-приемки работ;

3) в случае ненаправления Заказчиком подписанного Акта сдачи-приемки работ и/или письменных мотивированных возражений относительно его подписания Акт сдачи-приемки работ считается подписанным сторонами в том виде, в котором Заказчик его получил от Подрядчика, на 6-й рабочий день с даты получения Заказчиком оригинала Акта сдачи-приемки работ.

Риск того, что будет просрочка оплаты за выполненную Подрядчиком работу (оказанную Исполнителем услугу, поставленный Поставщиком товар). Для уменьшения негативного влияния данного комплаенс-риска в тексте договора рекомендуется ***зафиксировать порядок применения мер санкционирования в случае нарушения порядка и сроков оплаты***, зафиксировав в тексте договора следующие условия:

1) в случае просрочки Заказчиком оплаты Подрядчик вправе потребовать с Заказчика неустойку в размере 0,1 % от цены за каждый день просрочки. До внесения полной оплаты по договору право пользования результатом работ Заказчику не предоставляется;

2) в случае просрочки Заказчиком предоплаты/оплаты продолжительностью более 30 календарных дней Подрядчик вправе в одностороннем внесудебном порядке отказаться от исполнения договора с направлением письменного уведомления об отказе Заказчику за 5 рабочих дней до даты отказа. С даты отказа от исполнения договора сделка считается расторгнутой в части обязательств Подрядчика, а в части взаиморасчетов сторон сделка продолжает действовать до окончания таких расчетов.

Риск судебного иска от Заказчика (Подрядчика, Исполнителя, Поставщика). Полностью нивелировать данный комплаенс-риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации. Для этого необходимо добросовестно исполнить предусмотренные договором обязательства, а также обеспечить «правовую чистоту» проектных документов (проектные документы должны полностью соответствовать требованиям действующего законодательства. Кроме того, в текст договора рекомендуется включить

следующее условие: Стороны договора признают юридическую силу и возможность использования в случае спора положений, зафиксированных в договоре.

Риск признания сделки недействительной. В качестве примера рассмотрен договор об отчуждении исключительного права на программу для ЭВМ, который согласно п. 2 ст. 1234 ГК РФ должен быть заключен в письменной форме [21]. В случае несоблюдения этого условия сделка считается незаключенной, а исключительное право не переданным от правообладателя к правоприобретателю. Последствия от нарушения данного условия представлены в деле № А40-81328/2011 [86], где истец обратился в суд с требованием запретить использовать программу «HIST DoCoMo» и взыскать убытки в виде упущенной выгоды в размере 124,2 млн руб., а ответчик во встречном иске просил признать сделку недействительной.

Согласно гл. 37 ГК РФ существенными условиями договора подряда являются предмет договора, дата начала и дата окончания работ [21]. Следовательно, для нивелирования данного комплаенс-риска необходимо, чтобы в тексте договора существенные условия были точно сформулированы и корректно формализованы.

Риск того, что будет невозможно досрочно и в одностороннем порядке расторгнуть сделку. Анализ судебных решений показал, что сторона сделки, как правило, не может досрочно и в одностороннем порядке расторгнуть договор, не причинив существенного материального вреда, поэтому для уменьшения вероятности материализации данного комплаенс-риска и его возможного негативного влияния рекомендуется проектные работы дифференцировать на этапы с указанием даты их начала и окончания.

Риск того, что предмет договора будет сформулирован неточно и/или формализован некорректно. Уменьшение вероятности наступления данного комплаенс-риска возможно при повышении уровня зрелости в части управления коммуникациями и управления договорами в проекте.

Риск неверной квалификации вида сделки. Для уменьшения вероятности материализации данного комплаенс-риска рекомендуется обеспечить соответствие между текстом договора и требованиями действующего законодательства.

Риск допущения некорректных и неточных формулировок в тексте договора. Нивелировать риск можно при повышении

уровня зрелости в части управления коммуникациями проекта, так как выработка корректных и точных формулировок возможна при согласованных действиях заинтересованных сторон.

Риск того, что между сторонами будет не учтен порядок распределения экономии, которая может быть получена по факту выполненных работ (оказанных услуг, поставленных товаров). В соответствии со ст. 710 ГК РФ в случаях, когда фактические расходы Подрядчика оказались меньше тех, которые зафиксированы в тексте, Подрядчик сохраняет право на оплату работ по цене, предусмотренной договором [21].

Риск отсутствия связи с Заказчиком. Для нивелирования данного комплаенс-риска рекомендуется в текст договора включить следующее условие: длительный простой трудовых ресурсов Подрядчика, превышающий 5 рабочих дней, оплачивается Заказчиком по тарифу простоя трудовых ресурсов Подрядчика. Тариф простоя трудовых ресурсов Подрядчика равен 1 тыс. руб. за 1 чел./ч.

Риск того, что Заказчик не предоставит и/или будет предоставлять с большой задержкой информацию, необходимую для выполнения работ (оказания услуг, поставки товаров). Для нивелирования комплаенс-риска рекомендуется в текст договора включить следующие условия: сроки выполнения работ не учитывают время ожидания ответов на запросы Подрядчика, непосредственно связанные с выполнением работ по договору, если продолжение выполнения работ без решения указанных в запросе вопросов не представляется возможным. Срок выполнения работ продлевается на период простоя.

Риск изменения требований в процессе выполнения работ (оказания услуг, поставки товаров), т. е. выявление новых и/или существенное уточнение ранее согласованных требований. В качестве примера можно рассмотреть дело № А55-9384/2018 [87], где внесение частых корректировок Заказчиком в ранее согласованное техническое задание привело к тому, что новые требования Подрядчику пришлось реализовывать за свой счет.

Уменьшение вероятности материализации комплаенс-риска и его возможного негативного влияния зависит от методического инструментария, используемого Подрядчиком для выполнения работ (оказания услуг) — Agile или Waterfall (гибкая и каскадная методики разработки и управления проектами соответственно).

Если Подрядчик применяет методику Waterfall, то любые изменения требований могут привести к отклонению от запланированных проектных целей. В связи с этим рекомендуется в тексте договора фиксировать «жесткие» условия изменения требований, например, в следующем виде: изменение технических решений, техническая поддержка, наполнение контентом, прочие работы, не поименованные в договоре и приложениях к нему, не входят в объем работ по договору и выполняются Подрядчиком исключительно на основании заключенных Сторонами дополнительных соглашений либо самостоятельных договоров.

Если Подрядчик применяет методику Agile, то изменение требований не оказывает сильного негативного влияния на процесс достижения проектных целей, поэтому в текст договора рекомендуется включение более «мягких» условий, например: Заказчик и Подрядчик обсуждают изменения, предложенные любой из сторон, и приходят к одному из следующих решений:

а) изменения не вносятся в утвержденные подрядные работы;

б) изменения вносятся в утвержденные подрядные работы;

в) изменения не вносятся в утвержденные текущие подрядные работы, так как будут реализовываться в рамках самостоятельного договора.

Сроки реализации и стоимость изменений требований определяются Подрядчиком.

Риск того, что спецификация (устав, техническое задание и/или другая документация) будет неполной, недостоверной и/или не соответствовать требованиям национальных стандартов. Уменьшить вероятность материализации комплаенс-риска возможно, если проектные работы выполняют специалисты, обладающие необходимыми профессиональными компетенциями. Например, специалист по разработке спецификации должен соответствовать требованиям профессионального стандарта 06.022 «Системный аналитик».

Риск низкой вовлеченности Заказчика в процесс выполнения работ (оказания услуги). Согласно ст. 715 ГК РФ Заказчик вправе в любое время проверять ход и качество выполняемой работы [21]. Уменьшение вероятности материализации комплаенс-риска возможно при использовании инструментария управления проектами PMBOK Guide®, PRINCE2®, SCRUM и др.

Риск отсутствия у Заказчика корпоративной культуры, работников и опыта ведения деятельности в едином информационном пространстве с использованием информационных систем. Для нивелирования комплаенс-риска рекомендуется включить реестр рисков в качестве приложения к договору, где следует указать, что ответственность за управление данным риском закреплена за Заказчиком. В случае материализации комплаенс-риска также могут быть предусмотрены процедуры по изменению существенных и дополнительных условий договора.

Риск того, что у Заказчика будут отсутствовать отлаженные корпоративные процедуры по информационному взаимодействию и совместной работе его подразделений. Для нивелирования комплаенс-риска рекомендуется включить реестр рисков в качестве приложения к договору, в котором указать, что ответственность за управление данным риском закреплена за Заказчиком.

В случае материализации комплаенс-риска также могут быть предусмотрены процедуры по изменению существенных и дополнительных условий договора.

Риск отсутствия ключевых и квалифицированных специалистов на стороне Заказчика. Для уменьшения вероятности материализации комплаенс-риска в тексте договора рекомендуется формализовать следующее условие: «Ответственность за действия Заказчика, в том числе привлеченных Заказчиком третьих лиц, несет Заказчик».

Риск того, что не все заинтересованные лица со стороны Заказчика, участвующие в бизнес-процессах, автоматизируемых информационной системой, включены в процесс работы над созданием и согласованием проектных документов. Уменьшение вероятности материализации данного комплаенс-риска требует определенного уровня зрелости в части управления коммуникациями проекта, а именно должен быть создан механизм управления, включающий в элементы, которые своевременно создают, собирают, распространяют, хранят, получают и используют информацию.

Риск того, что будет проведена реструктуризация Заказчика (изменения организационной структуры, функциональных обязанностей, бизнес-процессов, локальных актов, финансово-экономической модели и др.). Для нивелирования

комплаенс-риска рекомендуется включить реестр рисков в качестве приложения к договору, в котором следует указать, что ответственность за управление данным риском закреплена за Заказчиком.

В случае материализации комплаенс-риска также могут быть предусмотрены процедуры по изменению существенных и дополнительных условий договора.

Риск того, что Подрядчик (Исполнитель, Поставщик) исполнитель) не исполнит свои обязательства, предусмотренные договором (например, невыполнение заявленных требований в срок либо невыполнение в полном объеме и др.). Для увеличения лояльности Заказчика и уменьшения вероятности материализации комплаенс-риска в части невыполнения Подрядчиком заявленных требований в срок или работ в полном объеме в тексте договора рекомендуется зафиксировать порядок санкционирования добавлением следующего условия: «В случае невыполнения или несвоевременного выполнения работ в полном объеме Заказчик вправе начислить Подрядчику неустойку в размере 0,1 % от цены работ по соответствующему этапу за каждый день просрочки обязательств».

В части, касающейся качества работ, необходимо опираться на ст. 723 ГК РФ, согласно которой в случаях, когда результат выполненной работы имеет ненадлежащее качество, Заказчик вправе по своему выбору потребовать от Подрядчика безвозмездного устранения недостатков в разумный срок, соразмерного уменьшения установленной за работу цены и/или возмещения своих расходов на устранение недостатков [21].

Риск того, что Подрядчик (Исполнитель, Поставщик) будет утаивать информацию о реальном положении дел от Заказчика и/или искажать ее. В соответствии со ст. 716 ГК РФ подрядчик обязан немедленно предупредить заказчика и до получения от него указаний приостановить работу при обнаружении не зависящих от подрядчика обстоятельств, которые представляют собой угрозу для получения запланированного результата либо создают невозможность завершения работ в срок [21]. Информирование Заказчика о реальном положении дел в ИТ-проекте является обязательством Подрядчика, которое закреплено в действующем гражданском законодательстве.

Риск отсутствия общего видения конечного продукта у заинтересованных сторон. Уменьшение вероятности материализации комплаенс-риска требует определенного уровня зрелости в части управления коммуникациями проекта, а именно должен быть создан механизм управления, включающий структурные и инфраструктурные элементы, которые своевременно создают, собирают, распространяют, хранят, получают и используют информацию.

