Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ» (ТУСУР)

ФАКУЛЬТЕТ ДИСТАНЦИОННОГО ОБУЧЕНИЯ (ФДО)

В. С. Николаенко

РИСК-МЕНЕДЖМЕНТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Учебное пособие

Томск 2024

УДК 005.334:351(075.8)
ББК 65.290-2я73
Н 634

Николаенко В. С.

Н 634 Риск-менеджмент в государственном управлении : учебное пособие / В. С. Николаенко. – Томск : Эль Контент, 2024. – 126 с.

ISBN 978-5-4332-0311-2

В учебном пособии представлены теоретические и практические аспекты управления различными видами рисков (негативными, позитивными, комплаенс-рисками, проектными, рисками внешней среды и др.) в системе публичного управления. Описан инструментарий оценки рисков, мониторинга и контроля, механизм воздействия и документального сопровождения.

Пособие предназначено для государственных (муниципальных) служащих, руководителей департаментов, подразделений, отделов, проектов, а также и студентов высших учебных заведений, обучающихся по направлениям подготовки в областях государственного управления и экономики.

ISBN 978-5-4332-0311-2

Оглавление

Введение

Необходимость управления рисками в системе публичного управления Российской Федерации обусловлена геополитическим давлением, которое создает каскад нежелательных рисков и негативных последствий в случаях их материализации. Яркими примерами наступления подобных последствий являются диверсия на «Северных потоках», введение потолка цен на сырую нефть и нефтепродукты, запрет на импорт товаров, экспортные ограничения, дискриминация отечественных компаний на мировом рынке и др. Анализ доктринальных документов недружественных стран, например, «Акт о противодействии противникам Америки посредством санкций», принятый Правительством США 24.07.2017, показывает, что геополитические противники намерены вести системную и планомерную работу, направленную против Российской Федерации и ее граждан, создавая новые угрозы для национальной безопасности.

Для элиминирования подобных нежелательных рисков отечественным законодателем актуализируются, разрабатываются и принимаются проактивные нормативные акты, доктрины, стратегии и национальные стандарты. Например, 172-ФЗ «О стратегическом планировании в Российской Федерации», 390-ФЗ «О безопасности», Стратегия национальной безопасности, Военная доктрина РФ, Доктрина информационной безопасности РФ, Стратегия экономической безопасности России до 2030 г., Стратегия научно-технологического развития, Стратегия экологической безопасности РФ на период до 2025 г. и др. Системообразующие механизмы управления рисками, методы оценки и способы воздействия на них законодатель закрепил в ГОСТ Р ИСО 31000 «Менеджмент риска. Принципы и руководство» и ГОСТ Р 31010 «Методы оценки риска».

Настоящее учебное пособие направлено на формализацию основных теоретических аспектов риск-ориентированного управления, представление практических инструментов по элиминированию угроз в государственном и муниципальном управлении, а также на формирование и развитие профессиональных компетенций в области управления рисками. Применение полученных знаний позволит государственным (муниципальным) служащим, руководителям департаментов, подразделений, отделов, проектов повысить шансы на достижение запланированных стратегических, тактических, операционных и проектных целей.

В первой главе пособия рассматриваются основные понятия и теоретические аспекты управления рисками, классификация рисков, а также приведены

материалы наиболее распространенных национальных и международных стандартов.

Во второй главе подробно анализируются процессы управления рисками и методы оценки, воздействия, мониторинга и контроля рисков. В данной главе представлен перечень универсальных коммерческих, комплаенс-, проектных и рисков внешней среды, механизм документального сопровождения риск-менеджмента.

В третьей главе описываются механизмы в системе публичного управления, ковенанты договора, элиминирующие комплаенс-риски, угрозы национальной безопасности Российской Федерации, управление рисками при осуществлении государственного контроля (надзора) и муниципального контроля, а также риски в сфере закупок товаров, работ, услуг для обеспечения го-сударственных и муниципальных нужд.

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

Соглашения, принятые в учебном пособии

Для улучшения восприятия материала в данном учебном пособии используются пиктограммы и специальное выделение важной информации.

Эта пиктограмма означает определение или новое понятие.

Пример

Эта пиктограмма означает пример. В данном блоке автор может привести практический пример для пояснения и разбора основных моментов, отраженных в теоретическом материале.

Контрольные вопросы по главе

1 Риски 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» [1]. Во французском «*risque*» трактуется как «объезжать утес». Другие специалисты предполагают, что слово «риск» имеет греческие корни «*ridsikon*», «*ridsa*», что означает «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 [2] ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство [3]
2. Угроза и/или опасность	И. Т. Балабанов [4] Д. М. Машков [5]
3. Неопределенность	Д. И. Филимонов [6] В. Н. Бурков и др. [7] И. И. Мазур и др. [8]
4. Условие или неопределенное событие, которое в случае наступления оказывает влияние на цели проекта (содержание, длительность, стоимость, качество)	Свод знаний управления проектами (версии 4, 5 и 6) (Project Management Body of Knowledge – PMBOK® Guide) [9–11]
5. Угроза или возможность	П. Сангхира [12]
6. Событие, которое одновременно несет угрозу, опасность, неопределенность и возможность	PricewaterhouseCoopers (PwC) [13]
7. Вероятность недополучения доходов и/или вероятность возникновения убытков	П. Г. Грабовый и др. [14]
8. Мера опасности	Е. И. Шохин [15]
9. Совокупность значений возможного ущерба	В. Ю. Королев и др. [16]
10. Возможность получения убытков от предпринимательской деятельности	ГК РФ (ст. 926 ГК РФ, ст. 933 ГК РФ) [17]
11. Действия, сделанные наудачу	В. Даль [18]

Содержание понятия «риск»	Источник
12. Неопределенное событие или совокупность неопределенных событий	Свод знаний управления рисками (Management of Risk: Guidance for Practitioners – M_o_R®) [19]
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®) [20]
14. Искусственная экономическая категория, совокупно отражающая меру реальности нежелательного отклонения от цели хозяйственной деятельности предприятия и размер обусловленного этим отклонением ущерба	Р. М. Качалов [21]
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) [13]
16. Вероятный неблагоприятный исход для субъекта	А. Г. Мадера [22, 23]

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

Современные позиции толкования понятия «риск» закреплены в отечественных и международных стандартах. В частности, в отечественном стандарте ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» риск характеризуется как влияние неопределенности на запланированные цели [2, 3], его структура представлена на рисунке 1.1.

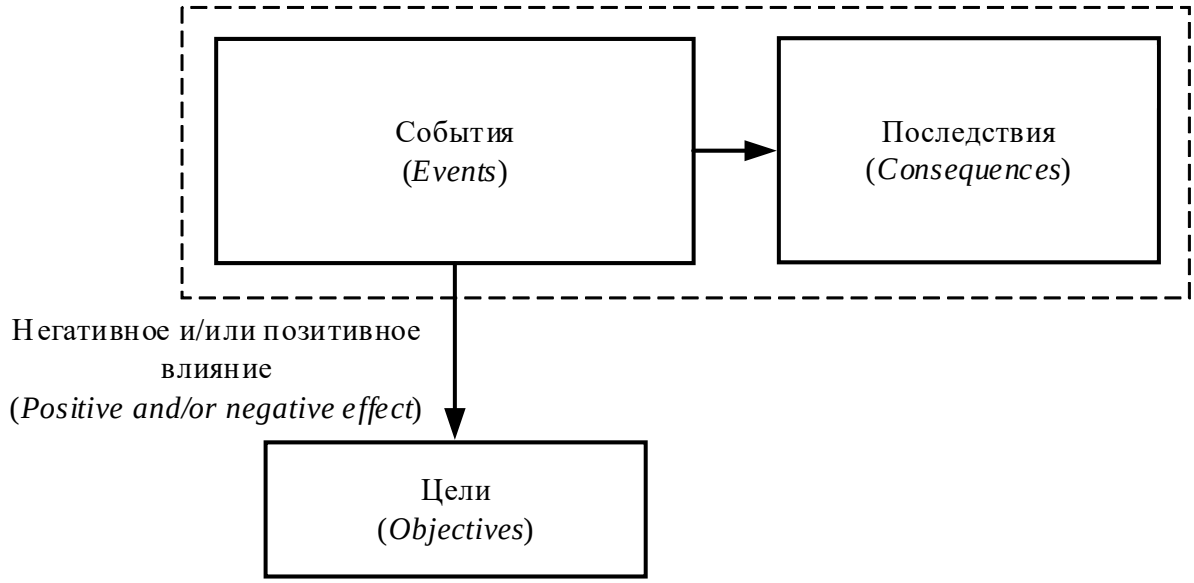


Рис. 1.1 – Структура риска согласно ГОСТ Р ИСО 31000-2010

В своде знаний управления проектами Project Management Body of Knowledge (PMBoK® Guide) 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 [9–11] (рис. 1.2).

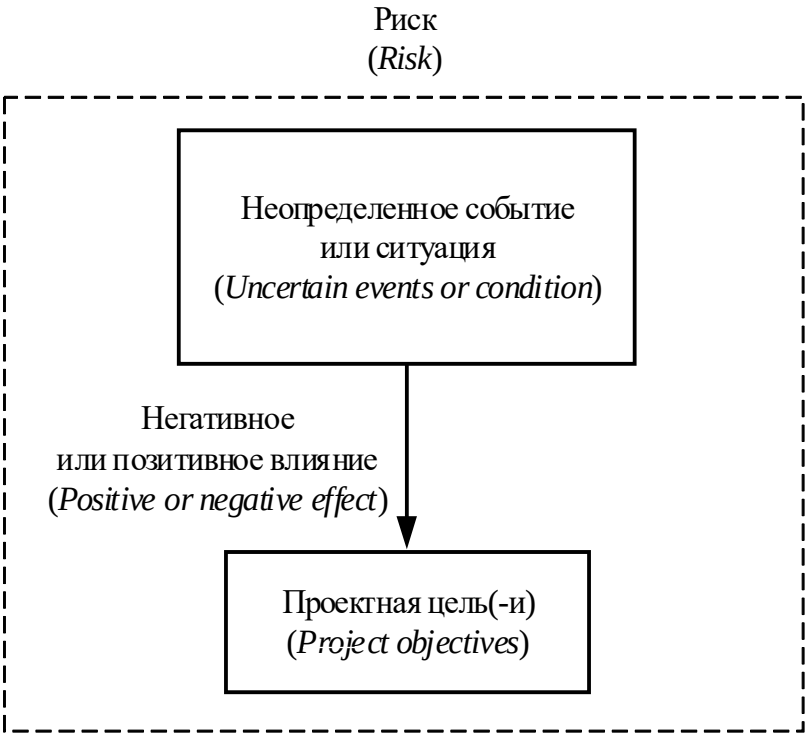


Рис. 1.2 – Структура риска согласно PMBOK® Guide

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 [13]. Структура риска, согласно своду правил COSO ERM, представлена на рисунке 1.3.

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 (рис. 1.4) [19].

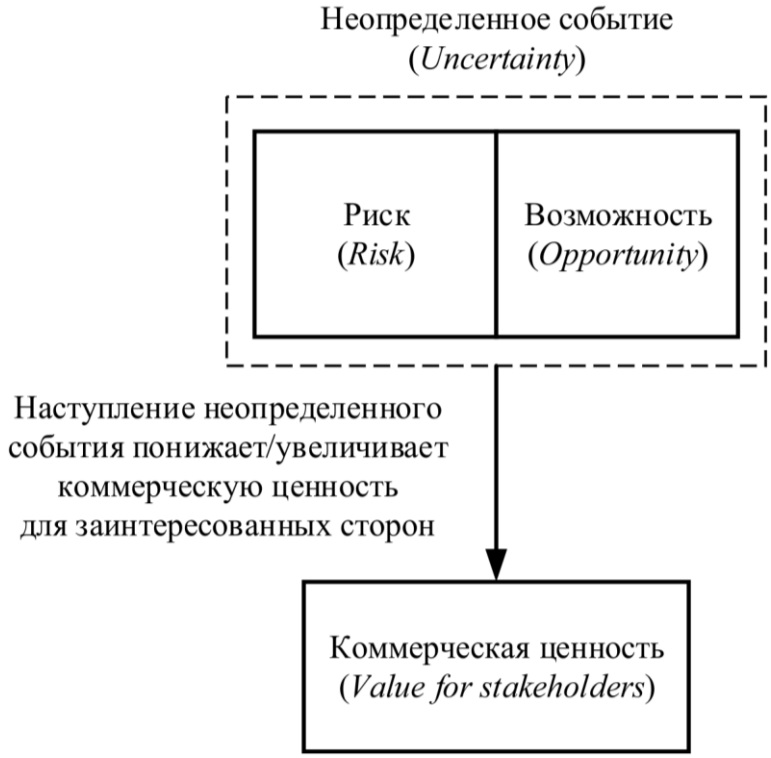


Рис. 1.3 – Структура риска согласно COSO ERM

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 (рис. 1.5) [20].

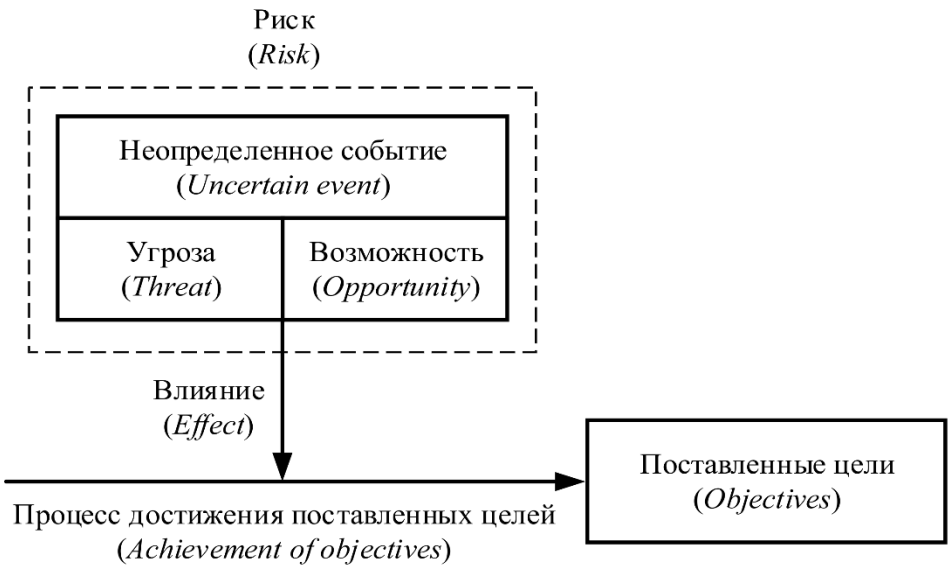


Рис. 1.4 – Структура риска согласно M_o_R®

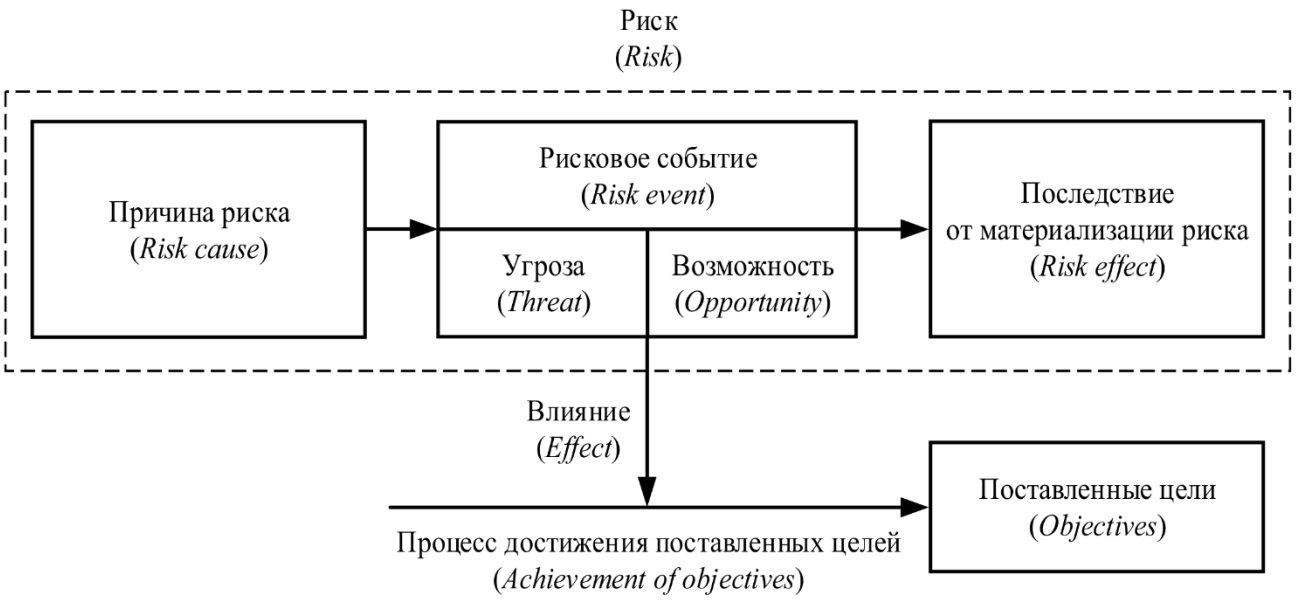


Рис. 1.5 – Структура риска согласно PRINCE2®

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

1. Неопределенность возникает, когда нет необходимой и достоверной информации. Риск же, напротив, базируется на накопленных предшественниками статистических данных, поэтому его материализация может быть спрогнозирована.
2. 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.).
3. Источники неопределенности, как правило, неизвестны. Риск же создают конкретные причины и источники, каждый из которых может быть идентифицирован.

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* (*рис. 1.6*).