Риск того, что в процессе выполнения работ (оказания услуг, поставки товаров) Подрядчик (Исполнитель, Поставщик) не сможет своими силами исполнить заявленные в договоре обязательства. Если сделка требует от Подрядчика выполнить работу лично, то Подрядчик вправе согласно ст. 706 ГК РФ привлечь к исполнению своих обязательств других лиц (субподрядчиков) [21].

Риск выявления Подрядчиком (Исполнителем, Поставщиком) скрытых, не обнаруженных на этапе планирования источников дополнительных затрат. В силу ст. 709 ГК РФ цена работы может быть твердой или приблизительной [21]. Следовательно, для уменьшения вероятности материализации комплаенс-риска рекомендуется использование условий, с учетом которых цена будет рассчитываться на основании фактически израсходованных ресурсов Подрядчика (T&M).

Риск распространения сведений, порочащих деловую репутацию Подрядчика (Исполнителя, Поставщика). Согласно ст. 152 ГК РФ деловая репутация признается нематериальным благом, защита которого гарантирована действующим законодательством, поэтому за распространение информации, которая порочит честь и достоинство, законодателем установлена гражданско-правовая, административная и уголовная ответственность [21].

Административным законом предусмотрена ответственность за оскорбление, т. е. унижение чести и достоинства, выраженное в неприличной форме (ст. 5.61 КоАП РФ [66]). Совершение данного правонарушения влечет наложение административного штрафа.

Уголовным законом предусмотрено такое понятие, как клевета (ст. 128.1 УК РФ), т. е. распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию [88].

Риск нарушения исключительных прав на результат интеллектуальной деятельности. Для увеличения лояльности Заказчика и уменьшения вероятности материализации комплаенс-риска в договоре следует формализовать следующие условия:

а) Подрядчик гарантирует Заказчику, что на момент предоставления Заказчику права использования результата выполненных работ, Подрядчик будет являться его единственным правообладателем;

б) в случае претензий со стороны третьих лиц по вопросам авторских, патентных или любых иных прав на результат работ, Подрядчик берет на себя обязательство самостоятельно урегулировать возникшие разногласия с третьими лицами и понести все расходы, необходимые для такого урегулирования, включая судебные издержки.

Риск взыскания правообладателем (автором) вознаграждения за использование его исключительных прав на результат интеллектуальной деятельности. Ярким примером материализации данного комплаенс-риска является дело № 2-38/2019 (2-4158/2018)~М-608/2018, в котором рассматривался спор между программистом, создавшим программу «eLearning Metadata Manager», с одной стороны, и ООО «Интервим» и Veeam Software Group GmpH, с другой стороны. Согласно материалам дела после увольнения программист обнаружил, что в созданной им программе исчез знак охраны авторского права «©», что стало основанием для обращения в суд [89].

Изучив обстоятельства дела, Приморский районный суд г. Санкт-Петербурга признал программиста автором программы «eLearning Metadata Manager», утвердил за ним исключительное право и взыскал в его пользу с ООО «Интервим» и Veeam Software Group GmpH по 1,6 млн руб. Кроме того, обе организации суд обязал выплатить 2,6 млн руб. за воспроизведение программы, а Veeam Software Group GmbH уплатить еще 17,6 млн руб. за предоставление коммерческого доступа к программе.

Уменьшение вероятности материализации комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте (договорами отчуждения исключительного права, передачи исключительного права на основании лицензии, договором авторского заказа, трудового договора и др.

Риск того, что правообладатель (автор) запретит использовать результат интеллектуальной деятельности. В качестве примера материализации данного комплаенс-риска рассмотрены материалы дела № А40-202764/18-110-1552 [90], согласно которым истец обратился в Арбитражный суд г. Москвы с требованием защитить его исключительные права и запретить ответчику использование специализированного медицинского мессенджера «Medsenger» для онлайн-взаимодействия врачей и пациентов.

Примером подобной ситуации является дело о плагиате программного кода (№ А60-27815/2012) [91], в котором правообладатель программы «Аптека-Урал» обратился в суд с требованием запретить правообладателю программы «Quartfarm» распространение и использование каким-либо иным способом его программы. В ходе судебного разбирательства Арбитражный суд Свердловской области установил, что программа «Quartfarm» является результатом переработки программы «Аптека-Урал».

Показательным является дело № А40-117808/10-12-740 [92], в котором истец просил суд взыскать с ответчика 1 485 497,00 руб. за нарушение исключительных прав на программу для ЭВМ.

Уменьшение вероятности материализации комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте, в частности, договорами отчуждения исключительного права, передачи исключительного права на основании лицензии, авторского заказа, трудовым договором и др.

Риск невозможности признания исключительного права на результат интеллектуальной деятельности за правообладателем (автором). Уменьшение вероятности материализации комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте, в частности, договором отчуждения исключительного права, договором передачи исключительного права на основании лицензии, договором авторского заказа, трудового договора и др.

Риск создания нежелательного производного произведения. В силу ст. 1259 ГК РФ производные произведения являются отдельными произведениями [21]. Следовательно, исключительные права на результат интеллектуальной деятельности будут принадлежать субъекту, который будет перерабатывать (модифици-

ровать) ранее созданную программу для ЭВМ, поэтому для нивелирования комплаенс-риска рекомендуется включить в текст договора следующее условие: Заказчик не имеет права изменять любым способом переданную ему во владение программу для ЭВМ, например, проводить декомпилирование, реассемблирование, реижиниринг и иные другие переработки (модификации).

Риск ограничения для последующих сублицензионных договоров. Для уменьшения возможного материального ущерба от материализации данного комплаенс-риска в тексте договора рекомендуется предусмотреть штраф за несогласованное ограничение для последующих сублицензионных договоров.

Риск расторжения договора в «сублицензионной цепочке» договоров. Для уменьшения возможного материального ущерба от материализации данного комплаенс-риска в тексте договора рекомендуется предусмотреть штраф за преждевременное расторжение договора.

Риск отсутствия связи с субподрядчиком. Согласно ст. 706 ГК РФ генеральный Подрядчик несет перед Заказчиком ответственность за последствия неисполнения или ненадлежащие исполнение обязательств субподрядчиком [21], уменьшение вероятности материализации данного комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте.

Риск того, что полученный субподрядчиком результат (оказанная услуга) не будут соответствовать ожиданиям заинтересованных сторон. Уменьшение вероятности материализации данного комплаенс-риска возможно при повышении уровня зрелости в части управления коммуникациями в проекте.

Риск судебного иска от субподрядчика. Полностью нивелировать данный комплаенс-риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации. Для этого необходимо добросовестно исполнить предусмотренные договором обязательства, а также обеспечить «правовую чистоту» проектных документов, т. е. проектные документы должны полностью соответствовать требованиям действующего законодательства. Кроме того, в текст договора рекомендуется включить следующее условие: Стороны признают юридическую силу и возможность использования в случае спора положения, зафиксированные в договоре.

Риск гибели и/или повреждения электронного оборудования (компьютеров, серверов и др.) и другого имущества в результате пожара, затопления водой и др. Уменьшение вероятности материализации комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте, а именно договором страхования (гл. 48 ГК РФ [21]).

Риск гибели и/или повреждения электронного оборудования (компьютеров, серверов и др.) и другого имущества в результате противоправных действий третьих лиц (умышленное уничтожение или повреждение имущества, уничтожение или повреждение имущества по неосторожности, хулиганство, вандализм). Уменьшение вероятности материализации данного комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте, а именно договором страхования (гл. 48 ГК РФ [21]).

Риск промышленного шпионажа. Промышленный шпионаж представляет собой форму недобросовестной конкуренции, при которой осуществляется незаконное получение, использование, разглашение информации, составляющей коммерческую, служебную или иную охраняемую законом тайну, с целью получения преимуществ при осуществлении предпринимательской деятельности.

Согласно ст. 3 Федерального закона от 29.07.2004 № 98-ФЗ «О коммерческой тайне» под коммерческой тайной понимается режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду [93].

В связи с этим для уменьшения возможного материального ущерба от материализации данного комплаенс-риска рекомендуется заключать с заинтересованными сторонами проекта соглашения о неразглашении конфиденциальной информации (non-disclosure agreement, NDA).

Риск утечки конфиденциальных данных. Для уменьшения возможного материального ущерба от материализации комплаенс-риска в договоре рекомендуется предусмотреть следующие условия:

а) условия договора, приложений и дополнительных соглашений к нему конфиденциальны и не подлежат разглашению в течение всего срока действия договора и в течение 3 лет после прекращения его действия;

б) в случае неисполнения или ненадлежащего исполнения обязательств конфиденциальности Сторона несет ответственность в соответствии с действующим законодательством и обязуется полностью возместить причиненный ущерб, включая упущенную выгоду.

Риск получения штрафа за нарушение действующего законодательства (например, привлечение к ответственности органами ФНС, Пенсионным фондом РФ и др.). Данный комплаенс-риск является внешним риском, который не может быть нивелирован либо ослаблен с помощью условий договора.

Риск изменения норм действующего законодательства. Полностью нивелировать данный комплаенс-риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации. Для этого необходимо добросовестно исполнить предусмотренные договором обязательства, а также обеспечить «правовую чистоту» проектных документов, т. е. проектные документы должны полностью соответствовать требованиям действующего законодательства.

Риск материализации обстоятельств непреодолимой силы, которые окажут значительное влияние на ход выполнения работ (оказания услуг). Для уменьшения возможного материального ущерба от материализации данного комплаенс-риска в тексте договора рекомендуется предусмотреть следующее условие: Сторона на время действия обстоятельств непреодолимой силы освобождается от ответственности за неисполнение/ненадлежащее исполнение договорных обязательств.

Под обстоятельствами непреодолимой силы понимаются стихийные бедствия, военные действия любого характера, блокады, эмбарго, забастовки, запрет на экспорт/импорт, эпидемия, антитеррористические мероприятия, розыскные и оперативные мероприятия правоохранительных органов.

Риск нарушения норм действующего законодательства. Полностью нивелировать комплаенс-риск с помощью условий

договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации. Для этого необходимо добросовестно исполнить предусмотренные договором обязательства, а также обеспечить «правовую чистоту» проектных документов, т. е. проектные документы должны полностью соответствовать требованиям действующего законодательства.

Примеры фрагментов текста договора, нивелирующего вышеперечисленные риски, представлены в приложении 1.

Литература

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

2. Nikolaenko V., Sidorov A. Analysis of 105 IT Project Risks // Journal of Risk and Financial Management, 2023. Vol. 16(1). No. 33. P. 1–20.

3. Аналитики заявили о росте кибератак на критическую инфраструктуру на 150 % [Электронный ресурс]: ГК «РосБизнесКонсалтинг». URL: https://clck.ru/W5Z2o (дата обращения: 04.04.2023).

4. Николаенко В.С. Управление компьютерными рисками в критических информационных инфраструктурах топливно-энергетического комплекса // Инновации в менеджменте. 2021. 4 (30). С. 10–17.

5. Фадейкина Н. Эволюция взглядов на категории «риск» и «неопределенность» в экономической науке // Риск: ресурсы, информация, снабжение, конкуренция. 2013. № 3. С. 202–208.

6. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ISO 31000:2009. Risk management – Principles and guidelines (IDT). М.: Стандартинформ, 2012. 19 с.

7. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. ISO 31000:2018. Risk management – Guidelines (IDT). М.: Стандартинформ, 2020. 19 с.

8. Балабанов И.Т. Риск-менеджмент. М.: Финансы и статистика, 1996. 192 с.

9. Машков Д.М. Научные подходы к управлению рисками промышленных предприятий // Инженерный вестник Дона. 2014. Т. 31. № 4–1. С. 65.

10. Филимонов Д.И. Классификация рисков кадровой безопасности в деятельности IT-структур // Экономика и предпринимательство. 2017. № 5–1 (82–1). С. 682–685.

11. Бурков В.Н., Новиков Д.А. Как управлять проектами. М.: Синтег, 1997. 188 с.

12. Мазур И.И., Шапиро В.Д. Управление проектами. М.: Высшая школа, 2001. 502 с.

13. Project management body of knowledge. Guide 4th edition (PMBOK-4). Project Management Institute (PMI), 2008. 506 p.

14. Project management body of knowledge. Guide 5th edition (PMBOK-5). – Project Management Institute (PMI), 2013. 616 p.

15. Project management body of knowledge. Guide 6th edition (PMBOK-6). Project Management Institute (PMI), 2017. 756 p.

16. Sanghera P. PMP exam in depth, second edition: project management professional study guie for the PMP exam. Course technology, a part of Cengage Learning, 2010. 592 p.

17. Enterprise Risk Management. Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017. 16 p.

18. Риски в современном бизнесе / Грабовый П.Г. [и др.]. М.: Алане, 1994. 200 с.

19. Шохин Е.И. Финансовый менеджмент. М.: Издательский дом «ФБК-ПРЕСС», 2002. 408 с.

20. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска. М.: Физматлит, 2011. 620 с.

21. Гражданский кодекс Российской Федерации (ГК РФ). Комментарии к последним изменениям. М.: АБАК, 2019. 752 с.

22. Даль В.И. Толковый словарь живого великорусского языка. М.: Цитадель, 1998. 11465 с.

23. Management of Risk: Guidance for Practitioners (M_o_R®). The Office of Government Commerce, 2010. 160 p.

24. Managing Successful Projects with PRINCE2 (PRINCE2®). TSO, 2017. 412 p.

25. Качалов Р.М. Управление хозяйственным риском. М.: Наука, 2002. 192 с.

26. Мадера А.Г. Риски и шансы. Неопределенность, прогнозирование и оценка. М.: Красанд, 2014. 448 с.

27. Мадера А.Г. Принятие решений в условиях неопределенности при актуализации в будущем множества возможных шансов и рисков // Экономические науки. 2014. № 4. С. 136–140.

28. Вигерс К., Битти Д. Разработка требований к программному обеспечению. 3-е изд., доп. СПб.: БХВ, 2022. 736 с.

29. Мануйленко В.В. От Базеля I к Базелю III: возможности реализации в российской банковской системе // Финансы и кредит, 2011. № 14 (446). С. 8–20.

30. Зубов В.П. Заметки о Джироламо Кардано // Вопросы истории естествознания и техники, 2010. Т. 31. № 3. С. 3–40.

31. Анцупов Л.П., Рустамов Т.Р. Из истории развития теории вероятностей // Студенческий вестник. 2022. № 47–5 (239). С. 19–22.

32. Галкина В., Колпакова Л. Деятельность лондонской страховой компании Ллойд на рынке страхования // Океанский менеджмент. 2018. № 1 (2). С. 7–16.

33. Курихин С.В. Теория внешней торговли в работе Адама Смита «Исследование о природе и причинах богатства народов» // Вектор экономики. 2019. № 5 (35). С. 139.

34. Милль Дж. С. Основы политической экономии. Т. 2. М.: 1980. 482 с.

35. Тюнен И.Г. Изолированное государство. М.: Экономическая жизнь, 1926. 329 с.

36. Найт Ф.Х. Риск, неопределенность и прибыль. М.: Дело, 2003. 360 с.

37. Макашева Н.А. Неопределенность, вероятность, этика: Дж. М. Кейнс, Л. Мизес, Ф. Найт // Вопросы экономики. 2013. № 10. С. 47–65.

38. Нейман Дж. фон, Моргенштерн О. Теория игр и экономическое поведение. М.: Наука, 1970. 708 с.

39. Меню Harvard Business Review [Электронный ресурс]: официальный сайт. URL: https://hbr.org/ (дата обращения: 04.04.2023).

40. Финансовая отчетность Apple Inc. по форме 10-K за 2021 год [Электронный ресурс]: United states securities and exchange commission, Washington. URL: https://clck.ru/rgwSv (дата обращения: 04.04.2023).

41. О бухгалтерском учете: Федеральный закон от 06.12.2011 № 402-ФЗ [Электронный ресурс]: КонсультантПлюс. URL: https://clck.ru/32sZGU (дата обращения: 04.04.2023).

42. О Кодексе корпоративного управления: Письмо Банка России № 06-52/2463 от 10.04.2014 [Электронный ресурс]: КонсультантПлюс. URL: https://clck.ru/34bht6 (дата обращения: 04.04.2023).

43. США вернули Colonial Pipeline большую часть от уплаченного хакерам выкупа [Электронный ресурс]: ГК «РосБизнесКонсалтинг». URL: https://clck.ru/VMkiJ (дата обращения: 04.04.2023).

44. Американская страховая компания заплатила хакерам $40 млн. Это крупнейший выкуп … [Электронный ресурс]: электронный журнал Inc. URL: https://clck.ru/ V2hpQ (дата обращения: 04.04.2023).

45. Бельгия заявила о масштабной кибератаке со «шпионскими» целями [Электронный ресурс]: ГК «РосБизнесКонсалтинг». URL: https://clck.ru/V5sbS (дата обращения: 04.04.2023).

46. All of JBS's U.S. Beef Plants Were Forced Shut by Cyberattack [Электронный ресурс]: информационное агентство «Bloom-berg». URL: https://clck.ru/VFrq5 (дата обращения: 04.04.2023).

47. McDonald's сообщил об утечке данных из-за хакерской атаки [Электронный ресурс]: FORBES: финансово-экономический журнал. URL: https://clck.ru/VU2P6 (дата обращения: 04.04.2023).

48. В одном из регионов ФРГ впервые ввели режим ЧС из-за кибератаки [Электронный ресурс]: ГК «РосБизнесКонсалтинг». URL: https://clck.ru/W4qKF (дата обращения: 04.04.2023).

49. «Алроса» не сможет заплатить по евробондам $7,75 млн из-за санкций [Электронный ресурс]: сетевое издание «ВЕДОМОСТИ». URL: https://clck.ru/rdwnT (дата обращения: 04.04.2023).

50. Николаенко В.С. Негативные и позитивные риски в ИТ-проектах // Вестник московского университета. Сер. 21 «Управление (государство и общество)». 2018. № 3. С. 91–124.

51. Ключников В.О. Идентификация рисков ИТ-проектов // Государственное управление. Электронный вестник, 2009. № 20. С. 1−7.

52. Ключников В.О. Опционный метод управления рисками в инвестиционных ИТ-проектах // Вестник Московского университета. Сер. 21 «Управление (государство и общество)». 2010. № 1. С. 69–78.

53. Ключников В.О. Реальные опционы в проектах информационных технологий // Российское предпринимательство. 2011. № 12-2. С. 118–124.

54. Никонов В.А. Управление рисками. Как больше зарабатывать и меньше тратить. М.: Альпина Паблишерз, 2009. 285 с.

55. Ефимов В.В. Сборник методов поиска новых идей и решений управления качеством. Ульяновск: УлГТУ, 2011. 194 с.

56. Crawley F., Tyler B. Hazard identification methods. Institute of Chemical Engineers, 2003. 98 p.

57. Card A., Ward J., Clarkson P. Beyond FMEA: the structured what-if technique (SWIFT) // Healthcare Risk Manage. 2012. Vol. 31. P. 23–29.

58. Авдошин С.М., Песоцкая Е. Ю. Информатизация бизнеса. Управление рисками. М. : ДМК Пресс, 2011. 176 с.

59. Песоцкая Е.Ю. Управление рисками в ИТ-проектах // Альманах современной науки и образования. 2008. № 1(8). С. 157−159.

60. Песоцкая Е.Ю. Управление рисками при внедрении ИТ-проектов // Успехи современного естествознания. 2008. № 1. С. 11−13.

61. Lewis S., Smith K. Lessons Learned from Real World Application of the Bow-tie Method // 6th Global Congress on Process Safety. 2010. P. 1−20.

62. Wijayanti D., Sukwika T., Ramli S. Analisis Insiden Fatality Akibat Covid-19 Menggunakan Metode 5 Why, SCAT, BowTie, dan ISM // Jurnal Migasian. 2022. 6(1). P. 84–92.

63. ГОСТ Р 31010-2011. Методы оценки риска. ISO/IEC 31010:2009. Risk management – Risk assessment techniques (IDT). М.: Стандартинформ, 2012. 74 с.

64. Merna T., Al-Thani F. Corporate risk management. John Wiley & Sons, Ltd, 2008. 2nd ed. 443 p.

65. The Department of Defense (DoD) United States of America. Risk Management Guide for DOD Acquisition, 2006. Sixth Edition. Version 1.0. 34 p.

66. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ). М.: Проспект, 2019. 688 с.

67. Талеб Н.Н. Черный лебедь. Под знаком непредсказуемости. 2-е изд., доп. М.: КоЛибри; Азбука-Аттикус, 2015. 736 с.

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

69. Дмитриев И.О., Николаенко В.С. Лидерство как позитивный риск, наступление которого необходимо для успешного завершения ИТ-проекта // Современные проблемы и тенденции развития экономики, управления и информатики в XXI в.: сб. науч. статей по материалам науч.-практ. конф. с междунар. участием; под ред. Шаминой Л.К. М.: Финансовый университет при Правительстве Российской Федерации, 2016. С. 12–16.

70. Российские системы распознавания и сопровождения лидера / Гага В.А. [и др.]. Томск: Изд-во Томского гос. ун-та, 2011. 196 с.

71. Селиховкин И. Управление ИТ-проектом. Эффективная система «с нуля» в любой организации. СПб., 2010. 90 с.

72. Поляков А.А., Ключников В. О. Опционный метод управления рисками в инвестиционных ИТ проектах // Вестник Московского университета. Сер. 21 «Управление (государство и общество)». 2010. № 1. С. 69–78.

73. Поляков А.А. Информационные системы в управлении // Вестник Московского университета. Сер. 21 «Управление (государство и общество)». 2006. № 3. С. 21–39.

74. Николаенко В.С. Модель зрелости проектного управления: управление рисками проекта // Инновации в менеджменте. 2021. № 1 (27). С. 38–47.

75. Об утверждении профессионального стандарта «Специалист по управлению рисками» (Код 08.018): Приказ Министерства труда и социальной защиты Российской Федерации № 564н от 30.08.2018 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/33yG92 (дата обращения: 04.04.2023).

76. О государственной гражданской службе Российской Федерации: Федеральный закон № 79-ФЗ от 27.07.2004 [Электронный ресурс]: КонсультанПлюс. URL: https://clck.ru/33yGte (дата обращения: 04.04.2023).

77. Национальный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 33001-2017. Информационные технологии. Оценка процесса. Понятия и определения. М.: Стандринформ, 2017. 16 с.

78. Межгосударственный стандарт ГОСТ ISO 9000-2011. Системы менеджмента качестве. Общие положения и словарь. М.: Стандартинформ, 2020. 28 с.

79. Smith D., Bruyns M., Evans S. A project manager's optimism and stress management and IT project success // International Journal of Managing Projects in Business. 2021. 4(1). P. 10–27.

80. Похолков Ю.П., Николаенко В.С. Адаптация инструментария риск-менеджмента для высших учебных заведений Российской Федерации // Вестник московского университета. Сер. 21 «Управление (государство и общество)». 2018. № 4. С. 102–115.