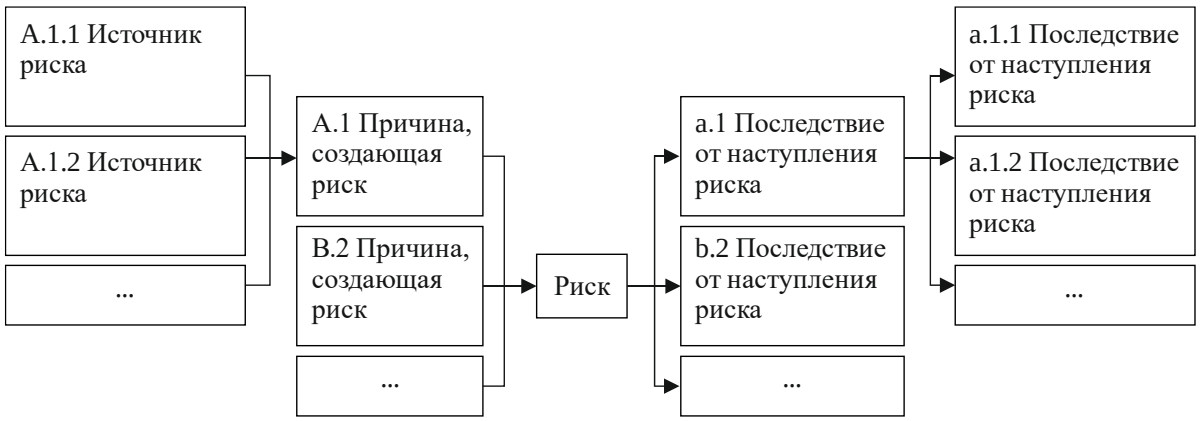


Рис. 1.6. – Структура риска: риск, причины, создающие риск, источники риска и последствия от наступления риска

Причины риска *– условия, имеющие потенциал создавать события, которые способны оказывать влияние на процесс достижения целей.*

Источники риска *– объекты, имеющие потенциал создавать события, способные оказывать влияние на процесс достижения целей.*

Последствия 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.

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, уста-

новлено, 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 (КИИ) 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 материализации рассмотрим рисунок 1.7, где t – это длительность проекта. В случае материализации негативного риска происходит увеличение длительности проекта на величину $t_{\text{негативный риск}}$, т. к. 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 $t_{\text{позитивный риск}}$.

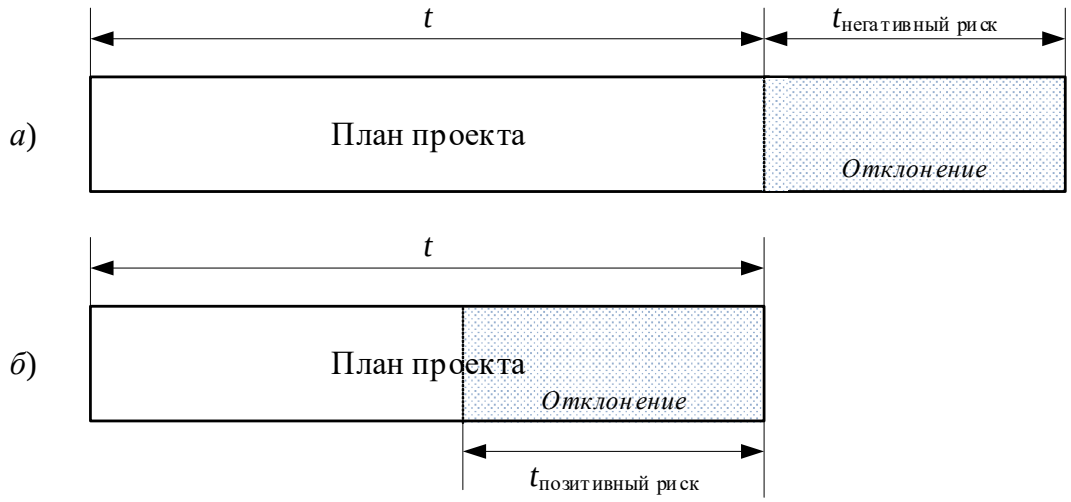


Рис. 1.7 – Влияние наступившего негативного риска (*а*) и позитивного риска (*б*) на план проекта, где t – длительность проекта

Влияние материализовавшихся негативного и позитивного рисков можно охарактеризовать формулами (1.1) и (1.2):

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

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

где $\mathrm{Im}_{negative}$ – 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.

Пример

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 пусконаладочные 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 $4 200 [24].

Далее рассмотрим значение понятия «управление рисками» (*risk management*).

Управление рисками *– это совокупность принципов, скоординированных действий и процессов по оценке, воздействию, мониторингу и контролю рисков* [2, 3] (*рис. 1.8*).

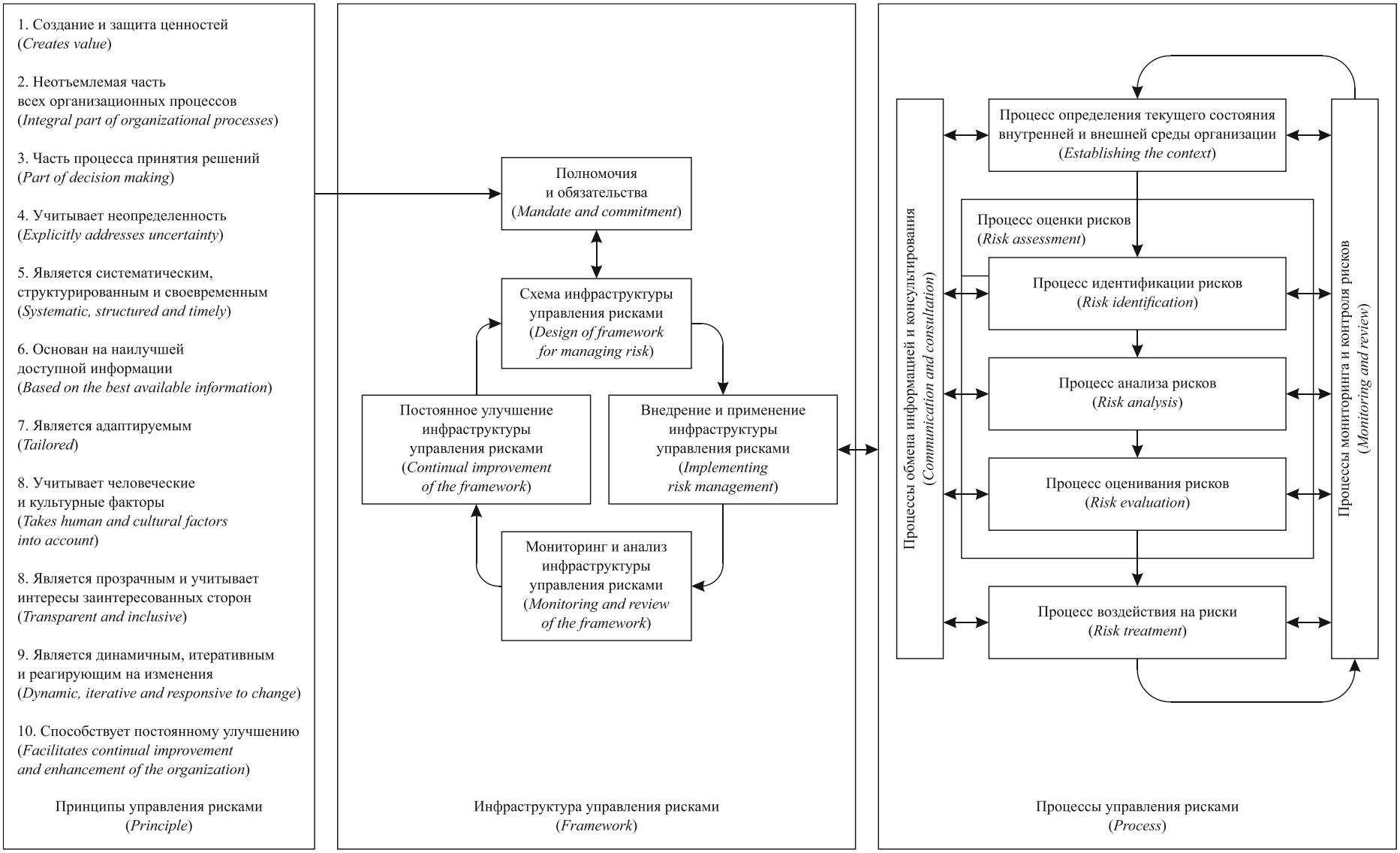


Рис. 1.8 – Взаимосвязь между принципами, инфраструктурой и процессами управления рисками согласно ГОСТ Р ИСО 31000-2010

Нужно отметить, что отечественный стандарт 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, на такие ценности 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* (*integral part of organizational processes*). Риск-менеджмент – это часть обязанностей руководства и неотъемлемая составляющая всех организационных процессов, 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*). Процессы управления рисками должны быть направлены 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 стандарту ГОСТ Р ИСО 31000-2010 для реализации перечисленных принципов в инфраструктуру управления рисками необходимо включить пять элементов:

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 управления рисками организации возможно 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*), в процессе которого руководство должно определить стратегию, сроки и ресурсы, необходимые для внедрения, а также провести

[1]KPI (*Key Performance Indicator*, ключевой показатель эффективности) – это измеримая величина, которая позволяет видеть, насколько продуктивно работники достигают поставленных целей, которые имеют ценность для организации.

обучающие сессии для среднего менеджмента и остальных работников. Применение инфраструктуры управления рисками предусматривает внедрение 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 в отношении улучшения инфраструктуры управления рисками.

Процессы управления рисками

Управление рисками согласно ГОСТ Р ИСО 31000-2010 включает семь процессов:

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. *Идентификация 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 analysis*): 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.

Подробнее процессы управления рисками рассмотрены в следующих разделах учебного пособия.

1.2 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.

В зависимости от причин возникновения выделяют:

1. *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.

2. *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.

3. *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.

4. *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.

5. *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 можно привести наиболее опасные хакерские атаки, которые произошли в 2021 г., в частности:

1. 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 [25].

2. 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 [26].

3. Масштабная компьютерная атака на информационные сети МВД Бельгии (26 мая 2021 г.) [27].

4. 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 [28].

5. Хакерская атака на американскую сеть «McDonald’s» (12 июня 2021 г.), в ходе которой были похищены данные клиентов ее ресторанов в Южной Корее и на Тайване [29].

6. Хакерская атака на районные компьютерные сети округа Анхальт-Биттерфельд (Германия) (11 июля 2021 г.), повлекшая введение властями округа 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 [30].

По масштабу воздействия выделяются:

1. *Макрориски* – 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 из самых глубоких падений ВВП (–7,8% в 2009 г.).

2. *Мезориски* – риски, последствия от наступления которых влияют на определенный регион или отрасль экономики.

3. *Микрориски* (*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 [31].

По функциональной области организации различают:

1. *Внутренние и внешние риски*. Если источники рисков находятся внутри организации, то эти риски называют внутренними рисками, если источники рисков находятся за пределами организации – внешними рисками.

2. *Коммерческие риски* – непредвиденные расходы (доходы), которые могут быть получены во время ведения финансово-хозяйственной деятельности организаций.

3. *Имущественные риски* – вероятность потери имущества по причине пожара, кражи, диверсии, халатности и др.

4. *Производственные риски* – возможный ущерб от остановки производства, гибели или повреждения оборудования, полученного брака продукции и др.

5. *Торговые риски* – возможные убытки из-за задержки или отказа от оплаты товара, непоставки товара, потери имущества во время транспортировки и др.

6. *Транспортные риски* – вероятность повреждения или потери товара во время перевозки автомобильным, морским, речным, железнодорожным и/или воздушным транспортом.

7. *Финансовые риски* – вероятность получения убытков (прибыли).

8. *Инвестиционные риски* – вероятность неполучения (получения) ожидаемого коммерческого эффекта. При рассмотрении инвестиционных рисков в негативном ключе выявляются следующие их подвиды:

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

2) *риски снижения доходности*, возникающие в результате снижения размера дивидендов по портфельным инвестициям и/или вкладам;
3) *риски прямых финансовых потерь*;
4) *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.

9. *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 проявляются в форме юридических санкций со стороны регулирующих и надзорных органов, отраслевых ассоциаций, а также лиц, права и интересы которых были нарушены.

10. *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.

Риски, **связанные с покупательной способностью денег**:

- *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.

Риски **по степени контролируемости**:

- неконтролируемые;
- частично контролируемые;
- контролируемые.

В зависимости от наступивших последствий риски могут быть:

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

По характеру последствий наступления рисковых событий 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.

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.

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.

Контрольные вопросы по главе 1

1. Чем различаются понятия «неопределенность» и «риск»?
2. Назовите и охарактеризуйте основные принципы управления рисками согласно ГОСТ Р ИСО 31000.
3. Перечислите основные элементы инфраструктуры управления рисками согласно ГОСТ Р ИСО 31000. Каковы их функции?
4. Перечислите и охарактеризуйте процессы управления рисками согласно ГОСТ Р ИСО 31000.
5. На какие классификационные группы распределяются риски?

2 Процессы управления рисками

2.1 Идентификация рисков

Одним из наиболее кропотливых процессов управления рисками считается идентификация рисков. По мнению В. О. Ключникова, сложность выявления рисков вызвана уникальностью бизнес-процессов [32–34]. Ученый в своих трудах отмечает, что время, затраченное на выявление рисков, представляет собой инвестицию в успех, т. к. 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**	
Retrospective	Ретроспективный анализ документов	В. А. Никонов [35]
Brainstorming	Мозговой штурм	А. Осборн [36]
Delphi	Метод «Дельфи»	О. Хелмер [36]
SWOT matrix	SWOT-анализ	К. Эндрюс [36]
STEEP matrix (PEST matrix)	STEEP-анализ / PEST-анализ	М. Портер [36]
Hazard and Operability Study (HAZOP)/Control Hazards and Operability Analysis или Computer Hazard and Operability Analysis (CHAZOP)	Исследование компьютерной опасности и работоспособности систем	Т. Клетз [37]
Structured What-If Technique (SWIFT)	Структурированный анализ сценариев методом «Что, если?»	Ф. Лавли [38]
Preliminary Hazard Analysis (PHA)	Предварительный анализ опасностей для систем	Э. Дж. Хенкли, Х. Кумамото [36]

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 А.

Метод «Мозговой штурм» (*Brainstorming*) является коллективным и творческим. Основные преимущества метода – выявление специальных рисков, легкость применения, а также коллаборация участников (рис. 2.1). В числе недостатков можно отметить низкое качество процесса идентификации рисков.

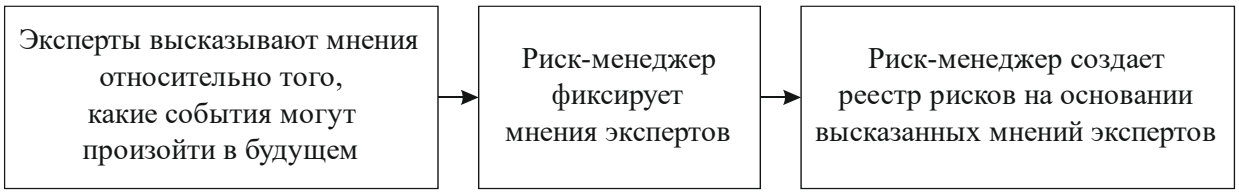


Рис. 2.1 – Идентификация рисков с помощью метода «Мозговой штурм»

Метод «Дельфи» (Delphi), созданный в 1960-е гг. 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 (рис. 2.2).

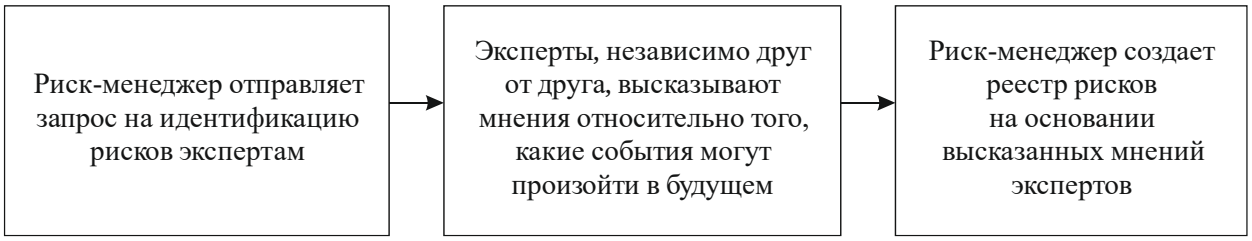


Рис. 2.2 – Идентификация рисков с помощью метода «Дельфи»

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). Т. Клетз при разработке HAZOP в первую очередь стремился избежать промышленных инцидентов, таких как пожары, выбросы вредных веществ и утечки химикатов. Со временем метод доказал свою работоспособность, и в 1974 г. HAZOP вошел в состав обязательных методов, применяемых для идентификации рисков. Позднее он был адаптирован и для разработки программ для ЭВМ, получив название «Computer Hazard and

Operability Analysis (CHAZOP)». 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**
Отрицательный	НЕТ	НЕТ информации, которая необходима для реализации ИТ-продукта
Количественные изменения	БОЛЬШЕ	Источников, в которых хранится актуальная информация о проекте, БОЛЬШЕ, чем необходимо
	МЕНЬШЕ	Сотрудников в проекте МЕНЬШЕ, чем необходимо
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
Замена	ПЕРЕМЕНА	В процессе реализации ожидается ПЕРЕМЕНА запланированных требований
	ДРУГОЙ	Проектом будет управлять ДРУГОЙ руководитель
Время	РАНО	Реализация проекта будет начата слишком РАНО
	ПОЗДНО	Реализация проекта будет начата слишком ПОЗДНО
Порядок или последовательность	ПРЕЖДЕ, ЧЕМ	Заказчик будет знакомиться с разработанным инкрементом программного кода ПРЕЖДЕ, ЧЕМ завершится тестирование
	ПОСЛЕ	Актуальная информация поступит ПОСЛЕ разработанных функций

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.

Главными достоинствами метода SWIFT являются простота использования, т. к. метод не требует предварительной подготовки, а также его графическое исполнение, что стимулирует творческий процесс. Идентификация возможных последствий для риска «На стороне Заказчика будут отсутствовать ключевые и квалифицированные специалисты» с помощью метода SWIFT представлена на рисунке 2.3.