81. Льюис Р.Д. Деловые культуры в международном бизнесе. От столкновения к взаимопониманию. М.: Дело, 1999. 440 с.

82. Решение Арбитражного суда Ямало-Ненецкого автономного округа по делу № А81-9472/2019 от 02.01.2020 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/kScgp (дата обращения: 04.04.2023).

83. Решение Арбитражного суда Томской области от 16.05.2017 г. по делу № А67-1623/2017 [Электронный ресурс]: электронная версия. URL: https://clck.ru/jec2f (дата обращения: 04.04.2023).

84. Решение Арбитражного суда города Москвы по делу № А40-248300/21-5-1672 от 09.02.2022 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/kRTqS (дата обращения: 04.04.2023).

85. Решение Арбитражного суда города Москвы по делу № А40-32033/19-47-287 от 02.10.2020 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/kTCuY (дата обращения: 04.04.2023).

86. Решение Арбитражного суда города Москвы по делу № А40-81328/11 от 07.04.2014 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/nTfSN (дата обращения: 04.04.2023).

87. Решение Арбитражного суда Самарской области по делу № А55-9384/2018 от 26.09.2018 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/jeqZv (дата обращения: 04.04.2023).

88. Комментарий к Уголовному кодексу Российской Федерации (УК РФ). 8-е изд., перераб. и доп. – М.: Проспект, 2019. 800 с.

89. Решение Приморского районного суда города Санкт-Петербурга по делу № 2-38/2019 (2-4158/2018;) ~ М-608/2018 от 11.06.2019 г. [Электронный ресурс]: электронная версия. URL: https:// clck.ru/ SiN5M (дата обращения: 04.04.2023).

90. Решение Арбитражного суда города Москвы по делу № А40-202764/18-110-1552 от 01.02.2019 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/jfczi (дата обращения: 04.04.2023 г.).

91. Решение Арбитражного суда Свердловской области по делу № А60-27815/2012 от 01.10.2012 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/jfedG (дата обращения: 04.04.2023).

92. Решение Арбитражного суда города Москвы по делу № А40-117808/10-12-740 от 30.11.2010 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/SiNiS (дата обращения: 04.04.2023).

93. О коммерческой тайне: Федеральный закон № 98-ФЗ от 29.07.2004 [Электронный ресурс]: КонсультантПлюс. URL: https: //clck.ru/gLnDf (дата обращения: 04.04.2023).

Приложение 1

ПРИМЕРЫ КОВЕНАНТОВ В ДОГОВОРЕ НА СОЗДАНИЕ ПРОГРАММЫ ДЛЯ ЭВМ

ДОГОВОР № XXXX
НА СОЗДАНИЕ ПРОГРАММЫ ДЛЯ ЭВМ

г. XXXXX XX.XX.XXXX

ООО «XXXXX», именуемое в дальнейшем **«Подрядчик»**, в лице генерального директора XXXXX X.X., действующего на основании Устава, с одной стороны и **ООО «YYYYY»,** в лице Генерального директора YYYYY Y.Y., действующего на основании Устава, именуемое в дальнейшем **«Заказчик»**, с другой стороны, а вместе именуемые **«Стороны»**, заключили настоящий Договор (далее — Договор) о нижеследующем:	*Риск признания сделки недействительной*

1. ПОНЯТИЯ

1.1. **Анкета** — опросный лист, заполняемый участником Программы лояльности (ПЛ) Заказчика. Анкета размещается в Личном кабинете сайта Заказчика. ***Обязательные поля анкеты*** — вопросы Анкеты, которые обязательны для заполнения участником Программы лояльности. ***Необязательные поля анкеты*** — вопросы Анкеты, которые необязательны для заполнения участником Программы лояльности.

1.2. **Партнер** — юридическое лицо и/или индивидуальный предприниматель, определенное Заказчиком в качестве Партнера, являющийся участником Программы лояльности, которому Заказчик предоставляет доступ к интерфейсу управления программным обеспечением (ПО) XXX с целью реализации Партнером маркетинговых активностей.

1.3. **ПО XXXXX, Система** — программа для ЭВМ «XXXXX XXXXX», предназначенный для решения задач автоматизации Программы лояльности

1.4. **Программа лояльности (ПЛ)** — программа потребительской лояльности, реализуемая в торговой сети Заказчика и/или его Партнеров, автоматизация которой производится с использованием ПО XXXXX.

1.5. **Программный продукт** — Личный кабинет (ЛК) участника Программы лояльности Заказчика, интегрированный с Системой, функциональность которого приведена в Приложении № 3 Договора.

1.6. **Сайт Личного кабинета участника Программы лояльности Заказчика** (далее — Личный кабинет участника Программы лояльности) — персональный раздел участника Программы лояльности на Сайте Программы лояльности Заказчика.

2. ПРЕДМЕТ ДОГОВОРА

2.1. Подрядчик обязуется по заданию Заказчика выполнить **комплекс работ (далее — работы)** по созданию Программного продукта в виде Личного кабинета участника Программы лояльности Заказчика с типовым дизайнерским решением, а Заказчик обязуется принять результат выполненных Подрядчиком работ и оплатить их в соответствии с условиями Договора.	
2.2. Содержание и объем работ, выполняемых Подрядчиком по Договору:	*Риск того, что предмет договора будет сформулирован неточно и/или формализован некорректно*
a) верстка дизайн-макетов и изобразительных элементов Программного продукта;	
b) адаптация и модификация Личного кабинета с использованием компонентов набора плагинов Модуля «Плагины Web-сайта» ПО XXXX для кастомизации под нужды Заказчика и обеспечения интеграции Личного кабинета с базой данных Заказчика, размещенной в Системе, с предварительным тестированием Программного продукта;	
c) адаптация Программного продукта для обеспечения взаимодействия с социальными сетями;	*Риск неверной квалификации вида сделки*
d) обеспечение доступности Программного продукта для использования участниками Программы лояльности, а именно размещение Личного кабинета в домене первого уровня на дисковом пространстве Поставщика услуг хостинга информационной и программной среды Личного кабинета (при условии регистрации домена Заказчиком и предоставления Заказчиком данных и сведений, необходимых для такого размещения).	
2.3. Описание функционала Личного кабинета указано в Приложении № 3 Договора.	

2.4. Дизайн ЛК представлен в Приложении № 1 Договора. Представленный дизайн является типовым и не подлежит изменению, кроме таких элементов, как контактные данные, логотип (товарный знак / знак обслуживания / коммерческое обозначение), цвет фона. 2.5. Изменение технических решений, техническая поддержка, наполнение контентом, прочие работы, не поименованные в Договоре и Приложениях к нему, не входят в объем работ по Договору и выполняются Подрядчиком исключительно на основании заключенных Сторонами дополнительных соглашений либо самостоятельных (отдельных) договоров. 2.6. Любые изменения и дополнения к Договору действительны лишь при условии, что они совершены в письменной форме и подписаны уполномоченными на то представителями Сторон.	*Риск изменения требований в процессе выполнения работ (оказания услуг), т. е. выявление новых и/или существенное уточнение ранее согласованных требований*

2.7. Работы по соответствующему Этапу считаются выполненными с момента подписания Сторонами Акта сдачи-приемки работ по соответствующему Этапу. 2.8. Описание Этапов указаны в Приложении № 4 Договора.	*Риск того, что будет невозможно досрочно и в одностороннем порядке расторгнуть сделку*

2.9. С момента зачисления на счет Подрядчика оплаты в соответствии с разделом 5 Договора, право использования результата выполненных работ (разработанного результата интеллектуальной деятельности) считается предоставленным Заказчику в соответствии с Договором на условиях **простой неисключительной лицензии**.	*Риск нарушения исключительных прав на результат интеллектуальной деятельности* *Риск ограничения для последующих сублицензионных договоров* *Риск расторжения договора в «сублицензионной цепочке» договоров*

При этом Заказчик вправе использовать результат выполненных работ в рамках Программы лояльности Заказчика, включая его воспроизведение (в том числе на ПК и мобильных устройствах и т. п.), его распространение (в том числе посредством предоставления Партнерам права его использования и т. п.) и доведение его до всеобщего сведения (в том числе посредством доведения до физических лиц (потребителей), для получения последними доступа к Личному кабинету из любого места и в любое время и т. п.) и прочее на протяжении всего срока действия исключительного права Подрядчика на результат работ по Договору без права на сублицензирование, изменение любым способом, декомпилирование, реассамблирование, реинжиниринг, осуществление иных модификаций, на территории всего мира.	*Риск создания нежелательного производного произведения*

2.10. Подрядчик заверяет Заказчика и гарантирует, что на момент предоставления Заказчику права использования результата выполненных работ (разработанного результата интеллектуальной деятельности): – Подрядчик будет являться единственным правообладателем результата выполненных по Договору работ, а также что выполненные по Договору работы и их результат не будут нарушать требования действующего законодательства РФ, в том числе не будут нарушать права и законные интересы третьих лиц (права собственности, авторские, смежные, договорные и связанные с ними личные неимущественные права); – не существует в настоящее время и не будет существовать каких-либо договоров, соглашений, лицензий, разрешений и иных обязательств Подрядчика, препятствующих Заказчику использовать результаты выполненных работ в соответствии с Договором.	*Риск нарушения исключительных прав (авторских прав) на результат интеллектуальной деятельности* *Риск того, что* правообладатель (автор) *запретит использовать результат интеллектуальной деятельности*

В случае возможных претензий со стороны третьих лиц по вопросам авторских, патентных или любых иных прав на результат работ по Договору (по состоянию на момент подписания Акта сдачи-приемки работ по Договору) Подрядчик берет на себя обязательство самостоятельно (без Заказчика) урегулировать возникшие разногласия с третьими лицами и понести все расходы, необходимые для такого урегулирования, включая судебные издержки. Согласно **ст. 406.1 ГК РФ** Подрядчик обязуется в срок не более **5 (пяти) рабочих дней** с даты предъявления соответствующего требования возместить все имущественные потери Заказчика, возникшие в случае предъявления третьими лицами к Заказчику требований в отношении результата выполненных Подрядчиком по Договору работ либо их части. Подрядчик не компенсирует имущественные потери Заказчика, возникшие в случае предъявления третьими лицами к Заказчику требований в отношении предоставленных Заказчиком Подрядчику для выполнения работ информации и материалов (в т. ч. включая, но не ограничиваясь, графические элементы, товарные знаки и знаки обслуживания, шрифты и иные элементы, требующие приобретения лицензии либо разрешения правообладателя на их использование). Заказчик примет необходимые действия, направленные на урегулирование конфликта с правообладателями в случае, если предоставленные Заказчиком Подрядчику в соответствии с Договором результаты интеллектуальной деятельности нарушат права указанных правообладателей, ввиду чего указанные правообладатели предъявят соответствующие мотивированные требования к Подрядчику. Заказчик возмещает документально подтвержденный ущерб, который был причинен Подрядчику правообладателями, чьи права были нарушены действиями Заказчика.	*Риск нарушения исключительных прав (авторский прав) на результат интеллектуальной деятельности* *Риск того, что правообладатель (автор) запретит использовать результат интеллектуальной деятельности*

3. ПРАВА И ОБЯЗАННОСТИ СТОРОН

3.1. **Подрядчик обязуется**:

3.1.1. Качественно и своевременно выполнить только те работы, которые предусмотрены Договором;

3.1.2. Безвозмездно устранить претензии и замечания к результату выполненных работ в течение **10 (десяти) рабочих дней** со дня доставки/вручения Подрядчику уведомления Заказчика о претензиях и замечаниях к результату выполненных работ, при условии, что претензии и замечания выявлены не позднее даты истечения гарантийного срока;

3.1.3. Нести иные обязанности, предусмотренные Договором.

3.2. **Заказчик обязуется**: 3.2.1. Направлять Подрядчику информацию, необходимую для выполнения Подрядчиком работ по Договору, в соответствии с письменными запросами Подрядчика, направленными по электронной почте. 3.2.2. Соблюдать порядок рассмотрения и согласования результатов работ согласно разделу 4 Договора. 3.2.3. Своевременно принять и оплатить результаты работ. 3.2.4. Предоставить данные, размещаемые в ЛК и доступные для редактирования Заказчиком в течение **5 (пяти) рабочих дней** с даты заключения Договора. 3.2.5. Предоставить форму Анкеты в течение **3 (трех) рабочих дней** с даты заключения Договора с указанием Обязательных и Необязательных полей. 3.2.6. За свой счет обеспечить регистрацию домена и получение SSL-сертификата на сайт с Личным кабинетом и предоставить Подрядчику для размещения Личного кабинета в течение **5 (пяти) рабочих дней** с даты заключения Договора. 3.2.7. Нести иные обязанности, предусмотренные Договором.	*Риск низкой вовлеченности Заказчика в процесс выполнения работ (оказания услуги)*

3.3. **Подрядчик имеет право**:

3.3.1. Указать в Программном продукте информацию о себе как о разработчике, а также ссылаться на выполненную работу в рамках портфолио.

3.3.2. Пользоваться иными своими правами, предусмотренными Договором.

3.4. **Заказчик имеет право**:

3.4.1. Проверять ход и качество выполнения работ, не вмешиваясь в деятельность Подрядчика.

3.4.2. Требовать выполнения работ в соответствии с условиями Договора.

3.4.3. Пользоваться иными своими правами, предусмотренными Договором.

3.5. Ответственность за действия ответственных и иных лиц Заказчика, в том числе привлеченных Заказчиком третьих лиц, несет Заказчик.	*Риск отсутствия ключевых и квалифицированных специалистов на стороне Заказчика (например, отсутствие лиц, которые могут определить требования к информационным системам)*

3.6. Подрядчик отвечает перед Заказчиком за действия (бездействие) всех третьих лиц, привлеченных им для выполнения работ по Договору, как за свои собственные.	*Риск того, что в процессе выполнения работ (оказания услуг) Подрядчик (Исполнитель) не сможет своими силами исполнить заявленные в договоре обязательства* *Риск того, что полученный субподрядчиком результат (оказанная услуга) не будут соответствовать ожиданиям заинтересованных сторон*

4. СДАЧА И ПРИЕМКА РЕЗУЛЬТАТОВ ВЫПОЛНЕННЫХ РАБОТ

4.1. Сдача результатов выполненных работ производится Подрядчиком в следующем порядке: 4.1.1. Подрядчик с помощью средств электронной почты, указывая в теме письма **«Результат работ готов к сдаче»**, извещает Заказчика о дате и времени сдачи выполненных работ. 4.1.2. В случае отсутствия обоснованных претензий и замечаний у Заказчика к результату работ Заказчик после сдачи работ сообщает об этом обратным электронным письмом Подрядчику, указывая в теме письма **«Результат работ принят»**. 4.1.3. При наличии обоснованных претензий и замечаний у Заказчика к результату работ Заказчик сообщает об этом электронным письмом Подрядчику, указывая в теме письма **«Мотивированный отказ от принятия результата работ»**, в котором излагает имеющиеся претензии и замечания. 4.1.4. Подрядчик обязан в течение **10 (десяти) рабочих дней** со дня получения от Заказчика Мотивированного отказа от принятия результата работ безвозмездно устранить претензии и замечания, указанные в Мотивированном отказе. После устранения указанных претензий и замечаний Подрядчик повторно с помощью средств электронной почты, указывая в теме письма **«Результат работ готов к сдаче»**, извещает Заказчика о дате и времени сдачи выполненных работ. Направление новых замечаний, не связанных с устранением ранее выявленных, не допускается. 4.1.5. В случае отсутствия ответа Заказчика на уведомление Подрядчика о готовности работ к сдаче и/или отсутствия письменных мотивированных возражений Заказчика в течение **2 (двух) рабочих дней** работы считаются принятыми Заказчиком без претензий по количеству и качеству на 3-й (третий) рабочий день с даты получения Заказчиком уведомления «Результат работ готов к сдаче».	*Риск того, что Заказчик откажется принимать выполненную работу (оказанную услугу)*

4.2. Подрядчик обязан в течение **2 (двух) рабочих дней** с даты принятия Заказчиком результата работ направить Заказчику оригинал подписанного со своей стороны Акта сдачи-приемки работ в 2-х экземплярах. 4.3. Заказчик обязан в течение **5 (пяти) рабочих дней** после получения от Подрядчика оригинала Акта сдачи-приемки работ направить Подрядчику подписанный Заказчиком оригинал и сканированную копию Акта сдачи-приемки работ. В случае если подписанный Акт сдачи-приемки работ и/или письменные мотивированные возражения относительно его подписания Заказчиком не направлены в указанный в п. 4.3 Договора срок Акт сдачи-приемки работ считается подписанным Сторонами в том виде, в котором Заказчик его получил от Подрядчика на 6-й (шестой) рабочий день с даты получения Заказчиком оригинала Акта сдачи-приемки работ.	*Риск того, что Заказчик откажется принимать выполненную работу* (*оказанную услугу*)

4.4. Подрядчик вправе сдавать работы поэтапно или единовременно.

5. РАЗМЕРЫ И ПОРЯДОК ОПЛАТЫ

5.1. Твердая цена выполненных Подрядчиком по Договору работ составляет **75 000 (семьдесят пять тысяч) российских рублей 00 копеек**. Твердая цена не включает в себя лицензионное вознаграждение Подрядчика за право пользования результатом работ (далее — Роялти). Роялти оплачивается Заказчиком отдельно в размере **2 000 (две тысячи) рублей 00 копеек в месяц**. Заказчик начинает выплачивать Роялти Подрядчику на следующий месяц, который идет за месяцем подписания Сторонами Акта сдачи-приемки работ. Заказчик производит оплату в рублях путем перечисления денежных средств на расчетный счет Подрядчика.	*Риск того, что Заказчик откажется от оплаты выполненной работы (оказанной услуги)*

5.2. Оплата выполненных Подрядчиком по Договору работ производится в соответствии со следующим графиком платежей: 5.2.1. **Предоплата в размере 50 %** от твердой цены работ, указанной в п. 5.1 Договора, вносится Заказчиком в течение **5 (пяти) рабочих дней** с даты подписания Договора и получения счета от Подрядчика. 5.2.2. **Оплата в размере 50 %** от твердой цены работ, указанной в п. 5.1 Договора, вносится Заказчиком в течение **5 (пяти) рабочих дней** с даты подписания Сторонами Акта сдачи-приемки работ. 5.3. Заказчик производит оплату в рублях путем перечисления денежных средств на расчетный счет Подрядчика.	*Риск того, что Заказчик откажется от оплаты выполненной работы (оказанной услуги)*

5.4. В случае если фактические расходы Подрядчика оказались меньше зафиксированных в п. 5.1 Договора, Подрядчик сохраняет право на оплату работ по цене, предусмотренной Договором, если Заказчик не докажет, что полученная Подрядчиком экономия повлияла на качество выполненных работ.	*Риск того, что между сторонами будет не учтен порядок распределения экономии, которая может быть получена по факту выполненных работ (оказанных услуг)*

6. СРОК ВЫПОЛНЕНИЯ РАБОТ

6.1. Сроки выполнения Подрядчиком работ – с **даты внесения Заказчиком предоплаты** по **00.00.0000 г.** включительно.	*Риск того, что сделка, заключенная между сторонами, будет недействительной*

6.2. Сроки выполнения работ не учитывают: a) время на проведение работ на стороне Заказчика либо третьих лиц, привлеченных Заказчиком, в случае проведения таких работ в соответствии с условиями Договора; b) время, фактически потраченное Заказчиком на рассмотрение, согласование и утверждение проектных документов, подготовленных Подрядчиком; c) время, фактически потраченное Заказчиком на рассмотрение и согласование результатов выполненных Подрядчиком работ; d) время ожидания ответов на запросы Подрядчика, непосредственно связанные с выполнением работ по Договору, если продолжение выполнения работ без решения указанных в запросе вопросов объективно не представляется для Подрядчика возможным. Срок выполнения работ продлевается на период вышеуказанных событий. 6.3. Длительный простой трудовых ресурсов Подрядчика, вызванный событиями, указанными в п. 6.2 Договора и превышающий **5 (пять) рабочих дней**, оплачивается Заказчиком по тарифу простоя трудовых ресурсов Подрядчика. **6.4.** Тариф простоя трудовых ресурсов Подрядчика равен **1 000 рублей 00 копеек** за **1 (один) человеко-час**.	*Риск отсутствия связи с Заказчиком* *Риск того, что Заказчик не предоставит и/или будет предоставлять с большой задержкой информацию, необходимую для выполнения работ (оказания услуг)*

7. ОТВЕТСТВЕННОСТЬ СТОРОН

7.1. За неисполнение или ненадлежащее исполнение своих обязательств по Договору Стороны несут ответственность в соответствии с Договором, а также действующим законодательством РФ.	*Риск судебного иска от Заказчика/ Подрядчика*

7.2. Все споры и разногласия между Сторонами, прямо или косвенно вытекающие из Договора или связанные с ним, подлежат рассмотрению в претензионном порядке. Претензия составляется в письменной форме и должна быть направлена в адрес Стороны заказным письмом, а сканированная копия претензии отправляется на электронный адрес уполномоченного представителя получающей Стороны. Срок ответа на претензию — **10 (десять) рабочих дней** со дня ее получения на электронный адрес уполномоченного представителя получающей Стороны. 7.3. В случае невозможности прийти к согласию (неполучения ответа на претензию, неурегулирования спора во внесудебном порядке и в иных случаях) спор, возникший из Договора или в связи с ним, подлежит передаче в Арбитражный суд г. XXXXX.	*Риск судебного иска от Заказчика/ Подрядчика*

7.4. В случае невыполнения, несвоевременного выполнения, выполнения не в полном объеме Подрядчиком работ по Договору Заказчик вправе начислить Подрядчику неустойку (пени) в размере **0,1% (ноль целых одной десятая)** от твердой цены работ по соответствующему Этапу за каждый день просрочки обязательств, но не более **20% (двадцати)** от твердой цены работ по данному Этапу.	*Риск того, что Подрядчик (Исполнитель) не исполнит свои обязательства, предусмотренные договором (например, невыполнение заявленных требований в срок, невыполнение заявленных требований в полном объеме и др.)*

7.5. В случае просрочки Заказчиком оплаты по Договору, Подрядчик вправе потребовать с Заказчика неустойку (пени) в размере **0,1% (ноль целых одной сотой процента)** от твердой цены работ за каждый день просрочки, но не более **20% (двадцати)** от твердой цены работ. До внесения полной оплаты по Договору право пользования результатом работ Заказчику не предоставляется. 7.6. В случае просрочки Заказчиком предоплаты/оплаты по Договору продолжительностью в совокупности более **30 (тридцати) календарных дней** Подрядчик вправе в одностороннем внесудебном порядке отказаться от исполнения Договора с направлением письменного уведомления об отказе Заказчику за **5 (пять) рабочих дней** до даты отказа. С даты отказа от исполнения Договора Договор считается расторгнутым в части обязательств Подрядчика, а в части взаиморасчетов Сторон Договор продолжает действовать до окончания таких расчетов.	*Риск того, что будет просрочка оплаты за выполненную Подрядчиком работу (оказанную Исполнителем услугу)*

7.7. Подрядчик не несет ответственности за несоответствие информации, переданной Заказчиком и необходимой для выполнения обязательств по Договору, действующему законодательству РФ.	*Риск того, что спецификация (устав, техническое задание и/или другая документация) будет неполной, недостоверной и/или не соответствовать требованиям национальных стандартов*

8. СРОК ДЕЙСТВИЯ ДОГОВОРА, ПОРЯДОК ЕГО ПРЕКРАЩЕНИЯ ИЛИ РАСТОРЖЕНИЯ

8.1. Договор вступает в силу с даты его заключения, указанного в преамбуле Договора, и действует на протяжении срока действия исключительного права правообладателя на Личный кабинет и Модуль «Плагины Web-сайта» соответственно.