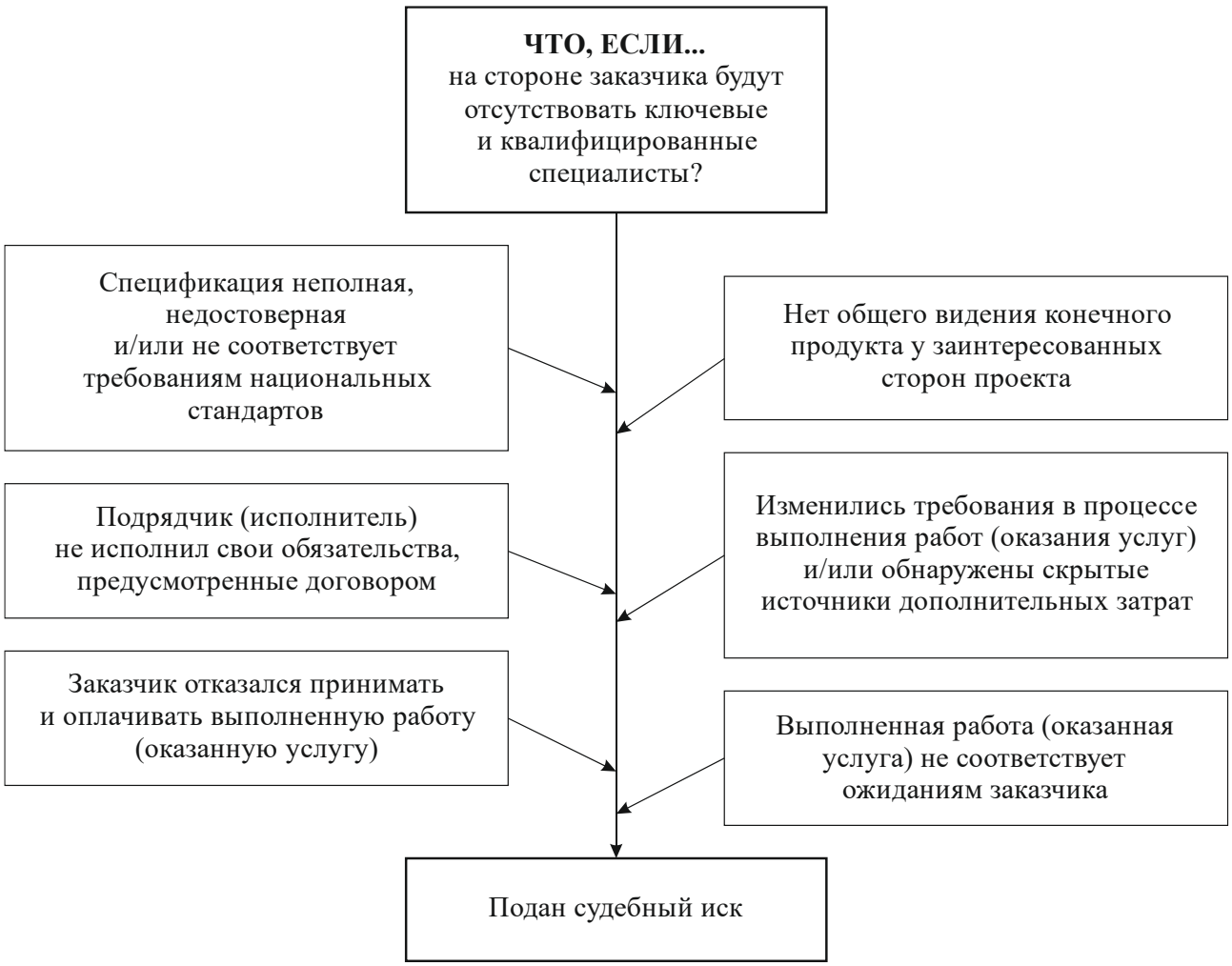


Рис. 2.3 – Идентификация последствий в результате наступления риска с помощью SWIFT

Preliminary Hazard Analysis (PHA). Метод PHA направлен на выявление угроз, которые могут 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.

Метод PHA распределяет риски на три класса:

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, к данным рисками относятся 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 актуальных для организации и/или проекта рисков рекомендуется использовать различные методы и привлекать сторонних экспертов [39–41]. Выявленные риски рекомендуется заносить в раздел «Идентификация» в реестре рисков, при этом следует фиксировать следующую информацию: тип риска; название и описание риска; класс риска; дату идентификации риска.

Пример раздела «Идентификация» в реестре рисков представлен в таблице 2.4.

Таблица 2.4 – Пример раздела «Идентификация» реестра рисков

Тип / Название риска	**Описание риска**	**Класс риска**	**Дата идентификации риска**
Негативный / Риск изменения условий контрактов сотрудников	Профсоюз работников кафетериев может потребовать пересмотра контрактов сотрудников кафетерия, чтобы они отражали новое распределение обязанностей и графиков работы кафетерия	Комплаенс-риск	XX.XX.XXXX
Негативный / Риск того, что выполненная работа (оказанная услуга, поставленный товар) 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	XX.XX.XXXX

Тип / Название риска	Описание риска	Класс риска	Дата идентификации риска
Негативный / Риск того, что партнеры откажутся от сотрудничества	Близлежащие рестораны могут не согласиться предоставить скидки, что уменьшит удовлетворенность работников программой для ЭВМ	Коммерческий риск	ХХ.ХХ.ХХХХ
Негативный / Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям 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

2.2 Анализ рисков

Процесс анализа рисков направлен на установление источников рисков, причин, создающих риски, и возможных последствий в случае их наступления. Согласно ГОСТ Р 31010-2011 «Методы оценки риска» оптимальными методами для проведения анализа считаются «Галстук-бабочка» (первый этап) и «Почему-почему» (табл. 2.5) [42, 43].

Таблица 2.5 – Методы, применяемые для анализа рисков

Название метода		Разработчики
Оригинал (англ.)	**В переводе на русский**	
Bow-tie	«Галстук-бабочка» (первый этап)	Б. Лангминд [42]
5Why	«Почему-почему»	С. Тоеда [43]

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 2.4.

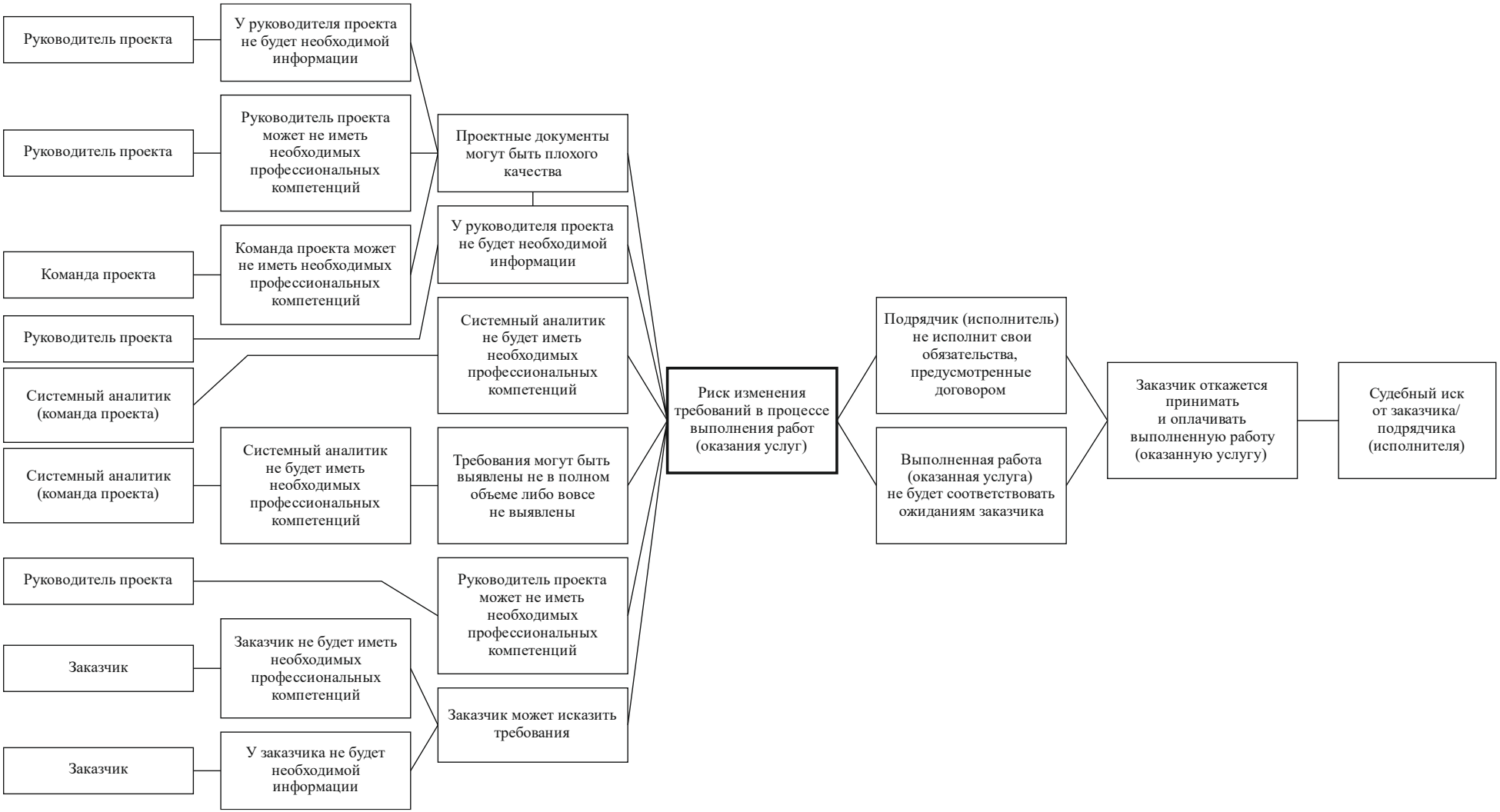


Рис. 2.4 – Анализ риска с помощью Bow-tie (первый этап)

Метод «Почему-почему» (*5Why, «Пять "почему"»*) был предложен Сакити Тоёда 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.

Таблица 2.6 – Анализ риска с помощью метода «Почему-почему»

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 методом «Почему-почему» позволил установить, что источниками рисков являются заинтересованные стороны проекта (рис. 2.5), а именно пользователь, заказчик, руководитель проекта, команда проекта, субподрядчик и конкурент.

Рис. 2.5 – 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**
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
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

Тип риска / Название риска	Причины, создающие риск	Источники риска	Последствия от наступления риска
Негативный / Риск того, что партнеры откажутся от сотрудничества	Партнерам будет невыгодно предоставлять скидки	Партнеры	Уменьшение удовлетворенности работников программой для ЭВМ
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

2.3 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 бóльший 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 [44]:

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 (2.1):

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

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;
- стоимость под риском (*Value-at-Risk,* VaR).

Качественные методы *– это методы, в которых используются экспертные мнения для оценивания характеристик вероятностей и влияний рисков.*

Качественные методы, как правило, 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. [45]**	
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

Таблица 2.9 – Коэффициенты оценивания возможного влияния в случае наступления риска

Влияние риска в случае наступления	**Коэффициент Харрингтона**		**Комментарии**
	PMBOK® Guide	**Merna T. и Al-Thani F. [45]**	
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 вероятности	0,0–0,1	0	Материальный ущерб отсутствует

Для увеличения точности рекомендуется получение трех видов экспертных оценок:

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

Полученные оценки необходимы для применения формул (2.2) и (2.3) расчета вероятности и влияния PERT (*Project Evaluation and Review Technique*):

$$A_{ij} = \frac{a_i^o + 4a_i^r + a_i^p}{6}, \tag{2.2}$$

$$B_{ij} = \frac{b_i^o + 4b_i^r + b_i^p}{6}, \tag{2.3}$$

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-риска по мнению j-эксперта; B_{ij} – расчетное значение возможного влияния в случае наступления i-риска по мнению j-эксперта; i – номер риска; j – номер эксперта.

Далее для каждого риска рассчитывается среднее арифметическое значение вероятности материализации риска и возможного влияния в случае его наступления по формулам (2.4) и (2.5):

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

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

где n – количество экспертных мнений.

Для визуализации полученных оценок используется специальный инструмент – *матрица рисков*. Пример матрицы рисков, который применяется Министерством обороны США (*The Department of Defense United States of America* – DoD), представлен на рисунке 2.6 [46].

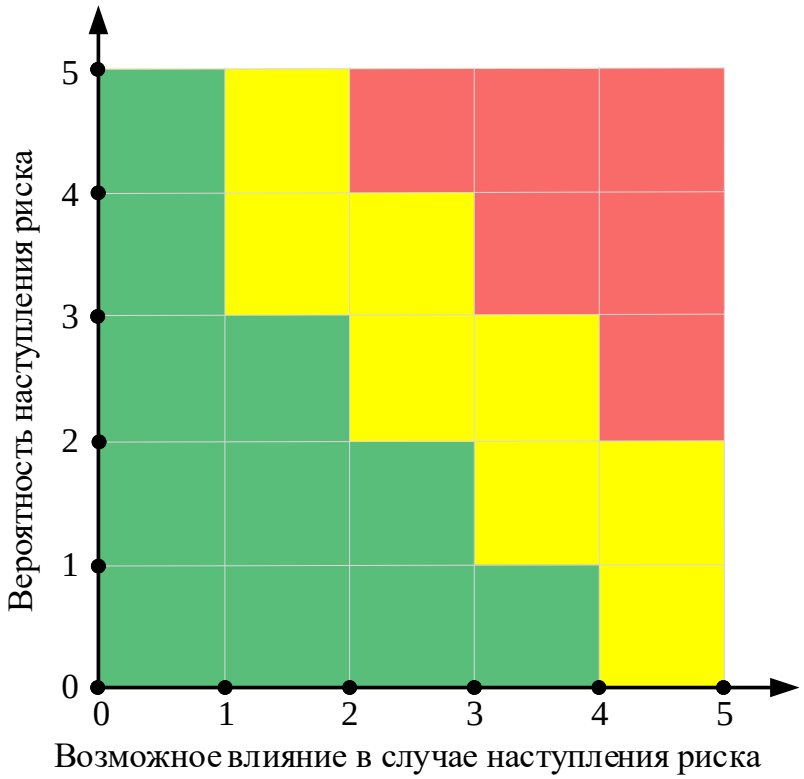


Рис. 2.6 – Матрица рисков Министерства обороны США

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.

T. Merna и F. Al-Thani предлагают распределять негативные риски на четыре группы [45]:

1. **Катастрофические риски, или «тигры»** (*tiger*) – это негативные риски, которые имеют высокую вероятность материализации и способны оказать значительное негативное влияние в случае их наступления. По мнению T. Merna и F. Al-Thani, материализация одного «тигра», например, «Проект покинул руководитель проекта», способна привести к полной остановке работ (оказания услуг, поставки товаров).
2. **Непредсказуемые риски, или «аллигаторы»** (*alligator*) – это 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, ст. 15.33.2 КоАП РФ) [47] и др.
3. **Часто встречаемые риски, или «щеночки»** (*puppy*) – это негативные риски, которые имеют высокую вероятность материализации, но при этом не способны оказывать какого-либо значительного влияния. 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 обладают способностью оказывать какое-либо значительное влияние. По мнению T. Merna и F. Al-Thani, «котята» не способны хоть как-то навредить проекту, поэтому данными негативными рисками можно пренебречь [45].

Матрица вероятности и влияния T. Merna и F. Al-Thani представлена на рисунке 2.7.

Отдельно следует выделить группу маловероятных, но очень опасных рисков, таких как промышленные катастрофы, потрясения, природные катаклизмы, пандемии и эпидемии. Н. Н. Талеб называет подобные риски «*черные лебеди*» [48].

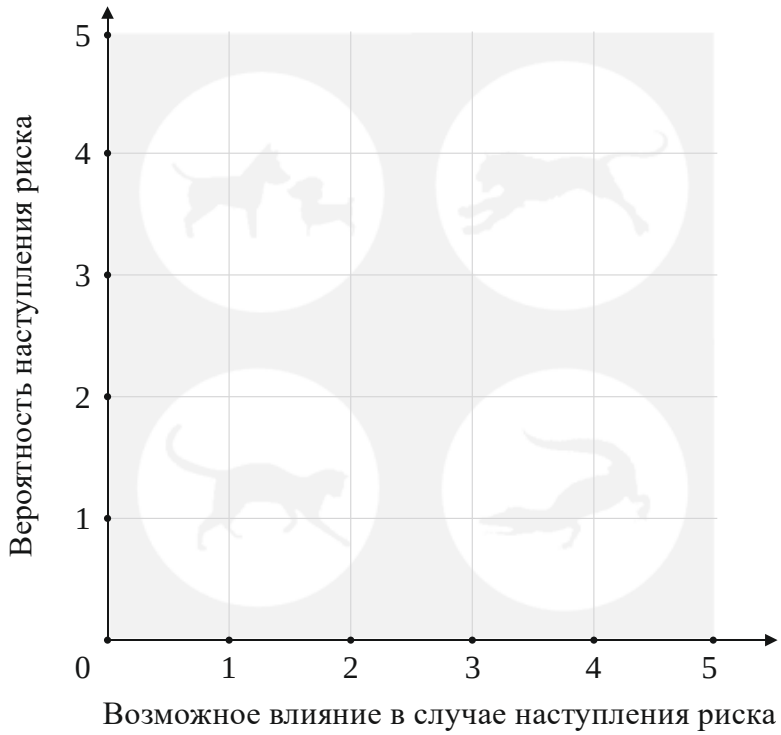


Рис. 2.7 – Матрица негативных рисков Т. Мерна и Ф. Ал-Хани

Позитивные риски автор настоящего пособия рекомендует распределять на четыре группы [49]:

1. *Созидательные риски, или «слоны»* – это 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»* – это 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 заблаговременно будут приняты стимулирующие меры, то в проект могут быть привлечены ведущие программисты, что позитивно повлияет на процесс достижения целей.
3. *Часто встречаемые риски, или «обезьяны»* – это позитивные риски, имеющие высокую вероятность материализации, но не способные оказывать значительное влияние. Отделение данных позитивных рисков от остальных имеет большую практическую ценность, т. к., «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»* – это 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 2.8 [49].

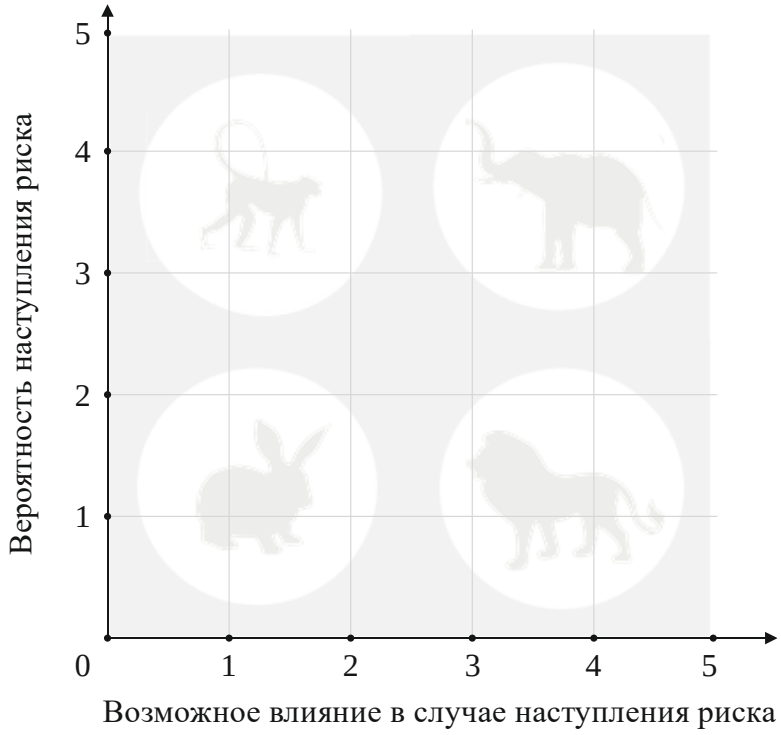


Рис. 2.8 – Матрица позитивных рисков

Рассмотрим примеры позитивных рисков в проектах.

Риск того, что численность участников проекта будет менее шести человек. В аналитических докладах The CHAOS Manifesto приводятся статистические данные, которые показывают, что проекты, в состав которых входило менее шести участников, были гораздо успешнее, чем проекты, в которых принимало участие более шести человек (табл. 2.10) [50].

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 до 70% [51].

Риск привлечения в проект руководителя проекта, имеющего профессиональное образование в области управления проектами (*опыт управления проектами более двух лет*). В аналитических отчетах The CHAOS Manifesto утверждается, что на успешное завершение проекта значительно влияют профессиональные и личные качества руководителя проекта. В частности, если он имеет профессиональное образование в области управления проектами, то проекты выполняются согласно общепринятым нормам, что нивелирует значительную часть негативных рисков. Кроме того, результаты исследования В. А. Гаги, С. А. Козловой, А. П. Тютюшева и Е. Н. Ярославцевой показали, что на эффективность и результативность рабочих групп значительно влияет эмоциональный интеллект руководителя [52]. Например, его негативные эмоции быстро передаются участникам проекта, что отражается на их координации, мотивации и энтузиазме.

Риск декомпозиции большого проекта на малые проекты (*длительностью не более четырех 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 (700–2 500 чел.-ч.) – 14%, долгосрочных ИТ-проектов (более 2 500 чел.-ч.) – 10% [51].

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* – мера того, насколько быстро риск станет оказывать влияние на одну или несколько стратегических, тактических, операционных или проектных целей;
- *выявляемость* – способность обнаружить 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**
Негативный / Риск изменения условий контрактов сотрудников	0,6	3	Зеленая
Негативный / Риск того, что выполненная работа (оказанная услуга) не принесет ожидаемого коммерческого эффекта	0,3	9	Желтая
Негативный / Риск того, что партнеры откажутся от сотрудничества	0,3	3	Зеленая
Негативный / Риск того, что выполненная работа (оказанная услуга) не будет соответствовать ожиданиям конечного пользователя	0,5	6	Желтая

2.4 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 производстве фильмов. Например, в картине 1994 г. «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 (например, трудовых, материальных резервов, резервов на покрытие инфляции, средств на возможные потери и др.) [9–11]. На рисунке 2.9 представлена структура бюджета проекта с учетом управленческих резервов и резервов на возможные потери.

Отдельно стоит отметить управленческий резерв, который, как правило, не входит в базовый план по стоимости.

Рис. 2.9 – Структура бюджета проекта с учетом управленческих резервов и резервов на возможные потери согласно PMBOK® Guide

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 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 – Стратегии 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

Тип риска	Стратегия воздействия	Описание стратегии воздействия
	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
	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 И. Селиховкина, самой результативной стратегией воздействия на негативные риски является *стратегия нивелирования*, суть которой заключается в ликвидации источников рисков [53]. 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.

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

№	Название	Название (перевод на русский)	Разработчики
1	Retrospective	Ретроспективный анализ документов	В. А. Никонов [35], А. А. Поляков и В. О. Ключников [54, 55]
2	Delphi	Метод «Дельфи»	О. Хелмер, Н. Далки и Н. Ресчер [36]
3	Brainstorming	Метод «Мозговой штурм»	А. Осборн [36]

№	Название	Название (перевод на русский)	Разработчики
4	Bow-tie	Метод «Галстук-бабочка» (2-й этап)	Б. Лангминд [42]
5	Method of Walt Disney	Метод Уолта Диснея	У. Дисней [36]

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.

Метод «Дельфи» (*Delphi*). 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» (рис. 2.10).

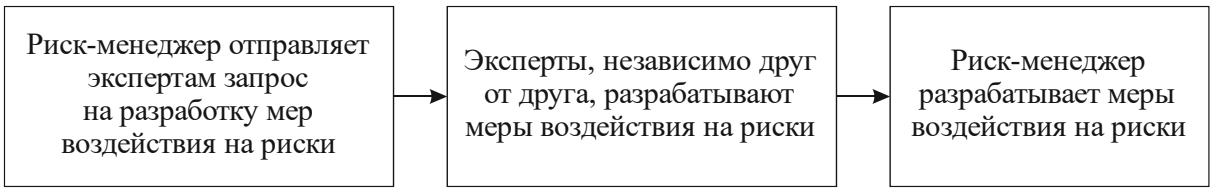


Рис. 2.10 – Разработка мер воздействия на риски с помощью метода «Дельфи»

Метод «Мозговой штурм» (*Brainstorming*). Результативно себя проявляет метод «Мозгового штурма» при работе в малых группах до шести человек (рис. 2.11). Творческая свобода и отсутствие критики дает возможность экспертам создать большое количество разнообразных мер воздействия не только для специальных рисков, но и пересмотреть механизм воздействия для универсальных рисков.

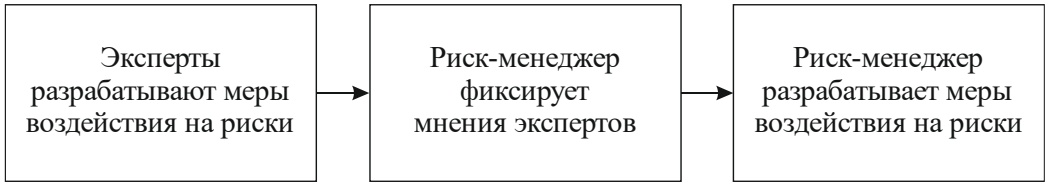


Рис. 2.11 – Разработка мер воздействия на риски
с помощью метода «Мозговой штурм»

Метод «Галстук-бабочка» (*Bow-tie*). Как уже отмечалось ранее, на втором этапе метода «Галстук-бабочка» разрабатываются «барьеры», которые направлены 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 «фантазера», «критика» и «реалиста». «Фантазер» отвечает за поиск творческих идей, включая фантастические и волшебные, «критик» ищет слабые места в предложенных мерах, а «реалист» оценивает достижимость и целесообразность разработанных мер воздействия на риски.

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

***Триггерными условиями* (*триггерами*)** *в управлении рисками называют 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*. Данный документ включает в себя следующую информацию:

- тип риска;
- название риска;
- стратегия воздействия;
- меры превентивного воздействия;
- владелец риска. Указывается конкретное лицо (группа лиц), которое будет управлять риском;
- триггерные условия;
- меры принятия рисков.

Пример плана управления рисками представлен в таблице 2.14.

Таблица 2.14 – Пример плана управления рисками

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

Контрольные вопросы по главе 2

1. Назовите и охарактеризуйте методы, которые используются для идентификации рисков.
2. Назовите и охарактеризуйте методы, которые используются для анализа рисков.
3. Чем отличаются количественные и качественные методы оценки рисков?
4. Опишите механизм качественной оценки рисков с использованием коэффициентов вербально-числовой шкалы Харрингтона.
5. Перечислите и охарактеризуйте стратегии управления рисками.

3 Риск-менеджмент в системе публичного управления

3.1 Ковенанты договора, элиминирующие комплаенс-риски

Несмотря на устоявшуюся деловую практику и закрепленные нормы права, регулирующие ход реализации проектов, необходимо отметить, что не все участники обладают достаточной управленческой зрелостью, и это 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.

T. Merna и F. Al-Thani отмечают, что наступление комплаенс-рисков достаточно редкое явление, однако материализация одного подобного риска является достаточным условием для причинения существенного материального ущерба [45]. Например, в рамках судебного разбирательства по делу № А81-9472/2019 томская ИТ-организация проиграла спор на общую сумму, равную 1 744 615,65 руб. [56]; по делу № А67-1623/2017 – 2 850 107,39 руб. [57]; по делу № А40-248300/21-5-1672 – 2 000 000,00 руб. [58]; по делу № А40-32033/19-47-287 – 15 830 400,00 руб. [59] и др.

В настоящем разделе рассмотрим способы элиминирования универсальных комплаенс-рисков.

Риск того, что выполненная работа (*оказанная услуга, поставленный товар*) *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 [57].

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, поставки товара). В силу ст. 708 ГК РФ цена в тексте договора может быть твердой (*Fixed Price*) либо приблизительной (Time & Materials / T&M) [17].

Риск того, что заказчик откажется принимать выполненную работу (*оказанную услугу*, *поставленный товар*). Для уменьшения вероятности наступления комплаенс-риска рекомендуется в тексте договора зафиксировать процедуру сдачи-приемки результата выполненных работ (оказанных услуг, поставленного товара). Например, в договоре могут быть зафиксированы следующие условия: «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) [17].

В случае отсутствия обоснованных претензий и замечаний заказчик после сдачи выполненной работы (оказанной услуги, поставленного товара) сообщает об этом обратным электронным письмом подрядчику, указывая в теме письма, что программа для ЭВМ принята.

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 десяти рабочих дней со дня получения мотивированного отказа безвозмездно устранить претензии и замечания. 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 двух рабочих дней программа для ЭВМ считается принятой заказчиком без претензий на третий 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*, *поставленного товара*). Согласно ст. 702 ГК РФ заказчик обязуется принять результат выполненных работ и оплатить его [17]. Следова-

тельно, 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 двух рабочих дней с даты принятия заказчиком результата работ направить заказчику оригинал подписанного со своей стороны акта сдачи-приемки работ в двух экземплярах;
2) заказчик обязан в течение пяти 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 шестой рабочий день с даты получения заказчиком оригинала акта сдачи-приемки работ.

Риск того, что будет просрочка оплаты за выполненную подрядчиком работу (*оказанную исполнителем услугу*, *поставленного поставщиком товара*). 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 пять 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, т. е. 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 можно рассмотреть договор об отчуждении исключительного права на программу для ЭВМ, который согласно п. 2 ст. 1234 ГК РФ должен быть заключен в письменной форме [17]. В случае несоблюдения этого условия сделка считается незаключенной, а исключительное право – не переданным от правообладателя к правоприобретателю. Последствия от нарушения данного условия наглядно представлены в деле № А40-81328/2011 [60], 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 [17]. 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 комплаенс-риск можно при повышении уровня зрелости в части управления коммуникациями проекта, т. к. 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 [17].

Риск отсутствия связи с заказчиком. Для нивелирования данного комплаенс-риска рекомендуется в текст договора включить следующее условие: «Длительный простой трудовых ресурсов подрядчика, превышающий пять рабочих дней, оплачивается заказчиком по тарифу простоя трудовых ресурсов подрядчика. Тариф простоя трудовых ресурсов определяется по согласованию сторон».

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. будут выявлены новые и/или произведено существенное уточнение ранее согласованных требований*. В качестве примера можно рассмотреть дело № А55-9384/2018 [61], 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 того, какой методический инструментарий использует подрядчик 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, т. к. 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 [17]. 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 себя элементы, которые своевременно создают, собирают, распространяют, хранят, получают и используют информацию.

Риск того, что будет реструктуризация заказчика, т. е. на стороне заказчика будут проведены изменения его 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, 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 подрядчик (*исполнитель, поставщик*) *не исполнит свои обязательства, предусмотренные договором* (*например, невыполнение заявленных требований в срок либо невыполнение в полном объеме и др*.). Для увеличе-

ния 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 [17].

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 грозят годности результата выполненных работ либо создают невозможность завершения работ в срок [17]. 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*. Согласно ст. 706 ГК РФ, если сделка требует от подрядчика выполнить работу лично, то подрядчик вправе привлечь к исполнению своих обязательств других лиц (субподрядчиков) [17].

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 [17].

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 [17].

Административным законом предусмотрена ответственность за оскорбление, т. е. унижение чести и достоинства, выраженное в неприличной форме (ст. 5.61 КоАП РФ) [47]. Совершение указанного 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 [62].

Риск нарушения исключительных прав на результат интеллектуальной деятельности. Для увеличения лояльности заказчика и уменьшения вероятности материализации комплаенс-риска в тексте договора рекомендуется 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 со-

зданной им программе исчез знак охраны авторского права «©», что стало основанием для обращения в суд [63]. 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, в частности, договором отчуждения исключительного права, договором 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 можно рассмотреть материалы дела № А40-202764/18-110-1552 [64], 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) [65], в котором правообладатель программы «Аптека-Урал» обратился в суд с требованием запретить правообладателю программы «Quartfarm» распространение и использование каким-либо иным способом его программного продукта. 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 [66], 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, договором отчуждения исключительного права, договором передачи исключительного права на основании лицензии, договором 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 [17]. Следовательно, исключительные права на результат интеллектуальной деятельности станут принадлежать субъекту, который будет перерабатывать (модифицировать) 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, реассамблирование, 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. Уменьшение вероятности материализации данного комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в проекте [17].

Риск того, что полученный субподрядчиком результат (*оказанная услуга*, *поставленный товар*) *не будет 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 [17]).

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 [17]).

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* [67].

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 тексте договора 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 трех 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, поставки товара*). 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 возможно 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.

3.2 Оценка угроз национальной безопасности Российской Федерации

Усиливающаяся нестабильность в мире, рост радикальных и экстремистских настроений стимулируют нарастание геополитический напряженности, направленной против России и ее граждан. Яркими примерами являются диверсия на «Северных потоках», террористические акты на территории России, введение потолка цен на сырую нефть и нефтепродукты, запрет на импорт товаров, экспортные ограничения, дискриминация отечественных компаний на мировом рынке, конфискация имущества граждан России в странах Европы и др. Эти и другие подобные им события формируют необходимость повышения внутренней стабильности и устойчивости России, наращивания ее экономического, политического, военного и духовного потенциала [68–74].

Ответом на возрастающую нестабильность и агрессию со стороны недружественных стран является реализация государственной политики в области обеспечения национальной безопасности в части укрепления обороны страны, государственной, общественной, информационной, экономической, экологической и международной безопасности, научно-технического развития, защиты традиционных российских духовно-нравственных ценностей, культуры и исторической памяти. Базовым документом, который закрепляет ключевые позиции данной политики, является Указ Президента Российской Федерации от 02.07.2021 «О Стратегии национальной безопасности Российской Федерации» (далее – Стратегия национальной безопасности), где под *угрозой национальной безопасности* понимается совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба *национальным интересам России*.

Проведенный анализ Конституции РФ (далее – Конституция), Федерального закона от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Россий-

ской Федерации» (далее – Закон 172-ФЗ), Федерального закона «О безопасности» от 28.12.2010 № 390-ФЗ (далее – Закон 390-ФЗ), Стратегии национальной безопасности, Военной доктрины РФ, Доктрины информационной безопасности РФ (далее – Информационная доктрина), Стратегии экономической безопасности России до 2030 г. (далее – Стратегия экономической безопасности), Стратегии научно-технологического развития, Стратегии экологической безопасности РФ на период до 2025 г. (далее – Стратегия экологической безопасности) [75–82] и других доктринальных и стратегических актов показал, что под «*риском*» понимается некая совокупность факторов, которая запускает процесс трансформации вызовов в угрозы, где *вызовы* – это совокупность факторов, которые способны при определенных условиях приводить к возникновению угроз.

Графическое представление связи между вызовами, рисками, угрозами и национальными интересами России представлено на рисунке 3.1.

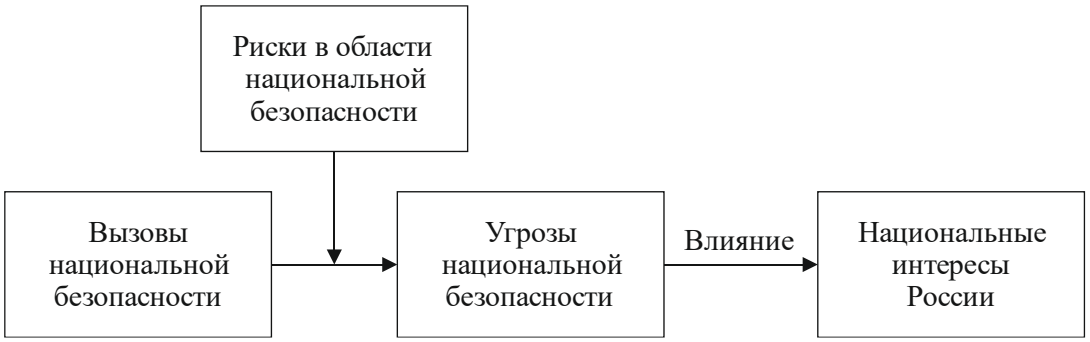


Рис. 3.1 – Связь между вызовами национальной безопасности, рисками в области национальной безопасности, угрозами национальной безопасности и национальными интересами России

В соответствии со ст. 23 Закона 172-ФЗ, стратегический прогноз России должен включать в себя оценку рисков социально-экономического развития и угроз национальной безопасности, оптимальный сценарий преодоления рисков и угроз национальной безопасности, а также поэтапные прогнозные оценки вероятного состояния социально-экономического потенциала и национальной безопасности.