8.2. Договор может быть досрочно расторгнут по письменному соглашению Сторон.	*Риск того, что будет невозможно досрочно и в одностороннем порядке расторгнуть сделку*

8.3. Сторона на время действия **обстоятельств непреодолимой силы**, освобождается от ответственности за неисполнение/ненадлежащее исполнение договорных обязательств. Под обстоятельствами непреодолимой силы понимаются препятствия для выполнения затронутой Стороной договорных обязательств, находящиеся вне разумного контроля затронутой Стороны, а именно стихийные бедствия, военные действия любого характера, блокады, эмбарго, забастовки, запрет на экспорт/импорт, эпидемия, антитеррористические мероприятия, розыскные и оперативные мероприятия правоохранительных органов, принятие законодательными органами нормативно-правовых актов, препятствующих Сторонам в исполнении договорных обязательств, возникновения которых невозможно было предвидеть и предусмотреть при заключении Договора, и наступления и действия которых (или последствий которых) невозможно было разумно избежать или преодолеть. Подтверждением наступления и действия обстоятельства непреодолимой силы является документ, выданный **Торгово-промышленной палатой РФ**. Сторона, подвергшаяся действию обстоятельства непреодолимой силы, обязана принять все разумные меры по уменьшению последствий такого события, а также по возможности незамедлительно уведомить другую Сторону о его наступлении, а равно о прекращении препятствования такого события исполнению затронутой Стороной договорных обязательств, при этом срок исполнения договорных обязательств приостанавливается Сторонами на срок, в течение которого будет действовать обстоятельство непреодолимой силы и его последствия, препятствующие исполнению затронутой Стороной договорных обязательств. Если обстоятельство непреодолимой силы или его последствия, препятствующие исполнению затронутой Стороной договорных обязательств, будут продолжаться **более 3 (трех) месяцев**, Стороны обязаны обсудить дальнейшую судьбу Договора и зафиксировать свои достигнутые по этому вопросу договоренности посредством заключения соответствующего дополнительного соглашения к Договору.	*Риск материализации обстоятельств непреодолимой силы, которые окажут значительное влияние на ход выполнения работ (оказания услуг)*

9. ГАРАНТИЙНЫЕ ОБЯЗАТЕЛЬСТВА

9.1. Гарантийный срок на выполненные работы по разработке ЛК устанавливается продолжительностью 12 (двенадцать) месяцев с даты подписания Сторонами окончательного Акта сдачи-приемки работ.	*Риск допущения ошибок участниками проекта при реализации проекта (bugs)*

9.2. В случае, если Заказчик или третья сторона без согласия Подрядчика вносят какие-либо изменения в программный код, гарантийные обязательства Подрядчика прекращаются.

10. КОНФИДЕНЦИАЛЬНОСТЬ

10.1. Условия Договора, приложений и дополнительных соглашений к нему конфиденциальны и не подлежат разглашению в течение всего срока действия Договора и в течение **3 (трех) лет** после прекращения его действия. 10.2. Стороны обязуются не разглашать третьим лицам информацию о любой хозяйственной деятельности другой Стороны и соблюдать конфиденциальность в отношении любой информации и документов, которые будут получены в связи с исполнением Договора. 10.3. В случае неисполнения или ненадлежащего исполнения Стороной обязательств, предусмотренных настоящим разделом Договора, Сторона несет ответственность в соответствии с действующим законодательством и обязуется полностью возместить причиненный ущерб, включая упущенную выгоду. 10.4. Помимо возмещения причиненного ущерба в случае разглашения конфиденциальной информации Сторона обязуется уплатить штраф в размере **1 000 000 (один миллион) рублей 00 копеек** в течение **30 (тридцати) календарных дней**.	*Риск утечки конфиденциальных данных*

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

11.1. Стороны признают юридическую силу и возможность использования в качестве письменных доказательств в случае спора и/или для толкования положений Договора составленных в соответствии с Договором в электронной форме документов, а равно сканированных копий тех документов, в отношении которых Договором или действующим законодательством РФ не предусмотрено, что они предоставляются в оригинале/в электронной форме – переданных посредством электронной почты путем обмена сообщениями между адресами электронной почты уполномоченных сотрудников/представителей Сторон. Поименованные в Договоре приложения к Договору будучи подписанными Сторонами составляют его неотъемлемую часть. **11.2.** Подтверждением направления письма (юридически значимого сообщения) на электронный почтовый ящик является сохраненная отправившей стороной в ее электронном почтовом ящике скан–копия претензии в формате PDF, JPEG, TIFF или PNG, а также распечатанная бумажная версия отправленного сообщения – такое письмо считается полученным адресатом в день его отправки отправителем.	Риск судебного иска от Заказчика/ Подрядчика

11.3. Договор составлен в двух экземплярах, имеющих одинаковую юридическую силу, по одному экземпляру для каждой из Сторон.

Приложения:

приложение № 1 «Типовое дизайнерское решение Личного кабинета»;

приложение № 2 «Анкета Участника Программы лояльности для реализации на сайте Программы лояльности»;

приложение № 3 «Описание функционала Личного кабинета участника Программы лояльности»;

приложение № 4 «Проектный план».

12. РЕКВИЗИТЫ И ПОДПИСИ СТОРОН

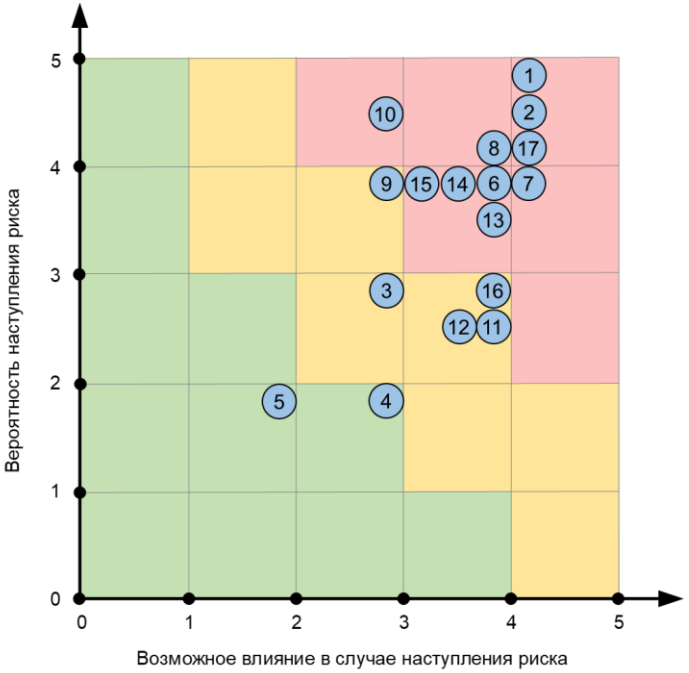
Подрядчик: **Заказчик:**

Приложение 2

РИСКИ ВНЕШНЕЙ СРЕДЫ: 2023 ГОД

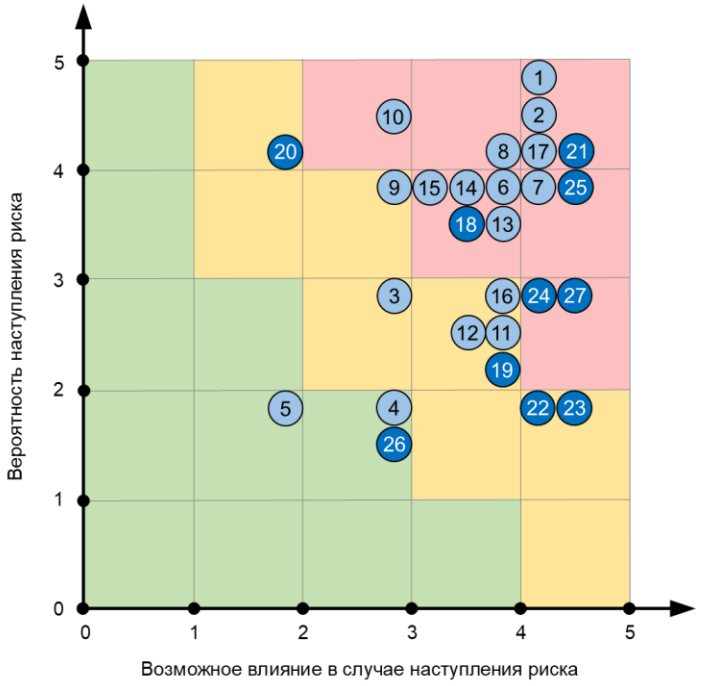
ЭКОНОМИКА

1. Риск изменения цен на нефть
2. Риск изменения цен на газ
3. Риск изменения цен на металл
4. Риск изменения цен на уголь
5. Риск изменения цен на пшеницу
6. Риск дефицита (профицита) федерального бюджета
7. Риск изменения курса валют
8. Риск внесения изменений в Федеральный закон «О федеральном бюджете»
9. Риск изменения размера государственного долга
10. Риск изменения темпов инфляции
11. Риск изменения ключевой ставки
12. Риск изменения процентов кредитных и депозитных ставок
13. Риск изменения темпов роста экономики
14. Риск изменения уровня жизни населения
15. Риск изменения фондовых индексов
16. Риск дефолта
17. Риск экономического кризиса



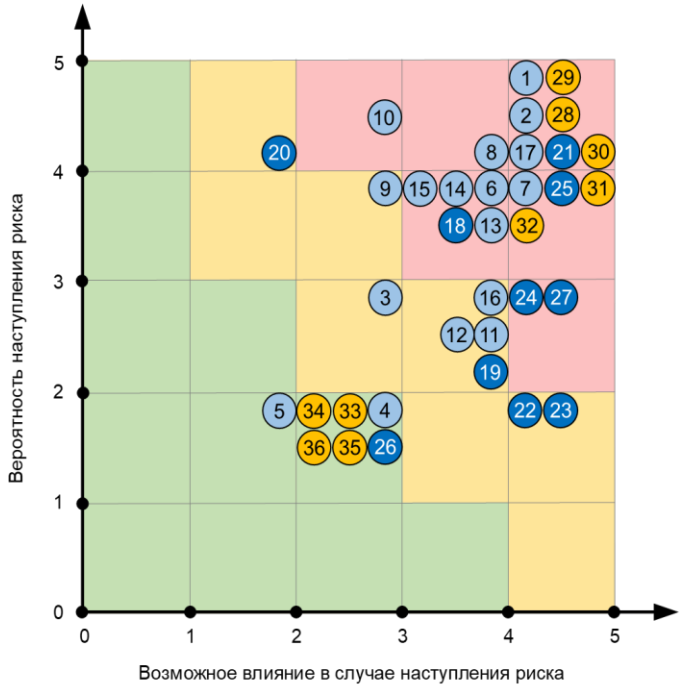
ОБЩЕСТВО

- 18. Риск изменения уровня смертности
- 19. Риск изменения уровня рождаемости
- 20. Риск того, что на рынке труда будут отсутствовать квалифицированные кадры
- 21. Риск социальной напряженности
- 22. Риск изменения уровня образования
- 23. Риск изменения уровня медицины
- 24. Риск изменения уровня преступности
- 25. Риск изменения уровня миграции
- 26. Риск голода
- 27. Риск изменения численности