В силу Стратегии национальной безопасности под *национальной безопасностью* понимается состояние защищенности национальных интересов России от внешних и внутренних угроз, при котором обеспечивается реализация конституционных прав и свобод граждан, достойные качество и уровень жизни, гражданский мир и согласие в стране, охрана государственного суверенитета России, ее независимости и государственной целостности, социально-экономическое

развитие страны. Согласно Закону 390-ФЗ *безопасность* – это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.

Согласно Стратегии национальная безопасность включает в себя восемь основных звеньев (рис. 3.2). Рассмотрим их подробнее.

Рис. 3.2 – Структура национальной безопасности России

1. *Экономическая безопасность*. Механизмы обеспечения экономической безопасности закреплены в Стратегии экономической безопасности, утвержденной Президентом РФ 13.05.2017. Важно отметить, что ключевое место в обеспечении экономической безопасности России занимает топливно-энергетический комплекс (далее – ТЭК), т. е. экономическая безопасность включает в себя энергетическую безопасность [83].

2. *Военная безопасность*. Механизмы обеспечения военной безопасности закреплены в Военной доктрине, утвержденной Президентом РФ 25.12.2014. Согласно Военной доктрине для реализации военной безопасности необходимо выполнение следующих условий: элиминирование угроз, связанных с применением военной силы и наличием способности противостоять враждебной военной силе.

3. *Государственная и общественная безопасность*. В соответствии с поправками к Конституции от 14.03.2020 в части ст. 67, Россия обеспечивает защиту своего суверенитета и территориальной целостности. Из этого следует, что государственная безопасность связана с защитой государственного суверенитета, независимостью государства на международной арене, а также с верховенством государства во внутренних делах. Как следует из Концепции общественной безопасности в Российской Федерации, утвержденной 14.11.2023 [84], общественная безопасность направлена на обеспечение защиты личности, общества и государства от таких факторов, как терроризм (ст. 205 УК РФ), захват заложников (ст. 206 УК РФ), организация незаконного вооруженного формирования или участие в нем (ст. 208 УК РФ), бандитизм (ст. 209 УК РФ) [85] и др. Основными показателями общественной безопасности являются *уровень преступности* и *уровень правонарушений*.

4. *Информационная безопасность*. Механизмы обеспечения информационной безопасности закреплены в Информационной доктрине, утвержденной Президентом РФ 05.12.2016. Важно отметить, что Информационная доктрина направлена (см. ч. III Информационной доктрины) на элиминирование угроз в области обороны страны, государственной и общественной безопасности, в экономической сфере, в области науки, технологий и образования, в области стратегической стабильности и равноправного стратегического партнерства и др.

5. *Безопасность в сфере науки, технологий и образования*. 21.07.2020 Президентом РФ был утвержден Указ «О национальных целях развития Российской Федерации на период до 2030 г.», в рамках которого были обозначены такие цели, как вхождение России в десятку ведущих стран мира по качеству общего образования, формирование эффективной системы выявления, поддержки и развития талантов у детей и молодежи, а также обеспечение присутствия России в десятке ведущих стран мира по объему научных исследований и разработок [86]. Также следует отметить, что механизмы обеспечения безопасности в сфере науки, технологий и образования закреплены в Стратегии научно-технологического развития, утвержденной Президентом РФ 01.12.2016. Согласно Стратегии научно-технологического развития такие понятия, как «проблема», «угроза» и «возможность» объединены в *большие вызовы*, под которыми понимается совокупность проблем, угроз и возможностей, сложность и масштаб которых таковы, что они не могут быть решены исключительно за счет увеличения материальных ресурсов.

6. *Экологическая безопасность*. Президентом РФ 19.04.2017 была утверждена Стратегия экологической безопасности, целями которой являются сохранение и восстановление природной среды, обеспечение качества окружающей среды, необходимого для благоприятной жизни человека и устойчивого развития экономики, ликвидация накопленного вреда окружающей среде вследствие хозяйственной и иной деятельности в условиях возрастающей экономической активности и глобальных изменений климата. Стоит отметить, что Стратегия экологической безопасности оперирует такими понятиями, как «глобальные (внешние) вызовы», «внутренние вызовы» и «внешние угрозы». В частности, согласно Стратегии экологической безопасности к *глобальным* (*внешним*) *вызовам* можно отнести последствия изменения климата на планете, рост потребления природных ресурсов при сокращении их запасов, сокращение биологического разнообразия и пр. К *внутренним вызовам* относятся увеличение объема образования отходов производства и потребления при низком уровне их утилизации, усиление деградации земель и почв, сокращение количества видов растений, криминализация и наличие теневого рынка в сфере природопользования и др. *Внешними угрозами* являются загрязнение атмосферного воздуха, лесные пожары, создание препятствий для миграции животных, отстрел мигрирующих видов животных, перемещение на территорию России зараженных организмов, способных вызвать эпидемии различного масштаба, и др.

7. *Безопасность в духовно-нравственной и культурной сферах*. В соответствии с поправками к Конституции от 14.03.2020 в части ст. 67.1, Россия чтит память защитников Отечества и обеспечивает защиту исторической правды. Более того, в новой ст. 68 Конституции зафиксировано, что культура в России является уникальным наследием ее многонационального народа, поэтому она поддерживается и охраняется государством. Стоит отметить, что введение данных поправок обусловлено возросшим количеством атак на отечественную историю, ростом числа фальсификаций и манипуляций ею. Кроме того, в Стратегии национальной безопасности отдельно отмечается, что абсолютная свобода личности, пропаганда вседозволенности, безнравственность и эгоизм, культ насилия, потребления и наслаждения, легализация наркотиков создает угрозу естественному продолжению жизни.

8. *Международная безопасность*. Основополагающим международно-правовым актом, который заложил основы существующего международного порядка, является Устав Организации Объединенных Наций (далее – Устав ООН), принятый 26.06.1945 [87]. XX в. показал, что ни одно государство в одиночку не

в силах обеспечить свою национальную безопасность, в связи с чем п. 97 Стратегии национальной безопасности закрепляет стремление России к обеспечению устойчивости системы международных отношений за счет укрепления центральной координирующей роли ООН и ее Совета Безопасности при разрешении глобальных и региональных проблем.

Проведенный анализ нормативно-правовых актов, закрепляющих основные положения обеспечения национальной безопасности России, позволил выявить и оценить вероятность наступления угроз национальной безопасности в экономической, военной и информационной сферах, а также оценить возможное влияние в случаях их материализации.

Оценка угроз экономической безопасности. В силу Стратегии экономической безопасности под *экономической безопасностью* следует понимать состояние защищенности национальной экономики от внешних и внутренних угроз, при котором обеспечиваются экономический суверенитет страны, единство ее экономического пространства, условия для реализации стратегических национальных приоритетов России.

Актуальность управления рисками в области экономической безопасности обусловлена внешними вызовами и угрозами. В качестве подтверждения вышесказанного можно привести официальные документы, такие как «Стратегия национальной безопасности США» и «Акт о противодействии противниками Америки посредством санкций», принятые Правительством США [88]. Анализ этих документов показывает, что США намерены и далее системно и планомерно осуществлять действия по использованию внешнеэкономического давления на мировых рынках с целью достижения конкурентных преимуществ.

Для элиминирования негативных последствий от реализации недружественных действий, в том числе США, в Стратегии экономической безопасности закрепляется перечень 25 угроз экономической безопасности. С данным перечнем можно ознакомиться в таблице 3.3. Стоит отметить, что для оценки этих угроз применялись качественные методы, методология которых закреплена в ГОСТ Р ИСО 31000 «Менеджмент риска. Принципы и руководство» и ГОСТ Р 31010 «Методы оценки риска». Оценка значений вероятностей и влияний была сформирована за счет формализации экспертного мнения. В частности, для оценки вероятностей наступления угроз и возможного влияния в случае их материализации была сформирована группа, включающая в себя десять респондентов, имеющих научные степени кандидатов (восемь респондентов) и докторов (два респондента) экономических наук. Численность обусловлена

двумя факторами: во-первых, возможностью верификации экспертных оценок; во-вторых, возможностью получения более достоверных оценок при большем количестве экспертных мнений.

Оценка включала в себя следующие этапы:

- формирование правил обработки экспертных мнений;
- оценивание вероятностей наступления угроз и возможного влияния в случае их материализации;
- анализ и обработка экспертных мнений.

Оценка значений вероятностей и влияний осуществлялась с использованием коэффициентов вербально-числовой шкалы Харрингтона (табл. 3.1, 3.2). Обработка экспертных мнений осуществлялась с помощью формул (3.1) и (3.2), где каждый эксперт представил три вида оценки по каждой угрозе – оптимистическую, наиболее вероятную (реалистическую) и пессимистическую.

$$A_{ij} = \frac{a_i^o + 4a_i^r + a_i^p}{6}, \tag{3.1}$$

$$B_{ij} = \frac{b_i^o + 4b_i^r + b_i^p}{6}, \tag{3.2}$$

где a_i^o, a_i^r и a_i^p – оптимистическая, реалистическая и пессимистическая оценка вероятности материализации угрозы национальной безопасности; b_i^o, b_i^r и b_i^p – оптимистическая, реалистическая и пессимистическая оценка возможного влияния в случае наступления угрозы национальной безопасности; A_{ij} – расчетное значение вероятности материализации i-угрозы по мнению j-эксперта; B_{ij} – расчетное значение возможного влияния в случае наступления i-угрозы по мнению j-эксперта; i – номер угрозы национальной безопасности; j – номер эксперта.

Далее для каждой угрозы рассчитывалось среднее арифметическое значение вероятности и влияния по формулам (3.3) и (3.4):

$$A_i = \frac{\sum_{j=1}^{n} A_{ij}}{n}, \tag{3.3}$$

$$B_i = \frac{\sum_{j=1}^{n} B_{ij}}{n}, \tag{3.4}$$

где n – количество экспертных мнений.

Таблица 3.1 – Коэффициенты вербально-числовой шкалы Харрингтона, применяемые для оценки влияния угрозы в случае наступления

Влияние угрозы	**Коэффициент Харрингтона**	**Комментарии**
Очень высокая	5	Максимально возможный ущерб
Высокая	4	Большой ущерб
Средняя	3	Приемлемый ущерб
Низкая	2	Незначительный ущерб
Очень низкая	1	Минимальный ущерб
Нет влияния	0	Ущерб отсутствует

Таблица 3.2 – Коэффициенты вербально-числовой шкалы Харрингтона, применяемые для оценки вероятности наступления угрозы

Вероятность угрозы	**Коэффициент Харрингтона**	**Комментарии**
Очень высокая	5	Гарантированное наступление угрозы
Высокая	4	Угроза наступит, но шанс избежать ее остается
Средняя	3	Нет гарантий, что угроза наступит, но все же такая возможность остается
Низкая	2	Остается возможность наступления угрозы
Очень низкая	1	Остается хоть и малая, но все же возможность наступления угрозы
Нет вероятности	0	Вероятность наступления угрозы отсутствует

На основании полученных оценок была построена матрица угроз в сфере экономической безопасности (рис. 3.3).

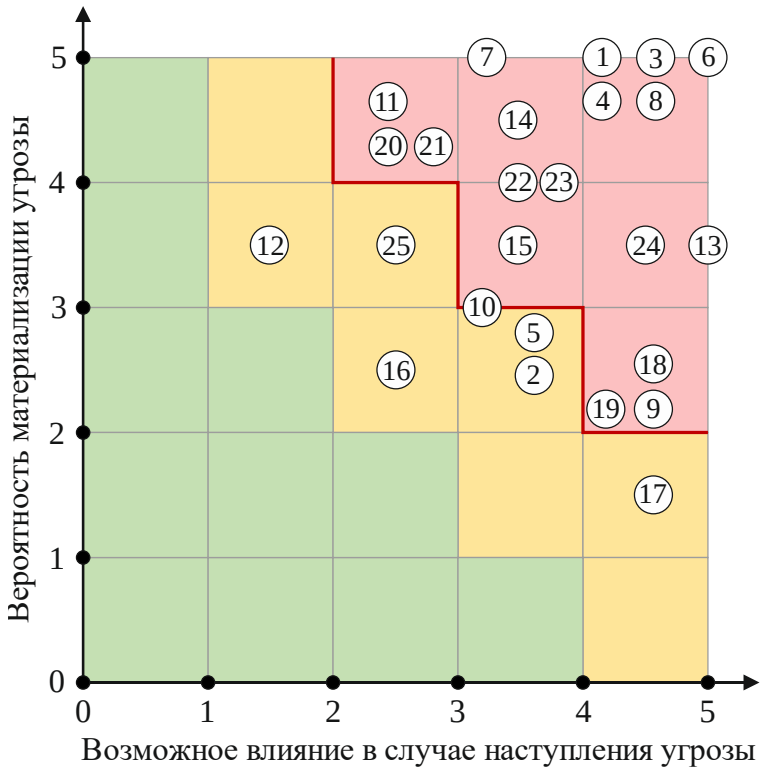


Рис. 3.3 – Матрица угроз в сфере экономической безопасности

Полученное распределение позволило установить, что 19 угроз (76% от общего количества угроз) пересекают границу толерантности и находятся в «критической области», где наиболее опасными являются:

- угроза № 1 (использование развитыми государствами своих преимуществ в уровне развития экономики и ИТ);
- угроза № 3 (использование дискриминационных мер в отношении ключевых секторов экономики России);
- угроза № 4 (повышение конфликтного потенциала в зонах экономических интересов России);
- угроза № 6 (изменение структуры мирового спроса на энергоресурсы и структуры их потребления);
- угроза № 8 (атака на информационные инфраструктуры финансово-банковской системы).

Высокая концентрация угроз в «критической области» указывает на:

- агрессивное поведение недружественных стран, которое направлено на дестабилизацию экономики России, а также на ухудшение уровня жизни населения;
- необходимость реализации эффективных и результативных элиминирующих мер, которые позволят обеспечить экономический рост и укрепление экономического суверенитета России;
- концентрацию фокуса государственного внимания на развитии системы стратегического планирования в сфере экономики с целью обеспечения устойчивого роста, создания условий для разработки и внедрения современных технологий, развития финансовой системы, повышения региональной зрелости России и эффективности внешнеэкономического сотрудничества, обеспечения безопасности экономической деятельности и развития человеческого потенциала.

Оценка угроз военной безопасности. Военная доктрина разделяет понятия «военная опасность» и «военная угроза». Под *военной опасностью* понимаются межгосударственные (внутригосударственные) отношения, которые способны при определенных условиях привести к возникновению военной угрозы, где *военная угроза* – это состояние межгосударственных (внутригосударственных) отношений, которые характеризуются реальной возможностью возникновения военного конфликта (рис. 3.4).

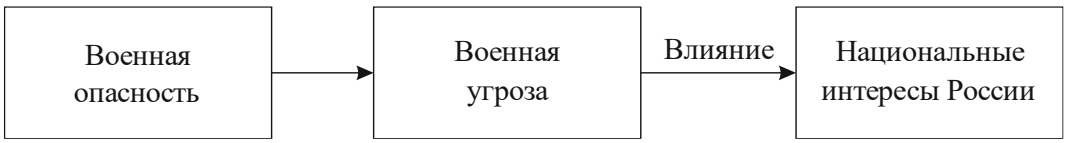


Рис. 3.4 – Связь между военной опасностью, военной угрозой и национальными интересами России

В Военной доктрине зафиксированы пять основных военных угроз (рис. 3.5), перечень которых представлен в таблице 3.3.

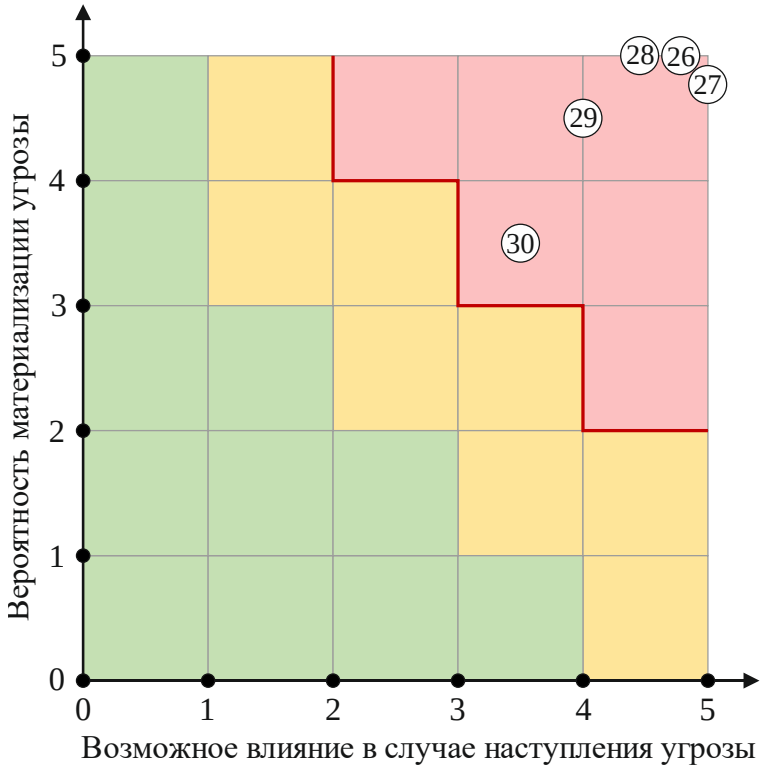


Рис. 3.5 – Матрица угроз в сфере военной безопасности

Распределение угроз в сфере военной безопасности показывает, что все угрозы находятся в «критической области» и носят экзистенциальный характер, что означает незамедлительную реализацию элиминирующих мер. В качестве примера подобных мер можно привести новую редакцию Военной доктрины Союзного государства, принятой 04.11.2022 Россией и Республикой Беларусь [89]. Сутью данного акта является повышение уровня согласованности оборонной политики министерств обороны двух стран с учетом изменений военно-политической обстановки. Кроме того, для сдерживания военных угроз Военная доктрина предусматривает поддержание в заданной степени готовности Вооруженных сил России к боевому применению, расширение взаимодействия с государствами-участниками БРИКС, а также укрепление системы коллективной безопасности в рамках ОДКБ.

Таблица 3.3 – Угрозы в сферах экономической, военной и информационной безопасности

№	Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
Оценка угроз в сфере экономической безопасности			
1	Угроза использования развитыми государствами своих преимуществ в уровне развития экономики и ИТ	5	4,2
2	Угроза структурных дисбалансов в мировой экономике и финансовой системе (например, рост частной и суверенной задолженности)	2,5	3,5
3	Угроза использования дискриминационных мер в отношении ключевых секторов экономики России (например, ограничение доступа к иностранным финансовым ресурсам и современным технологиям)	5	4,5
4	Угроза повышения конфликтного потенциала в зонах экономических интересов Российской Федерации	4,6	4,1
5	Угроза колебаний конъюнктуры мировых товарных и финансовых рынков	3,7	3,5
6	Угроза изменения структуры мирового спроса на энергоресурсы и структуры их потребления (например, за счет развития энергосберегающих технологий, «зеленых технологий» и др.)	5	4,8
7	Угроза создания межгосударственных экономических объединений без участия России в сфере регулирования торгово-экономических и финансово-инвестиционных отношений	5	3,1
8	Угроза атак на информационные инфраструктуры финансово-банковской системы	4,7	4,5
9	Угроза исчерпания экспортно-сырьевой модели экономического развития	2,1	4,5
10	Угроза отсутствия российских несырьевых компаний среди глобальных лидеров мировой экономики	3	3,2
11	Угроза изменения объема инвестиций в реальный сектор экономики (например, из-за неблагоприятного инвестиционного климата, избыточных административных барьеров, неэффективной защиты права собственности и др.)	4,5	2,5
12	Угроза изменения темпов развития в области разработки и внедрения новых и перспективных технологий (например, из-за недостаточного уровня квалификации и ключевых компетенций отечественных специалистов)	3,5	1,5

№	Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
13	Угроза истощения ресурсной базы топливно-сырьевых отраслей по мере исчерпания действующих месторождений	3,5	5
14	Угроза ограниченности масштабов российского несырьевого экспорта	4,5	3,5
15	Угроза изменения темпов экономического роста	3,5	3,5
16	Угроза несбалансированности национальной бюджетной системы	2,5	2,5
17	Угроза неэффективности государственного управления	1,5	4,5
18	Угроза изменения уровня криминализации и коррупции в экономической сфере	2,5	4,5
19	Угроза изменения доли теневой экономики	2,2	4,2
20	Угроза дифференциации населения по уровню доходов	4,2	2,5
21	Угроза изменения качества образования и медицинской помощи	4,2	2,7
22	Угроза международной конкуренции за кадры высшей квалификации	4	3,5
23	Угроза нехватки трудовых ресурсов	4	3,7
24	Угроза дифференциации регионов и муниципальных образований по уровню и темпам социально-экономического развития	3,5	4,5
25	Угроза избыточных требований в области экологической безопасности	2,5	1,5
Оценка угроз в сфере военной безопасности			
26	Угроза резкого обострения военно-политической обстановки (межгосударственных отношений) и создание условий для применения военной силы	5	4,8
27	Угроза воспрепятствования работе систем государственного и военного управления России (нарушение функционирования стратегических ядерных сил, систем предупреждения о ракетном нападении, контроля космического пространства, объектов хранения ядерных боеприпасов, атомной энергетики, атомной, химической, фармацевтической и медицинской промышленности и других потенциально опасных объектов)	4,8	5
28	Угроза создания и подготовки незаконных вооруженных формирований (деятельность незаконных вооруженных формирований на территории России и/или на территориях ее союзников)	5	4,5
29	Угроза демонстрации военной силы в ходе проведения учений на территориях государств, сопредельных с Россией и ее союзниками	4,5	4

№	Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
30	Угроза активизации деятельности вооруженных сил отдельных государств (групп государств) с проведением частичной или общей мобилизации	3,5	3,5
Оценка угроз в сфере информационной безопасности			
31	Угроза использования рядом зарубежных стран информационно-технологического воздействия в военных целях	5	4,5
32	Угроза технической разведки рядом зарубежных стран в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса	5	4,2
33	Угроза оказания информационно-психологического воздействия, которое направлено на дестабилизацию внутриполитической и социальной ситуации, и приводящего к подрыву суверенитета и нарушению территориальной целостности	5	3,5
34	Угроза дискриминации отечественных СМИ со стороны ряда зарубежных стран	4,5	3,5
35	Угроза утечки персональных данных	4,5	3
36	Угроза кибератак в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности России и ее союзников	4,5	4,5
37	Угроза кибератак на критические информационные инфраструктуры	3	5

Оценка угроз информационной безопасности. Расширение областей применения ИТ является фактором развития национальной экономики и совершенствования функционирования государственных и общественных институтов. Однако с ростом темпа цифровизации увеличивается и количество утечек персональных данных, кибератак, распространения ложных сведений (фейков), повышается деструктивное информационное воздействие на население и др.

Актуальность данных угроз подтверждают результаты исследования, которое было проведено экспертно-аналитическим центром InfoWatch. Согласно полученным данным, в России за 2022 г. количество утекших записей персональных данных и платежной информации превысило более 667 млн ед., что в 2,67 раза больше по сравнению с 2021 г. В дополнение к сказанному стоит упо-

мянуть доклад замминистра иностранных дел России Олега Сыромолотова, в котором говорилось, что НАТО отрабатывает кибердудары по российским сетям и моделирует поражение госучреждений в Калининградской области и энергосистемы Москвы [90].

Яркими примерами подобных кибердударов являются атаки в июне 2023 г. на радиостанции России, в результате чего в нескольких регионах были озвучены фейковые сообщения [91]. В качестве другого примера кибердудара можно привести атаку на сайт и мобильное приложение РЖД, которое произошло 05.07.2023 [92].

Для элиминирования подобных угроз Информационная доктрина в разделе III закрепляет основные информационные угрозы и состояние информационной безопасности России. Перечень основных угроз в сфере информационной безопасности, а также их оценки вероятностей и влияний представлены в таблице 3.3.

Анализ матрицы, представленной на рисунке 3.6, показывает высокую концентрацию угроз в сфере информационной безопасности в «критической области», что может свидетельствовать об их экзистенциальном характере. Например, если в зимний период будет совершена кибератака на критические информационные инфраструктуры (далее – КИИ) энергетики и ТЭК Сибирского федерального округа, то данная атака подвергнет опасности жизни и здоровье более 17 млн человек.

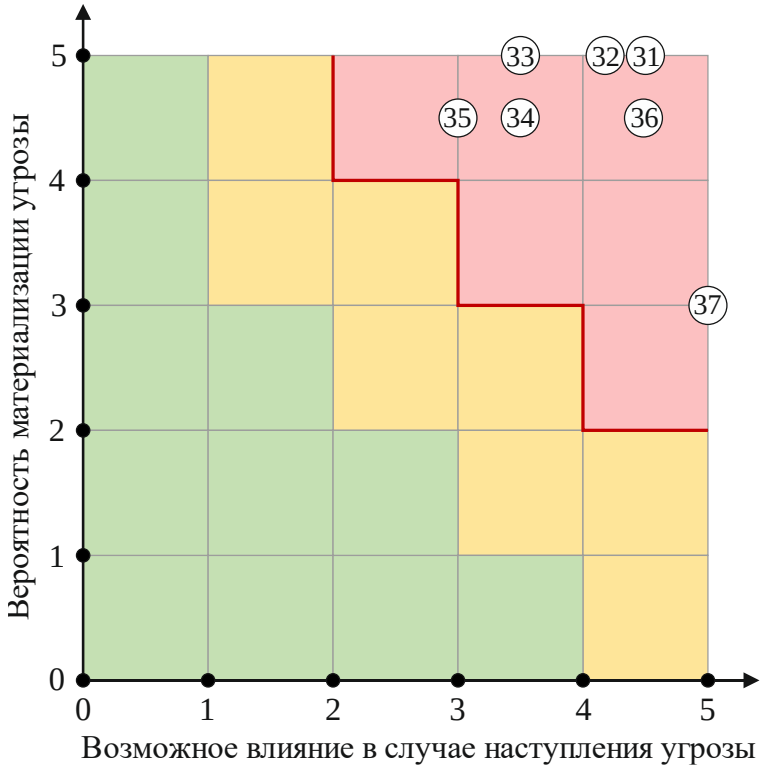


Рис. 3.6 – Матрица угроз в сфере информационной безопасности

Как один из примеров мер элиминирования кибератак на отечественные КИИ можно привести императивные механизмы, закрепленные в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (далее – Закон 187-ФЗ) [93]. Целью Закона 187-ФЗ является информационный суверенитет России в ключевых областях, таких как банковский сектор, государственное управление, медицина, образование и др.

3.3 Управление рисками при осуществлении государственного контроля (надзора) и муниципального контроля

Риск-ориентированный подход

В послании Федеральному Собранию 04.12.2014 [94] (далее – Послание) Президент РФ обозначил необходимость изменения подходов в работе надзорных, контрольных и правоохранительных органов. Согласно Посланию необходимость обновления обусловлена «тотальным, бесконечным контролем» под которым подразумевается сплошная проверка подконтрольных объектов с определенной периодичностью. «Навязчивость надзора и контроля», по словам Президента РФ, вместо того, чтобы пресекать нарушения, создают проблемы и закрывают дорогу многим законопослушным и инициативным гражданам.

Для достижения поставленной Президентом РФ цели было принято решение о реализации в системе государственного контроля (надзора) и муниципального контроля риск-ориентированного подхода.

Так, на уровне федерального законодательства в 2015 г. были внесены первые упоминания о риск-ориентированном подходе, которые нашли свое отражение в Федеральном законе от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» [95]. В частности, была включена ст. 8.1. «Применение риск-ориентированного подхода при организации государственного контроля (надзора)» [96].

Новая норма предусматривала применение с 1 января 2018 г. органами государственного контроля (надзора) при организации отдельных видов госконтроля риск-ориентированного подхода как метода организации и проведения госконтроля (надзора), согласно которому выбор интенсивности проведения

контрольных мероприятий (формы, продолжительности, периодичности) ставится в зависимость от отнесения деятельности юрлица и/или ИП к определенной категории риска либо определенному классу опасности.

До внедрения риск-ориентированного подхода модель контрольно-надзорной деятельности обязывала контрольно-надзорные органы осуществлять сплошную проверку подконтрольных объектов с определенной периодичностью, что часто приводило к неэффективному расходованию ресурсов. Вместе с тем количество подконтрольных объектов существенно превышало потенциальные возможности контрольно-надзорного органа по их проверке. Поэтому в целях снижения общей административной нагрузки на субъекты хозяйственной деятельности и повышения уровня эффективности контрольно-надзорной деятельности было принято решение о переходе на риск-ориентированную модель контроля (надзора) – от тотального контроля (надзора) к дифференцированному планированию проверок в зависимости от уровня риска причинения вреда охраняемым законом ценностям.

В целях реализации указанной нормы было принято Постановление Правительства РФ от 17 августа 2016 г. № 806 «О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации» [97] (далее – Постановление Правительства РФ № 806). В частности, предусматривалась апробация нового механизма до 2018 г. на трех видах госнадзора:

- федеральном государственном надзоре в сфере связи;
- федеральном государственном санитарно-эпидемиологическом надзоре;
- федеральном государственном пожарном надзоре.

Постепенно перечень видов федерального государственного контроля (надзора), в отношении которых применяется рассматриваемый подход, расширяется, и в 2021 г. перечень насчитывает 34 позиции. В дальнейшем планируется распространение риск-ориентированного подхода более чем на 200 видов госконтроля.

Для понимания конечных результатов работы по внедрению риск-ориентированного подхода при осуществлении контрольно-надзорной деятельности целесообразно ознакомиться с основными ее направлениями и этапами, обозначенными в Паспорте приоритетной программы «Реформа контрольной и надзорной деятельности» от 21 декабря 2016 г. № 12 (далее – Программа) [98].

Согласно Программе развитие ведомственных систем управления рисками в контрольно-надзорных органах предполагает несколько этапов, связанных с достижением каждого из четырех уровней зрелости ведомственных систем управления рисками, включая:

- формирование исчерпывающих реестров подконтрольных объектов, установление категорий риска (классов опасности) и критериев отнесения к ним объектов, отнесение объектов к определенной категории риска (классу опасности), внедрение модели поддержки перечней объектов в актуальном состоянии, обеспечение публичности и доступности перечней объектов, их категорий риска (классов опасности) и критериев отнесения к ним объектов;
- создание системы сбора объективных данных, позволяющей вести учет причиненного вреда, определение индикаторов риска и показателей для внедрения «динамической модели», а также внедрение модели актуализации индикаторов риска и показателей для «динамической модели» в зависимости от изменений профилей риска;
- переоценка на регулярной основе рисков в зависимости от фактического распределения ущерба по категориям риска (классам опасности), в том числе с использованием массивов «больших данных»;
- внедрение межведомственных карт рисков, проведение международных сопоставлений эффективности систем управления рисками.

Риск-ориентированный подход является ядром концепции реформирования системы госконтроля (надзора), муниципального контроля в РФ, закрепление которого реализовано в Федеральном законе от 31 июля 2020 г. 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» [99] (далее – Закон 248-ФЗ).

Сам термин «риск-ориентированный подход» в документе не встречается, но базовые начала новой системы оценки рисков в Законе 248-ФЗ описаны.

Основы системы оценки и управления рисками

Базовым правилам управления рисками причинения вреда (ущерба) охраняемым законом ценностям при осуществлении государственного контроля (надзора), муниципального контроля посвящена отдельная гл. 5 Закона 248-ФЗ [100]. Она содержит не только основы системы оценки и управления рисками причинения вреда (ущерба) охраняемым законом ценностям, но и категории риска причинения вреда (ущерба) и индикаторы риска нарушения обязательных

требований, включая порядок отнесения объектов госконтроля (надзора), муниципального контроля к таким категориям и выявления индикаторов риска нарушения обязательных требований, а также правила учета рисков причинения вреда (ущерба) охраняемым законом ценностям при проведении контрольных (надзорных) мероприятий.

Так, ст. 22 Закона 248-ФЗ [101] предусматривает необходимость осуществления госконтроля (надзора), муниципального контроля на основе управления рисками причинения вреда (ущерба), определяющего выбор профилактических мероприятий и контрольных (надзорных) мероприятий, их содержание (в том числе объем проверяемых обязательных требований), интенсивность и результаты. Отметим, что если из буквального толкования действующей редакции ст. 8.1 Закона 294-ФЗ [102] следует, что применение риск-ориентированного подхода предусмотрено как возможность, а не обязанность (употребляется конструкция «может применяться»), то в Законе 248-ФЗ соответствующая норма предполагает обязательное использование риск-ориентированного подхода при организации и осуществлении госконтроля (применяется формулировка «контроль (надзор) осуществляются»).

Стоит отметить, что систему управления рисками причинения вреда (ущерба) планировалось распространить только на государственный контроль (надзор) в РФ. Упоминания в контексте применения такой системы о муниципальном контроле в первоначальной редакции Проекта Федерального закона «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (далее – Законопроект о госконтроле), который впоследствии стал Законом 248-ФЗ, не было. Но в процессе доработки текста документа было решено указать о применении системы оценки рисков и в отношении муниципального контроля.

Статья 22 Закона 248-ФЗ [103] содержит определения понятий:

- ***риск причинения вреда (ущерба)*** *– вероятность наступления событий, следствием которых может стать причинение вреда* (*ущерба*) *различного масштаба и тяжести охраняемым законом ценностям;*
- ***оценка риска причинения вреда (ущерба)*** *– деятельность контрольного* (*надзорного*) *органа по определению вероятности возникновения риска и масштаба вреда* (*ущерба*) *для охраняемых законом ценностей;*

- ***управление риском причинения вреда (ущерба)*** *– осуществление на основе оценки рисков причинения вреда (ущерба) профилактических мероприятий и контрольных (надзорных) мероприятий в целях обеспечения допустимого уровня риска причинения вреда (ущерба) в соответствующей сфере деятельности.*

……

Согласно Закону 248-ФЗ контрольным (надзорным) органам предписано обеспечивать организацию постоянного мониторинга (сбора, обработки, анализа и учета) сведений, используемых для оценки и управления рисками причинения вреда (ущерба), а Правительству РФ – определить общие требования к порядку организации оценки риска причинения вреда (ущерба) при осуществлении госконтроля (надзора), муниципального контроля, включая требования к установлению критериев и категорий риска, порядку отнесения объектов контроля к категориям риска, установлению индикаторов риска нарушения обязательных требований, порядку их выявления, источникам сведений, используемых при оценке риска, и порядку их сбора, обработки, анализа и учета, порядку информирования контролируемых лиц об отнесении объектов контроля к категориям риска, периодичности проведения плановых контрольных (надзорных) мероприятий в зависимости от категории риска (ч. 6 ст. 22 Закона 248-ФЗ; [104]).

Категории и индикаторы риска

Закон 248-ФЗ выделяет шесть категорий риска причинения вреда (ущерба):

- чрезвычайно высокий риск;
- высокий риск;
- значительный риск;
- средний риск;
- умеренный риск;
- низкий риск (ч. 1 ст. 23 Закона 248-ФЗ; [105]).

От отнесения объектов контроля к определенным категориям риска будут зависеть виды и периодичность проведения в отношении них плановых контрольных (надзорных) мероприятий (табл. 3.4).