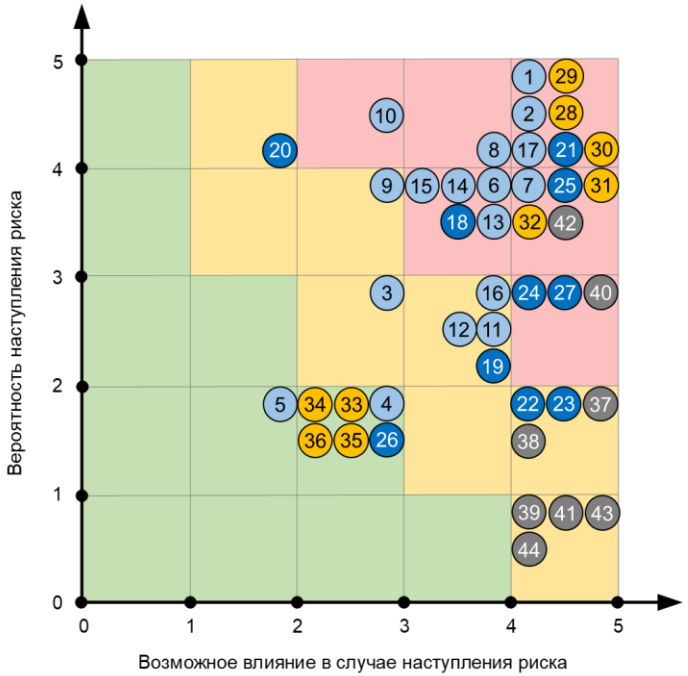
ПОЛИТИКА

- 28. Риск изменения геополитического давления
- 29. Риск расширения альянса НАТО
- 30. Риск военного конфликта
- 31. Риск террористического акта
- 32. Риск изменения норм действующего законодательства
- 33. Риск интеграции РФ с внешними субъектами
- 34. Риск государственного переворота
- 35. Риск национализации и экспроприации имущества
- 36. Риск массовых беспорядков



ОКРУЖАЮЩАЯ СРЕДА

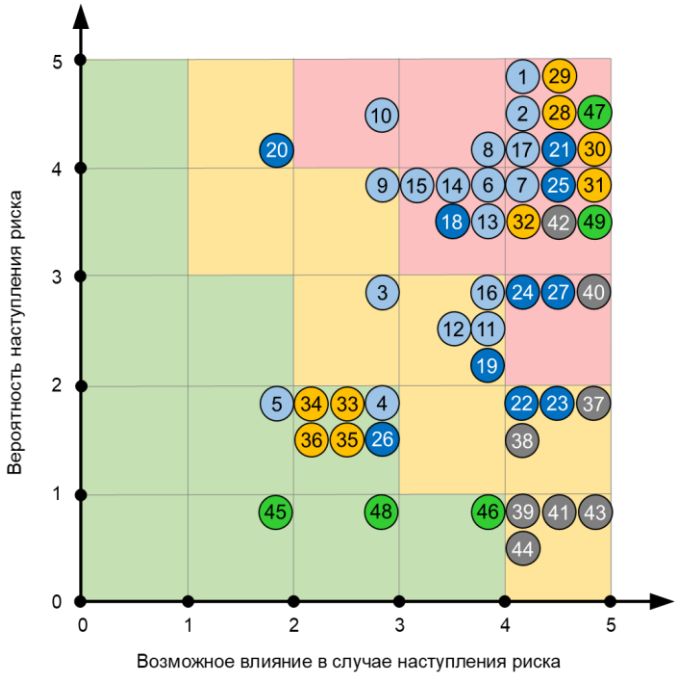
- 37. Риск нехватки природных ресурсов
- 38. Риск изменения климата
- 39. Риск загрязнения окружающей среды
- 40. Риск пандемии
- 41. Риск наводнения
- 42. Риск радиоактивного заражения
- 43. Риск тайфуна
- 44. Риск землетрясения



ТЕХНИКА И ТЕХНОЛОГИИ

- 45. Риск атаки искусственного интеллекта (ИИ)
- 46. Риск отключения Интернета
- 47. Риск кибератак на критическую информационную инфраструктуру (КИИ)
- 48. Риск использования новых технологий
- 49. Риск поломки оборудования

- Оценка риска не изменилась по сравнению с прошлым годом
- Новый риск
- Оценка риска выросла по сравнению с прошлым годом
- Оценка риска снизилась по сравнению с прошлым годом



Приложение 3

РЕЕСТР 170 УНИВЕРСАЛЬНЫХ РИСКОВ

Номер риска	Название риска
1. КОММЕРЧЕСКИЕ РИСКИ (БИЗНЕС-РИСКИ)	
Риски, связанные с пользователем (клиентом)	
1.1	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям пользователя (клиента)
1.2	Риск низкой вовлеченности пользователя (клиента) в процесс выполнения работы (оказания услуги, поставки товара)
Риски, связанные с коммерческим эффектом	
1.3	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не принесет ожидаемый коммерческий эффект
Риски, связанные с конкурентами	
1.4	Риск того, что конкуренты будут оказывать влияние на ход выполнения работы (оказания услуги, поставки товара)
Риски, связанные с товарами-субститутами	
1.5	Риск того, что товары-субституты будут оказывать влияние на ход выполнения работы (оказания услуги, поставки товара)
2. КОМПЛАЕНС-РИСКИ	
Риски, связанные с Заказчиком	
2.6	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям Заказчика
2.7	Риск того, что Заказчик откажется принимать и/или оплачивать выполненную работу (оказанную услугу, поставленный товар)
2.8	Риск того, что будет просрочка оплаты за выполненную Подрядчиком работу (оказанную Исполнителем услугу, поставленный Поставщиком товар)
2.9	Риск судебного иска от Заказчика
2.10	Риск признания сделки недействительной
2.11	Риск того, что будет невозможно досрочно и односторонне порядке расторгнуть сделку

2.12	Риск того, что существенные условия сделки будут сформулированы и формализованы в тексте договора неточно и/или некорректно
2.13	Риск неверной квалификации вида сделки
2.14	Риск допущения неточных и/или некорректных формулировок в тексте договора
2.15	Риск того, что между сторонами будет не учтен порядок распределения экономии, которая может быть получена по факту выполненной работы (оказанной услуги, поставленного товара)
2.16	Риск отсутствия связи с Заказчиком
2.17	Риск того, что Заказчик не предоставит и/или будет предоставлять с большой задержкой информацию, необходимую для выполнения работы (оказания услуги, поставки товара)
2.18	Риск изменения требований в процессе выполнения работы (оказания услуги, поставки товара), т.е. будут выявлены новые и/или будет существенное уточнение ранее согласованных требований
2.19	Риск того, что спецификация (устав, техническое задание и/или другая документация) будет неполной, недостоверной и/или не соответствовать требованиям национальных стандартов
2.20	Риск низкой вовлеченности Заказчика в процесс выполнения работы (оказания услуги, поставки товара)
2.21	Риск отсутствие у Заказчика корпоративной культуры, работников и опыта ведения деятельности в едином информационном пространстве с использованием информационных систем
2.22	Риск того, что у Заказчика будут отсутствовать отлаженные корпоративные процедуры по информационному взаимодействию и совместной работы его подразделений
2.23	Риск отсутствия ключевых и квалифицированных специалистов на стороне Заказчика (например, отсутствие лиц, которые могут определить требования к информационным системам)
2.24	Риск того, что не все заинтересованные лица со стороны Заказчика, участвующие в бизнес-процессах, автоматизируемых информационной системой, включены в процесс работы над созданием и согласованием проектных документов

2.25	Риск того, что будет реструктуризация Заказчика, т.е. на стороне Заказчика будут изменения его организационной структуры, функциональных обязанностей, бизнес-процессов, локальных актов, финансово-экономической модели и др.
Риски, связанные с Подрядчиком (Исполнителем, Поставщиком)	
2.26	Риск того, что Подрядчик (Исполнитель, Поставщик) не исполнит свои обязательства, предусмотренные договором (например, невыполнение заявленных требований в срок, невыполнение заявленных требований в полном объеме и др.)
2.27	Риск того, что Подрядчик (Исполнитель, Поставщик) будет утаивать информацию о реальном положении дел от Заказчика и/или искажать ее
2.28	Риск отсутствия общего виденья конечного продукта у заинтересованных сторон
2.29	Риск того, что в процессе выполнения работы (оказания услуги, поставки товара) Подрядчик (Исполнитель, Поставщик) не сможет своими силами исполнить заявленные в договоре обязательства
2.30	Риск выявления Подрядчиком (Исполнителем, Поставщиком) скрытых, не обнаруженных на этапе планирования источников дополнительных затрат
2.31	Риск распространения сведений, порочащих деловую репутацию Подрядчика (Исполнителя, Поставщика)
2.32	Риск судебного иска от Подрядчика (Исполнителя, Поставщика)
Риски, связанные с исключительным правом на результат интеллектуальной деятельности (РИД)	
2.33	Риск нарушения исключительных прав (авторских прав) на РИД
2.34	Риск взыскания правообладателем (автором) вознаграждения за нарушение исключительных прав (авторских прав) на РИД
.35	Риск того, что правообладатель (автор) запретит использовать РИД
2.36	Риск невозможности признания исключительного права (авторского права) на РИД за правообладателем (автором)
2.37	Риск создания нежелательного производного произведения
2.38	Риск ограничения для последующих сублицензионных договоров

2.39	Риск расторжения договора в «сублицензионной цепочке» договоров
Риски, связанные с субподрядчиком (субисполнителем, субпоставщиком)	
2.40	Риск отсутствия связи с субподрядчиком (субисполнителем, субпоставщиком)
2.41	Риск того, что полученный субподрядчиком (субисполнителем, субпоставщиком) результат (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям заинтересованных сторон
2.42	Риск судебного иска от субподрядчика (субисполнителя, субпоставщика)
Риски, связанные с имуществом	
2.43	Риск гибели и/или повреждения электронного оборудования (компьютеров, серверов и др.) и другого имущества в результате пожара, затопления водой и др.
2.44	Риск гибели и/или повреждения электронного оборудования (компьютеров, серверов и др.) и другого имущества в результате противоправных действий третьих лиц (умышленное уничтожение или повреждение имущества, уничтожение или повреждение имущества по неосторожности, хулиганство, вандализм)
Криминальные риски	
2.45	Риск промышленного шпионажа
2.46	Риск утечки конфиденциальных данных
2.47	Риск ограбления
Риски государственных(муниципальных) контрактов	
2.48	Риск признания недействительными государственного (муниципального) контракта (доступ к исполнению контракта без конкурентной борьбы)
2.49	Риск отказа от заключения государственного (муниципального) контракта
2.50	Риск того, что государственный (муниципальный) Заказчик откажется принимать и (или) оплачивать выполненную работу (оказанную услугу, поставленный товар)
2.51	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать требованиям государственного (муниципального) контракта
2.52	Риск того, что государственный (муниципальный) Заказчик в одностороннем порядке откажется от исполнения государственного (муниципального) контракта

3. ПРОЕКТНЫЕ РИСКИ	
Риски, связанные с руководителем проекта	
3.53	Риск того, что руководитель проекта допустит ошибку при оценивании стоимости проектных работ
3.54	Риск того, что руководитель проекта допустит ошибку при оценивании длительности проектных работ
3.55	Риск не учета отпусков и государственных праздников при создании плана проекта
3.56	Риск того, что руководитель проекта допустит ошибку при оценивании ресурсов, которые необходимы для выполнения проектных работ
3.57	Риск нерационального расходования ограниченных ресурсов проекта
3.58	Риск отсутствия знаний, навыков и опыта у руководителя проекта
3.59	Риск ухода руководителя проекта из проекта
3.60	Риск низкой производительности труда у руководителя проекта
3.61	Риск отсутствия заинтересованности руководителя проекта в успешном завершении проекта
3.62	Риск занятости руководителя проекта в других проектах
3.63	Риск неправильного ранжирования задач руководителем проекта
3.64	Риск завышения качества руководителем проекта
3.65	Риск отсутствия в проекте инструментария управления проектом (например, PRINCE2, SCRUM и др.)
3.66	Риск отсутствия ресурсов необходимых для выполнения проектных работ
3.67	Риск того, что по факту проектные работы окажутся значительно сложнее, чем предполагалось изначально
3.68	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений
3.69	Риск отсутствия резервов, необходимых для принятия материализовавшихся рисков
3.70	Риск потери и/или отсутствия контроля руководителем проекта
3.71	Риск конфликта между руководителем проекта и заинтересованными сторонами (например, Заказчиком, участниками команды и др.)