Таблица 3.4 – Зависимость проведения плановых мероприятий от категории риска причинения вреда (ущерба)

Категории риска	**Периодичность проведения плановых мероприятий**
Чрезвычайно высокий риск	Максимальная частота проведения плановых контрольных (надзорных) мероприятий – не менее одного, но не более двух контрольных (надзорных) мероприятий в год
Высокий риск	Средняя частота проведения плановых контрольных (надзорных) мероприятий – не менее одного контрольного (надзорного) мероприятия в четыре года и не более одного контрольного (надзорного) мероприятия в два года
Значительный риск	
Средний риск	Минимальная частота проведения плановых контрольных (надзорных) мероприятий – не менее одного контрольного (надзорного) мероприятия в шесть лет и не более одного контрольного (надзорного) мероприятия в три года
Умеренный риск	
Низкий риск	Плановые контрольные (надзорные) мероприятия не проводятся

Стоит отметить, что в первоначальной версии Законопроекта о госконтроле была предусмотрена иная периодичность плановых проверок:

- для объектов контроля из категории чрезвычайно высокого риска – не менее одного, но не более двух контрольно-надзорных мероприятий в год, если федеральным законом не предусмотрено установление режима постоянного государственного контроля (надзора);
- для объектов контроля, отнесенных к категориям высокого или значительного риска причинения вреда (ущерба), – не менее одного контрольно-надзорного мероприятия в четыре года и не более одного контрольно-надзорного мероприятия в год;
- для объектов контроля категорий среднего и умеренного риска – не менее одного контрольно-надзорного мероприятия в шесть лет и не более одного контрольно-надзорного мероприятия в два года.

Но многие эксперты указывали на несовершенство исходного текста этих норм – в частности, Комитет Госдумы по безопасности и противодействию коррупции в своем заключении на проект отметил, что «такая правовая конструкция сама по себе нивелирует основы системы оценки и управления рисками и допускает возможность установить большую частоту проведения плановых контрольно-надзорных мероприятий для объектов с наименьшей категорией риска». В процессе доработки текста документа соответствующие положения были скорректированы.

Важным нововведением Закона 248-ФЗ является норма о возможности освобождения контролируемого лица от проведения плановых контрольных

(надзорных) мероприятий в случае заключения договора страхования рисков причинения вреда (ущерба). Речь идет о договоре, объектом которого выступают имущественные интересы контролируемого лица, связанные с его обязанностью возместить вред (ущерб) охраняемым законом ценностям, причиненный вследствие нарушения контролируемым лицом обязательных требований. Но такая возможность будет доступна только в случае ее закрепления в федеральном законе о конкретном виде контроля (ч. 9 ст. 25 Закона 248-ФЗ; [106]).

В первоначальной редакции Законопроекта о госконтроле страхованию рисков причинения вреда (ущерба) была отведена отдельная статья, которая помимо расшифровки сути договора страхования предусматривала, что заключение контролируемым лицом со страховой организацией такого договора не может быть основанием для освобождения контролируемого лица от уголовной или административной ответственности за нарушения обязательных требований. Кроме того, в ней содержался открытый перечень требований для страховых организаций, желающих осуществлять страхование рисков причинения вреда (ущерба) контролируемыми лицами (например, обязательное членство в профессиональном объединении страховщиков, наличие не менее чем трехлетнего опыта ведения операций по страхованию гражданской ответственности граждан и организаций и т. п.). Также была закреплена обязанность страховой организации информировать контрольно-надзорные органы о заключении с контролируемым лицом договора страхования рисков причинения вреда (ущерба). Но в окончательный текст Закона 248-ФЗ эти нормы не вошли.

В соответствии с Законом 248-ФЗ критерии риска должны учитывать:

- тяжесть причинения вреда (ущерба) охраняемым законом ценностям (такая оценка проводится на основе сведений о степени тяжести фактического причинения вреда, ущерба в подобных случаях, потенциальном масштабе распространения вероятных негативных последствий, влекущих его причинение, с учетом сложности преодоления таких последствий);
- вероятность наступления негативных событий, которые могут повлечь причинение вреда (ущерба) охраняемым законом ценностям (учитываются предшествующие данные о фактическом причинении вреда (ущерба) вследствие наступления событий, вызванных определенными источниками и причинами риска причинения вреда (ущерба), по различным видам объектов контроля с выделением видов

объектов контроля, характеризующихся схожей или различной частотой случаев фактического причинения вреда (ущерба);

- добросовестность контролируемых лиц (оценивается с учетом сведений о: реализации контролируемым лицом мероприятий по снижению риска причинения вреда и его предотвращению; наличии внедренных сертифицированных систем внутреннего контроля; предоставлении контролируемым лицом доступа контрольному (надзорному) органу к своим информресурсам; независимой оценке соблюдения обязательных требований; добровольной сертификации, подтверждающей повышенный необходимый уровень безопасности охраняемых законом ценностей; заключении контролируемым лицом со страховой организацией договора добровольного страхования рисков причинения вреда или ущерба).

Решение о проведении внеплановой проверки контрольным (надзорным) органом принимается на основе индикаторов риска. Стоит отметить, что согласно ч. 9 ст. 23 Закона № 248-ФЗ под индикаторами риска понимаются отклонения объекта контроля (надзора) от параметров, которые могут привести к материализации риска. Перечень индикаторов риска для вида федерального контроля утверждается федеральным органом исполнительной власти, для вида регионального контроля – высшим исполнительным органом государственной власти субъекта Российской Федерации, для муниципального контроля – представительным органом муниципального образования (ч. 10 ст. 23 Закона № 248-ФЗ; [107]).

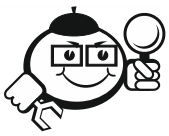
В качестве примера индикаторов риска для вида регионального контроля можно привести перечень индикаторов риска, утвержденный Постановлением Администрации Томской области от 08.07.2022 № 315а [108] (далее – Постановление № 315а). Согласно Постановлению № 315а в сфере перевозок пассажиров и багажа легковым такси на территории Томской области основанием для внеплановой проверки объекта контроля (надзора) является неоднократное объявление предостережений о недопустимости нарушения обязательных требований либо неоднократное привлечение данного объекта к административной ответственности за нарушение обязательных требований в сфере перевозок пассажиров и багажа легковым такси.

Также в Законе 248-ФЗ прописан порядок отнесения объектов госконтроля (надзора), муниципального контроля к категориям риска и выявления индикаторов риска нарушения обязательных требований. Для этого контрольные (надзорные) органы могут использовать сведения, характеризующие уровень рисков

причинения вреда (ущерба), полученные с соблюдением требований законодательства РФ из любых источников, обеспечивающих их достоверность. Например, это могут быть сведения, собранные в ходе проведения профилактических мероприятий, контрольных (надзорных) мероприятий, использования специальных режимов госконтроля (надзора), полученные от госорганов, органов местного самоуправления и организаций в рамках межведомственного информационного взаимодействия, при реализации полномочий в рамках лицензирования и иной разрешительной деятельности, из представленной отчетности, по результатам предоставления государственных и муниципальных услуг, из обращений граждан и организаций (включая контролируемых лиц), из сообщений СМИ, а также сведения, содержащиеся в информресурсах, в том числе обеспечивающих маркировку, прослеживаемость, учет, автоматическую фиксацию информации. Перечень таких сведений об объектах контроля является открытым (ч. 1 ст. 24 Закона 248-ФЗ; [109]).

3.4 Риски в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд

Высокая вероятность заключения контрактов с недобросовестными, ненадежными и недостаточно квалифицированными подрядчиками (исполнителями, поставщиками), поиск баланса между качеством выполняемых работ (оказываемых услуг, поставляемых товаров) и доступной рыночной ценой, а также низкие шансы на успешное закрытие сделок являются универсальными проблемами как для коммерческих, так и государственных (муниципальных) заказчиков. В частности, согласно данным из АИС «Мониторинг» за 2017–2019 гг. средний уровень исполнения государственных контрактов до их расторжения за 2017–2019 гг. составил 66% [110]. Среди основных причин прекращения отношений Аналитический центр при Правительстве РФ называет существенное неисполнение подрядчиками (исполнителями, поставщиками) своих обязательств, где особенно остро их недобросовестность и недостаточная квалификация проявлялась во время выполнения работ по созданию ИТ-продуктов [110]. Стоит отметить, что ИТ-продукт является обобщенным понятием, которое используется для замены таких наименований как информационная система, ИТ-результат, ИТ-услуга, ИТ-товар и других синонимов и близких по смыслу понятий, закрепленных в приказе Минкомсвязи России от 22.09.2020 № 486 и применяемых ИТ-организациями во время создания программ для ЭВМ и БД [111].


Пример

Дело № А40-263677/21-51-1834. Во время приемки государственным заказчиком было установлено, что разработанная операционная система Astra Linux SE не обеспечивает совместимость со всеми процессорами на архитектуре VLIW [112]. Из-за того, что запрашиваемый ИТ-продукт не был создан, государственный заказчик был вынужден инициировать процедуру расторжения контракта и принудить подрядчика компенсировать убытки на сумму 58 886 928,04 руб.

Дело № А03-5595/2021. Было установлено, что во время процедуры приемки средств защиты информации для 92 медицинских организаций Алтайского края государственный заказчик обнаружил существенные отступления от технического задания, что стало основанием для расторжения контракта [113]. Недобросовестность подрядчика явилась причиной обращения государственного заказчика в суд.

Дело № А56-107933/2019. Государственный заказчик в одностороннем порядке отказался от исполнения контракта на сумму 9 982 051,75 руб. [114]. Причиной конфликта между сторонами стало отсутствие документов у подрядчика, которые бы подтверждали его исключительные права на медицинскую информационную систему «Авиценна», хотя согласно условиям контракта и требованиям приказа Минцифры России от 17.12.2020 № 715 подрядчик (исполнитель, поставщик) обязан был передать исключительные права на созданные им в ходе выполнения работ результаты интеллектуальной деятельности (РИД) [115].

Более того, судебная практика показывает, что нередки случаи, когда подрядчики (исполнители, поставщики) не приступают к выполнению работ, направленных на создание и/или развитие государственных (муниципальных) ИТ-продуктов.


Пример

Дело № А03-14616/2020, где исполнитель после заключения государственного контракта так и не приступил к оказанию услуг по доработке медицинской информационной системы АРМ «Поликлиника» [116].

По результатам анализа решений судов, где одной из сторон являлась ИТ-организация (ОКВЭД 62.0), было установлено, что основными часто встречаемыми комплаенс-рисками во время заключения и исполнения государственных контрактов являются:

- *риск* отказа от заключения государственного (муниципального) контракта;
- *риск* отказа от исполнения государственного (муниципального) контракта;
- *риск* несоответствия полученного результата заявленным требованиям государственного (муниципального) контракта;
- *риск* отказа от приемки (оплаты) выполненных работ (оказанных услуг, поставленных товаров);
- *риск* признания государственного (муниципального) контракта недействительным.

Необходимость заключения контрактов с добросовестными, надежными и квалифицированными подрядчиками (исполнителями, поставщиками) также обусловлена ростом количества заключенных контрактов и их общей стоимостью. Например, согласно отчету о работе Департамента государственного заказа Томской области общая стоимость заключенных контрактов в 2022 г. по сравнению с 2018 г. увеличилась на 34,8%, с 6 879,50 млн руб. до 19 756,74 млн руб. (табл. 3.5) [117]. За 2019–2022 гг. 52 ИТ-организациями Томской области, занятыми разработкой программного обеспечения и консультационными услугами в данной области (ОКВЭД 62.0), было заключено 1 067 государственных контрактов, где в 2019 г. общая сумма заключенных контрактов составила 528 млн руб., в 2020 г. – 522 млн руб., в 2021 г. – 519 млн руб., в 2022 г. – 288 млн руб. Средняя цена одного контракта в 2019 г. превысила 1,7 млн руб., в 2020 г. – 1,6 млн руб., в 2021 г. – 2,4 млн руб., в 2022 г. – 1,2 млн руб.

Таблица 3.5 – Итоги реализации контрактной системы в Томской области за 2018–2022 гг.

Показатели	**2018 г.**	**2019 г.**	**2020 г.**	**2021 г.**	**2022 г.**
Количество заключенных контрактов, шт.	5 757	5 133	4 908	5 031	5 422
Общая стоимость заключенных контрактов, млн руб.	6 879,5	9 102,37	14 310,99	14 873,78	19 756,74

Результаты анализа судебной практики и динамики исполнения государственных контрактов наглядно показывают не только ускорение темпов цифровизации в секторе государственного управления, но и увеличение спроса на добросовестных и квалифицированных подрядчиков (исполнителей, поставщиков), которые могут успешно достигать запланированных проектных целей и создавать надежные отечественные ИТ-продукты.

Для определения подрядчиков (исполнителей, поставщиков) в сфере закупок работ, услуг и товаров, направленных на удовлетворение государственных и муниципальных нужд, заказчик применяет определенные легальные механизмы их оценки. В частности, данные механизмы закреплены в специальных нормах Федеральных законов «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ (далее – Закон № 44-ФЗ) и «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 № 223-ФЗ (далее – Закон № 223-ФЗ) [118, 119]. Представленные нормативно-правовые акты регулируют процессы планирования закупок работ (услуг, товаров), определения подрядчиков (исполнителей, поставщиков), заключения контрактов и их исполнения, мониторинга закупок работ (услуг, товаров), аудита в сфере закупок работ (услуг, товаров), а также контроля за соблюдением законодательства Российской Федерации и иных нормативных правовых актов о контрактной системе в сфере закупок работ (услуг, товаров) для обеспечения государственных и муниципальных нужд.

Рассмотрим подробнее этапы проведения закупок и способы определения подрядчиков (исполнителей, поставщиков), которые закреплены в Законе № 44-ФЗ с целью идентификации механизма выявления лучшего контрагента среди участников закупки (рис. 3.7).

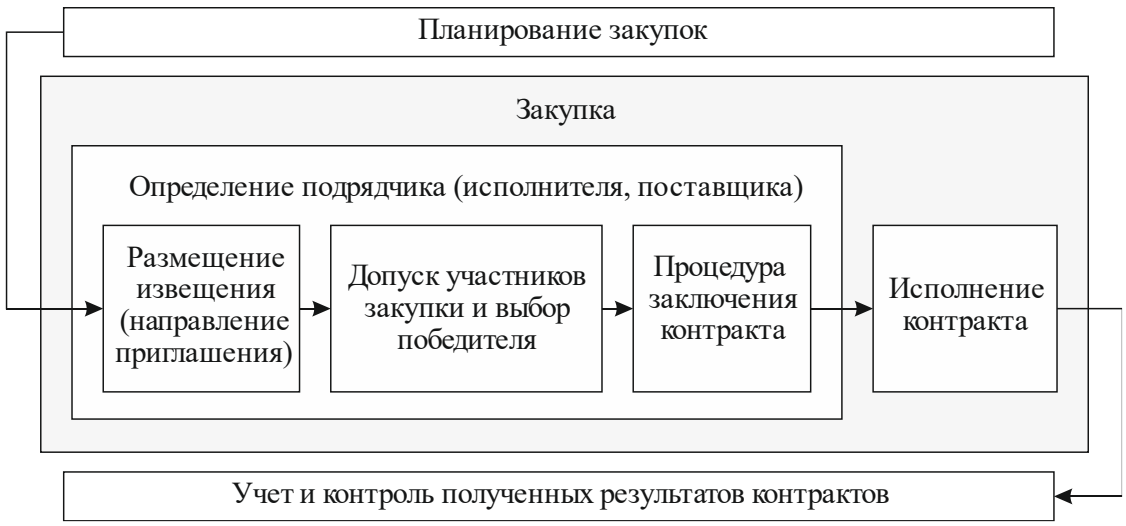


Рис. 3.7 – Этапы проведения закупок согласно Закону № 44-ФЗ

Согласно ст. 24 Закона № 44-ФЗ государственные (муниципальные) заказчики обязаны использовать конкурентные способы определения контрагента либо осуществлять закупки у единственного подрядчика (исполнителя, поставщика) (рис. 3.8).

Законодатель дифференцирует конкурентные способы на открытые и закрытые. Под *открытыми конкурентными способами* понимается порядок, при котором информация о закупке сообщается неограниченному кругу лиц, а под *закрытыми* – порядок, при котором информация сообщается ограниченному кругу лиц, которые способны осуществить выполнение работ, оказание услуг и/или поставку товаров.

Рассмотрим подробнее способы определения подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ.

Рис. 3.8 – Способы определения подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ

Конкурс

По общему правилу, уставленному Законом № 44-ФЗ, *конкурс* – это способ определения подрядчика (исполнителя, поставщика), где победителем признается тот участник закупки, который предлагает лучшие условия контракта.

Как следует из ст. 48 Закона № 44-ФЗ, открытый конкурс в электронной форме начинается с размещения государственным (муниципальным) заказчиком

на электронной площадке (РТС-тендер, Сбербанк-АСТ и др.) и в единой информационной системе (далее – ЕИС) извещения об осуществлении закупки, после которого участники закупки могут приступить к процедуре подачи заявок.

Открытый конкурс предусматривает разбиение заявки на три части. Первая часть заявки включает в себя информацию о характеристиках работы, услуги и/или товара, а также наименование страны их происхождения. Вторая часть заявки состоит из документов, которые подтверждают, что участник закупки соответствует единым и дополнительным требованиям, которые предъявляются ко всем участникам закупки (ст. 31 Закона № 44-ФЗ). Перечень единых и дополнительных требований, предъявляемых к участникам закупки, представлен в таблице 3.6. Третья часть заявки содержит информацию о цене контракта.