3.72	Риск того, что будет потеряна информация о материализовавшихся рисках, которая может потребоваться руководителю проекта в последующих проектах
3.73	Риск привлечения в проект руководителя проекта, который имеет профессиональное образование в области управления проектами
3.74	Риск привлечения в проект руководителя проекта, который имеет опыт управления проектами более 2-х лет
3.75	Риск того, что руководитель проекта будет самостоятельно формировать команду проекта
3.76	Риск изменения содержания проекта
3.77	Риск изменения длительности проекта
3.78	Риск изменения стоимости проекта
3.79	Риск изменения качества проекта
3.80	Риск декомпозиции большого проекта на малые проекты (длительностью не более 4-х месяцев)
Риски, связанные с участниками проекта	
3.81	Риск простоя трудовых ресурсов
3.82	Риск конфликта интересов между заинтересованными сторонами
3.83	Риск того, что не все заинтересованные стороны будут выявлены
3.84	Риск ухода на «больничный» участника проекта
3.85	Риск допущения ошибок участниками проекта при реализации проекта (bugs)
3.86	Риск значительной временной задержки в получении ответов на задаваемые вопросы между участниками проекта
3.87	Риск эффекта Кассандры, т.е. будет наблюдаться переизбыток каналов коммуникаций, доносящих актуальную информацию
3.88	Риск того, что фактическое время работы участников проектов будет менее 8 часов в день
3.89	Риск отсутствия знаний, навыков и опыта у участников проекта, необходимых для реализации требований
3.90	Риск ухода ключевого участника проекта из проекта
3.91	Риск перегрузки трудовых ресурсов (например, из-за переработки, работы сверхурочно и др.)
3.92	Риск того, что участники проекта будут неправильно оценивать трудозатраты, которые необходимы для выполнения проектных работ

3.93	Риск того, что участники проекта будут неправильно декомпозировать проектные работы
3.94	Риск занятости участников проекта в других проектах
3.95	Риск изменения состава участников проекта в процессе реализации проекта
3.96	Риск непонимания участниками проекта того, какой результат должен быть получен по завершению проекта
3.97	Риск нескоординированных действий участников проекта
3.98	Риск низкой производительности труда у участников проекта
3.99	Риск отсутствия заинтересованности у участников проекта в успешном завершении проекта
3.100	Риск негативной социально-психологической атмосферы
3.101	Риск недостатка коммуникаций между участниками проекта
3.102	Риск использования устаревших технологий участниками проекта
3.103	Риск привлечения в проект высококвалифицированного работника
3.104	Риск того, что численность участников проекта будет не более 6 человек
3.105	Риск коллаборации между руководителем и участниками проекта (групповая выработка решений, реализация индивидуальных идей и др.)
3.106	Риск привлечения в проект сторонних экспертов и советников
3.107	Риск того, что согласованные заинтересованными сторонами изменения будут утеряны
3.108	Риск того, что запрошенная функциональность программы для ЭВМ будет реализована, но никто не будет ее использовать
Риски, связанные с оборудованием	
3.109	Риск отключения электричества
3.110	Риск отключение интернета
3.111	Риск применения ранее не используемых технологий участниками проекта
3.112	Риск поломки оборудования
4. РИСКИ ВНЕШНЕЙ СРЕДЫ	
Риски, связанные с экономикой	
4.113	Риск изменения цен на нефть
4.114	Риск изменения цен на газ
4.115	Риск изменения цен на металлы
4.116	Риск изменения цен на уголь
4.117	Риск изменения цен на зерно

4.118	Риск дефицита (профицита) федерального бюджета
4.119	Риск изменения курса валют
4.120	Риск внесения изменений в Федеральный закон «О федеральном бюджете»
4.121	Риск изменения размера государственного долга
4.122	Риск изменения темпов инфляции
4.123	Риск изменения ключевой ставки Банка России
4.124	Риск изменения процентов кредитных и депозитных ставок
4.125	Риск изменения темпов роста экономики
4.126	Риск изменения уровня жизни населения
4.127	Риск изменения фондовых индексов
4.128	Риск дефолта
4.129	Риск экономического кризиса
Риски, связанные с обществом	
4.130	Риск изменения уровня смертности
4.131	Риск изменения уровня рождаемости
4.132	Риск изменения численности населения
4.133	Риск того, что на рынке труда будут отсутствовать квалифицированные кадры
4.134	Риск социальной напряженности
4.135	Риск изменения уровня образования
4.136	Риск изменения уровня медицины
4.137	Риск изменения уровня преступности
4.138	Риск изменения уровня миграции
4.139	Риск голода
Риски, связанные с политикой	
4.140	Риск изменения геополитического давления
4.141	Риск расширения альянса НАТО
4.142	Риск военного конфликта
4.143	Риск террористического акта
4.144	Риск изменения норм действующего законодательства
4.145	Риск нарушения норм действующего законодательства
4.146	Риск материализации обстоятельств непреодолимой силы, которые окажут значительное влияние на ход выполнения работ (оказания услуг, поставки товаров)
4.147	Риск интеграции РФ с внешними субъектами
4.148	Риск государственного переворота
4.149	Риск национализации и экспроприации имущества
4.150	Риск массовых беспорядков

Риски, связанные с окружающей средой	
4.151	Риск нехватки природных ресурсов
4.152	Риск изменения климата
4.153	Риск загрязнения окружающей среды
4.154	Риск пандемии
4.155	Риск наводнения
4.156	Риск радиоактивного заражения
4.157	Риск тайфуна
4.158	Риск землетрясения
Риски, связанные с техникой и технологиями	
4.159	Риск атаки искусственного интеллекта (ИИ)
4.160	Риск отключения глобальной компьютерной сети Интернет
4.161	Риск атаки на критическую инфраструктуру
4.162	Риск атаки на критическую информационную инфраструктуру (КИИ)
4.163	Риск заражения КИИ вредоносным программным обеспечением
4.164	Риск частичного и/или полного отказа в обслуживании КИИ
4.165	Риск использования новой технологии
4.166	Риск неправомерного доступа, копирования, предоставления и/или распространения конфиденциальной информации
4.167	Риск неправомерного уничтожения и/или модификации конфиденциальной информации
4.168	Риск неправомерного блокирования конфиденциальной информации
4.169	Риск поломки оборудования из-за отсутствия импортных комплектующих
4.170	Риск нехватки электроэнергии

Учебное издание

Николаенко Валентин Сергеевич

БЕЗУПРЕЧНЫЙ РИСК-МЕНЕДЖМЕНТ

Учебное пособие

Подписано в печать 07.11.23. Формат 60x84/16.
Усл. печ. л. 8,14. Тираж 100 экз. Заказ 265
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Томский государственный университет
систем управления и радиоэлектроники»
634050, г. Томск, пр. Ленина, 40.
Тел. (3822) 53-30-18. E-mail: rio@main.tusur.ru

РЕЦЕНЗИЯ
на учебное пособие канд. экон. наук,
доцента кафедры автоматизации обработки информации ТУСУР
Николаенко Валентина Сергеевича
«БЕЗУПРЕЧНЫЙ РИСК-МЕНЕДЖМЕНТ»

Управление рисками является одним из направлений менеджмента, который позволяет значительно повысить шансы на успешное достижение стратегических, тактических, операционных и проектных целей. В частности, исследования проведенные The Standish Group в 50 000 проектах показали, что полученный материальный ущерб от наступления одного негативного риска в среднем оценивается в 1 000 долл. Глубокий анализ причин наступления негативных рисков позволил установить, что данных материальных потерь можно было бы избежать превентивно воздействуя на негативные риски. Более того, эксперты The Standish Group в своих трудах отмечают, что стоимость проведения одной превентивной меры не превышал бы 1 долл.

В представленной рукописи, основываясь на материалах национальных (ГОСТ Р ИСО 31000-2010, ГОСТ Р ИСО 31000-2019 и др.) и международных (PMBOK® Guide, M_o_R®, PRINCE2®, COSO ERM и ISO) стандартов управления рисками автор последовательно рассматривает:

- понятия риска, неопределенности и риск-менеджмента;
- классификации рисков в зависимости от причин возникновения, масштаба воздействия, функциональной области организации, покупательной способностью денег, степени контролируемости, наступивших последствий, характера последствий наступления рисковых событий, частоты наступлений в ранее заключенных сделках и завершенных проектах и времени актуализации (наступления) рисков относительно фаз жизненного цикла проекта;
- анализ внутренней и внешней среды объектов риска, идентификацию рисков, анализ рисков, оценивание рисков, воздействие на риски, мониторинг и контроль рисков, а также методы оценки рисков;
- механизм внедрения риск-менеджмента в организации и проекты, который включает в себя документальное сопровождение, оценку результативности и эффективности от использования риск-менеджмента, возможные ментальные ловушки и влияние деловой культуры процессы управления рисками;
- способы элиминирования универсальных комплаенс-рисков с помощью ковенантов договора.

Следует отметить, что содержание ряда разделов рукописи основано на научных публикациях автора, посвященных проблемам управления рисками. В частности, «Analysis of 105 IT Project Risks», «Управление компьютерными рисками в критических информационных инфраструктурах топливно-

энергетического комплекса», «Негативные и позитивные риски в ИТ-проектах», «Внедрение риск-менеджмента в ИТ-проекты», «Лидерство как позитивный риск, наступление которого необходимо для успешного завершения ИТ-проекта», «Модель зрелости проектного управления: управление рисками проекта» и «Адаптация инструментария риск-менеджмента для высших учебных заведений Российской Федерации». Материалы рецензируемого учебного пособия ориентированы на освоение студентами профессиональных компетенций, прописанных в Государственном образовательном стандарте по направлению подготовки «Программная инженерия». Приобретенные знания позволят студентам успешно решать следующие профессиональные задачи: анализировать риски внешней среды, идентифицировать рисковые события, выявлять источники риска и прогнозировать возможные сценарии в случаях их материализации, оценивать вероятность и влияние рисков, разработать меры превентивного воздействия на риски и меры принятия рисков, а также осуществлять мониторинг и контроль рисков с помощью триггерных условий.

Принимая во внимание актуальность представленных в пособии материалов и их конкретную привязку к специфике профессиональной деятельности выпускника по направлению подготовки «Программная инженерия», считаю целесообразным опубликование рукописи В. С. Николаенко «Безупречный риск-менеджмент» в качестве учебного пособия по направлению подготовки «Программная инженерия».

Профессор школы инженерного предпринимательства Томского политехнического университета, д-р экон. наук, профессор

Никулина И.Е.