Таблица 3.6 – Единые и дополнительные требования, предъявляемые к участникам закупки согласно ст. 31 Закона № 44-ФЗ

№	Название требования	Описание требования
Единые требования		
1	Соответствие требованиям	Если лицо, осуществляющее выполнение работ, оказание услуг, поставку товара не соответствует требованиям, которые установлены законодательством РФ, то участник закупки не может принимать участие в закупках
2	Непроведение ликвидации участника закупки	Если в отношении участника закупки проводится процедура ликвидации, имеется решение арбитражного суда о признании данного лица несостоятельным (банкротом) или открыто конкурсное производство, то он не может принимать участие в закупках
3	Неприостановление деятельности участником закупки	Если на дату подачи заявки деятельность участника закупки приостановлена, то он не может принимать участие в закупках
4	Отсутствие у участника закупки недоимки по налогам, сборам, задолженности по иным обязательным платежам за прошедший календарный год	Размер недоимки по налогам, сборам, задолженности по иным обязательным платежам за прошедший календарный год не должен превышать 25% балансовой стоимости активов участника закупки
5	Отсутствие у участника закупки судимости за преступления в сфере экономики	Если у участника закупки имеется судимость за преступления в сфере экономики или преступления, предусмотренные ст. 289 (Незаконное участие в предпринимательской деятельности), 290 (Получение взятки), 291 (Дача взятки), 291.1 (Посредничество во взяточничестве) УК РФ, то он не может принимать участие в закупках
6	Отсутствие у участника закупки фактов привлечения к административной ответственности по ст. 19.28 КоАП РФ	Если у участника закупки имеется факт привлечения к административной ответственности по ст. 19.28 (Незаконное вознаграждение от имени юридического лица) КоАП РФ в течение 2 лет, то он не может принимать участие в закупках

№	Название требования	Описание требования
7	Обладание участником закупки исключительными правами на РИД	Если участник закупки не обладает исключительными правами на РИД, то он не может принимать участие в закупках
8	Отсутствие между участником закупки и заказчиком конфликта интересов	Под конфликтом интересов понимаются случаи, при которых руководитель заказчика, член комиссии по осуществлению закупок, руководитель контрактной службы заказчика, контрактный управляющий состоят в браке с физическими лицами либо близкими родственниками, которые являются выгодоприобретателями
9	Участник закупки не является офшорной компанией	Под офшорной компанией понимается иностранная компания, правовой статус которой определяется по законодательству места ее регистрации
10	Отсутствие у участника закупки оснований, ограничивающих его участие в закупке	Если у участника закупки имеются ограничения для участия в закупках, установленных законодательством РФ, то он не может принимать участие в закупках
11	Отсутствие участника закупки в реестре недобросовестных подрядчиков (исполнителей, поставщиков)	В реестр недобросовестных подрядчиков (исполнителей, поставщиков) включается информация об участниках закупок, уклонившихся от заключения контрактов, а также лицах, которые не исполнили либо исполнили ненадлежащим образом свои обязательства. Если участник закупки внесен в реестр недобросовестных подрядчиков (исполнителей, поставщиков), то он не может принимать участие в закупках
Дополнительные требования к участникам закупок отдельных видов работ, услуг, товаров		
12	Наличие финансовых ресурсов	Участник закупки должен иметь финансовые ресурсы, которые необходимы для исполнения контракта
13	Наличие оборудования и материальных ресурсов	Участник закупки должен иметь на праве собственности или ином законном основании оборудование и другие материальные ресурсы, которые необходимы для исполнения контракта
14	Наличие опыта работы	Участник закупки должен иметь опыт работы, связанный с предметом контракта, и соответствующую деловую репутацию
15	Наличие необходимого количества специалистов и иных работников	Участник закупки должен иметь необходимое количество специалистов и иных работников определенного уровня квалификации для исполнения контракта

Необходимо отметить, что согласно ст. 14 Закона № 44-ФЗ и постановления Правительства РФ от 16.11.2015 № 1236 для организаций, выполняющих работы, оказывающих услуги и поставляющих товары в сфере ИТ установлен запрет на допуск ИТ-продуктов и баз данных (БД), происходящих из иностранных государств, а также исключительных прав на такие ИТ-продукты и их прав использования [120]. Исключениями являются только ИТ-продукты, которые внесены в единый реестр программ для ЭВМ и БД и в единый реестр программ для ЭВМ и БД из государств – членов Евразийского экономического союза [121].

В соответствии с требованиями ст. 39 Закона № 44-ФЗ для определения подрядчиков (исполнителей, поставщиков) государственный (муниципальный) заказчик формирует комиссию, предназначенную для рассмотрения и документального сопровождения всех частей заявок, которые поступают от участников закупки.

Для успешного заключения контракта оператор электронной площадки и ЕИС, комиссия и участники закупки совершают в определенный срок предусмотренный порядок действий. В частности, в течение двух рабочих дней после даты окончания подачи заявок комиссия оценивает первые части заявок. Оценка осуществляется с помощью критериев и показателей, зафиксированных в ст. 32 Закона № 44-ФЗ и постановлении Правительства РФ от 31.12.2021 № 2604 (далее – Постановление № 2604) [122]. В силу закрепленных требований заказчик обязан указывать используемые критерии и их величины значимости, причем количество критериев должно быть не менее чем два, где одним из критериев должна быть цена контракта или сумма цен единиц работ, услуг, товара.

Необходимо отметить, что сумма величин значимости всех используемых критериев составляет 100%. Перечень критериев оценки заявок участников закупки согласно Закону № 44-ФЗ и Постановлению № 2604 представлен на рисунке 3.9.

Порядок оценки заявок, предельные величины значимости критериев оценки заявок, а также требования к форме документа закреплены в Постановлении № 2604 [122]. Согласно данному постановлению для оценки заявок могут применяться такие критерии оценки, как *цена контракта*, *сумма цен единиц товара*, *работы*, *услуги* ($БЦ_i$), *расходы* ($БР_i$), *характеристики объекта закупки* ($БХ_i$) и *квалификация участников закупки*. Причем для оценки квалификации участников закупки могут использоваться один либо несколько показателей – наличие закупки финансовых ресурсов, наличие на праве собственности или ином законном основании оборудования и других материальных ресурсов, наличие опыта выполнения работ, оказания услуг, поставки товара, связанного с предметом контракта, наличие деловой репутации, а также наличие специалистов и иных работников определенного уровня квалификации.

Рис. 3.9 – Перечень критериев оценки заявок участников закупки согласно Закону № 44-ФЗ и Постановлению № 2604

В зависимости от выбранных показателей критерия оценки «квалификация участников закупки» государственный (муниципальный) заказчик имеет право запрашивать документы, подтверждающие наличие свободных денежных средств на счетах участников закупки, оборудования, материальных ресурсов, специалистов и др. (табл. 3.7).

Таблица 3.7 – Перечень показателей критерия оценки «квалификация участников закупки» согласно Постановлению № 2604

№	Название показателя	Описание показателя
1	Наличие финансовых ресурсов	Проверка наличия свободных денежных средств на счетах участника закупки
2	Наличие на праве собственности или ином законном основании оборудования и других материальных ресурсов	Проверку оборудования и наличие необходимых для выполнения контракта материальных ресурсов заказчик осуществляет путем изучения подтверждающих документов, таких как инвентаризационные карточки учета объектов основных средств, договоры аренды (лизинга), выписки из ЕГРН, договоры аренды объектов недвижимого имущества и иные документы
3	Наличие опыта выполнения работ, оказания услуг, поставки товара, связанного с предметом контракта	Оценку опыта у участника закупки заказчик осуществляет путем изучения договоров, актов, требований об уплате неустоек (штрафов, пеней) и др., которые имеются у участника закупки. Данные документы могут быть использованы, только если они предоставлены участником закупки в полном объеме, со всеми приложениями. По результатам изучения заказчик определяет общую цену исполненных участником закупки договоров, общее количество исполненных участником закупки договоров, наибольшую цену одного из исполненных участником закупки договоров
4	Наличие деловой репутации	Оценка деловой репутации. Для оценки деловой репутации учитывается индекс деловой репутации участников закупки. Согласно ГОСТ Р 66.0.01-2017 *индексом деловой репутации* является целое числовое значение в интервале от 0 до 100, которое присваивается субъекту предпринимательской деятельности по результатам работы [123]
5	Наличие специалистов и иных работников определенного уровня квалификации	Оценку уровня квалификации специалистов и иных работников заказчик осуществляет посредством изучения трудовых книжек и иных документов, которые подтверждают профессиональную квалификацию специалистов и работников участника закупки

В силу п. 29 Постановления № 2604 показатели, связанные с деловой репутацией, могут применяться исключительно для юридических лиц и/или индивидуальных предпринимателей. В случае применения данного показателя осуществляется оценка индекса деловой репутации в соответствии с националь-

ными стандартами в области оценки деловой репутации субъектов предпринимательской деятельности. Проведенный анализ методических рекомендаций Технического комитета по стандартизации «Оценка опыта и деловой репутации предприятий» [124] и действующих национальных стандартов, закрепляющих порядок проведения оценки опыта и деловой репутации субъектов предпринимательской деятельности, показал, что общие положения, требования и руководящие принципы закреплены в ГОСТ Р 66.0.01 [123]. Также было установлено, что национальная система стандартов формирует порядок оценки деловой репутации для различных видов экономической деятельности, а именно для лиц, осуществляющих архитектурно-строительное проектирование [125], осуществляющих инженерные изыскания [126], строительных организаций [127], производящих и реализующих пожарно-техническую продукцию [128], выполняющих работы (оказывающих услуги) в области обеспечения пожарной безопасности объектов защиты [129], выполняющих перевозки крупногабаритных тяжеловесных грузов [130] и оказывающих охранные услуги [131]. Важно отметить, что в национальной системе стандартов отсутствует формализованный порядок оценки деловой репутации субъектов, которые ведут предпринимательскую деятельность в области ИТ, что, в свою очередь, создает значительные препятствия в определении добросовестных, надежных и квалифицированных подрядчиков (исполнителей, поставщиков) способных выполнять работы по созданию и/или развитию государственных (муниципальных) ИТ-продуктов.

После оценки первых частей заявок комиссия с помощью электронной площадки формирует протокол и затем, не позднее одного часа с момента его получения, оператор электронной площадки направляет уведомление каждому участнику закупки о наилучшем предложении и сообщает о дате и времени проведения процедуры подачи предложений о цене контракта (ст. 48 Закона № 44-ФЗ).

Участники закупки, первые части заявок которых были одобрены комиссией, по своему выбору могут подать предложение о цене контракта в течение одного часа. Если участник закупки не делает предложений по цене, тогда в работу берется ценовое предложение, которое он представил в третьей части своей заявки.

Комиссия, в течение двух рабочих дней после даты получения вторых частей заявок, оценивает их и формирует с помощью электронной площадки соответствующий протокол. После получения протокола о рассмотрении вторых частей заявок оператор электронной площадки и ЕИС в течение одного часа

направляет государственному (муниципальному) заказчику ценовые предложения, которые поступили от участников закупки.

В течение одного рабочего дня, оценив ценовые предложения и результаты первых и вторых частей заявок, комиссия присваивает порядковые номера участникам закупки, которые прошли конкурсный отбор. Согласно ст. 48 Закона № 44-ФЗ порядковый номер уменьшается по степени выгодности, т. е. первый номер присваивается участнику закупки, который предложил самые выгодные условия исполнения контракта. Этот участник закупки признается победителем открытого конкурса.

После определения победителя государственный (муниципальный) заказчик формирует протокол о подведении итогов определения подрядчика (исполнителя, поставщика), который в течение одного часа размещается оператором на электронной площадке и в ЕИС. Отметим, что этот протокол в силу ст. 51 Закона № 44-ФЗ является основанием для последующего заключения контракта, в связи с чем не позднее двух рабочих дней, следующих за днем размещения вышеуказанного протокола, государственный (муниципальный) заказчик формирует в ЕИС проект контракта без подписи.

Победитель закупки в течение пяти рабочих дней по своему выбору может подписать проект контракта, подготовить протокол разногласий либо отказаться от заключения контракта. Если победитель закупки подписывает проект контракта усиленной электронной подписью, то государственный (муниципальный) заказчик не позднее двух рабочих дней подписывает контракт со своей стороны и размещает его в ЕИС.

Этапы и сроки проведения открытого конкурса в электронной форме по определению подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ представлены на рисунке 3.10.

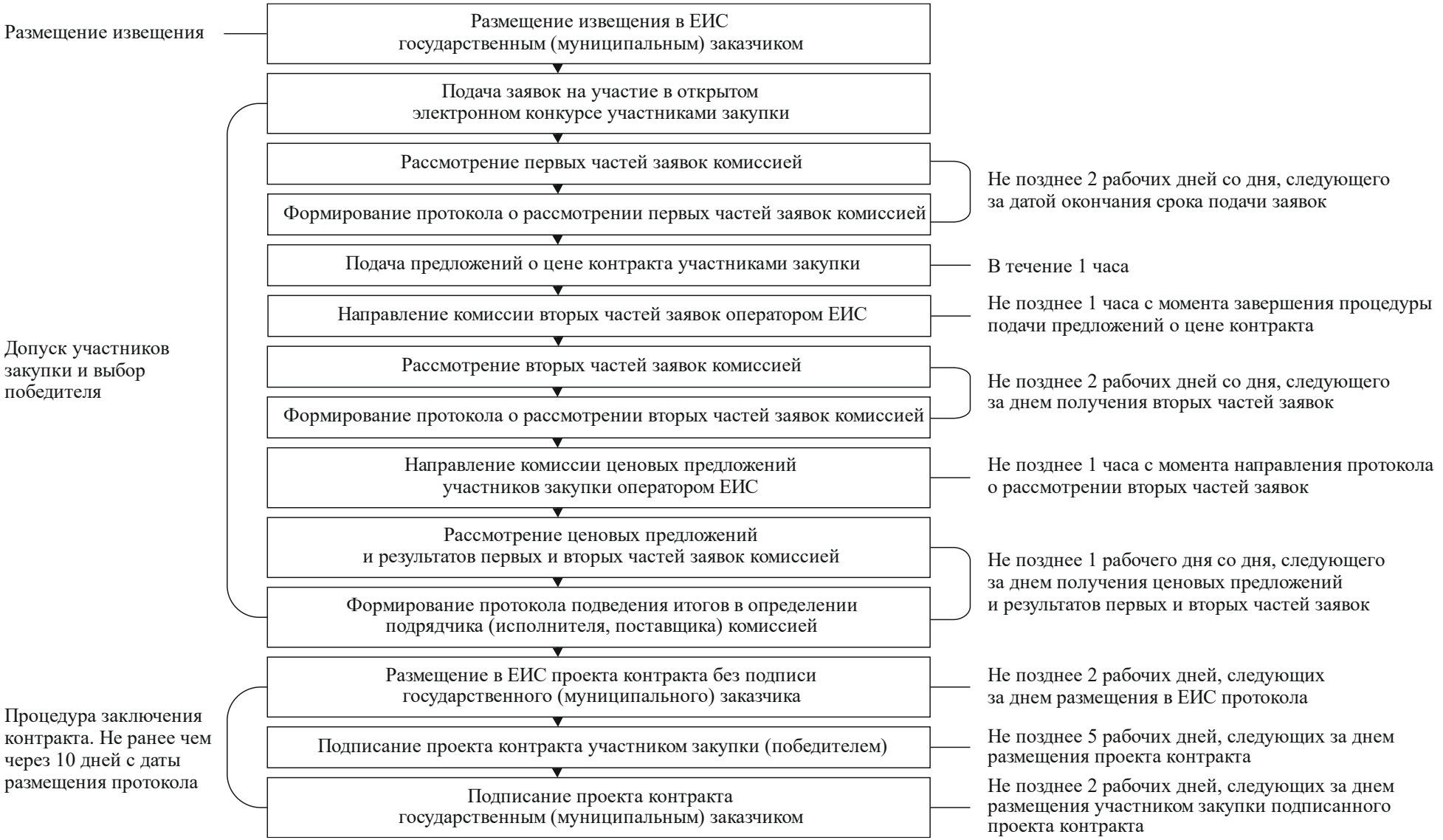


Рис. 3.10 – Этапы и сроки проведения открытого конкурса в электронной форме по определению подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ

Аукцион

Аукцион – это способ определения подрядчика (исполнителя, поставщика), где победителем признается тот участник закупки, который предлагает наиболее низкую цену контракта. Согласно ст. 24 Закона № 44-ФЗ и распоряжению Правительства РФ от 21.03.2016 № 471-р (далее – Распоряжение № 471-р) государственные (муниципальные) заказчики обязаны проводить аукцион в электронной форме только для определенных работ, услуг и товаров [132].

Процедура проведения открытого аукциона в электронной форме отличается от процедуры открытого конкурса в электронной форме. В частности, в силу ст. 49 Закона № 44-ФЗ участники закупки имеют право, пока не наступила дата окончания подачи заявок, подавать свои ценовые предложения, предусматривающие снижение начальной (максимальной) цены контракта (НМЦ) от 0,5% до 5%.

Комиссия государственного (муниципального) заказчика не позднее двух рабочих дней со дня, следующего за датой окончания подачи заявок, рассматривает и присваивает каждой заявке порядковый номер согласно возрастанию цены контракта. Победителю закупки присваивается первый номер. Принятое решение фиксируется в протоколе подведения итогов комиссией, который в течение одного часа размещается оператором на электронной площадке и в ЕИС. Данный протокол согласно ст. 51 Закона № 44-ФЗ является основанием для последующего заключения контракта. Процедура заключения контракта открытого аукциона аналогична процедуре открытого конкурса в электронной форме.

Этапы и сроки проведения открытого аукциона в электронной форме по определению подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ представлены на рисунке 3.11.

Рис. 3.11 – Этапы и сроки проведения открытого аукциона в электронной форме по определению подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ

Запрос котировок в электронной форме

Запрос котировок в электронной форме – это способ определения подрядчика (исполнителя, поставщика), где победителем признается тот участник закупки, который предлагает наиболее низкую цену контракта. В отличии от аукциона участники могут размещать свое предложение только один раз, не видя ценовые предложения других участников.

В соответствии с условиями ст. 24 Закона № 44-ФЗ законодатель применяет для запроса котировок ограничения по ценовому критерию. В частности, запрос котировок может применяться для контрактов, цена которых не превышает 10 млн руб. [133]. Согласно нормам Закона № 44-ФЗ годовой объем закупок государственного (муниципального) заказчика, осуществляемых с помощью данного способа определения подрядчика (исполнителя, поставщика), не должен превышать 20% и совокупного годового объема закупок. Однако согласно вступившему в силу Федеральному закону от 28.04.2023 № 154-ФЗ «О внесении изменений в Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» до 31.12.2026 данные ограничения не действуют [133].

Однако если закупаются работы, услуги и товары, необходимые для нормального жизнеобеспечения граждан, лекарственные препараты, спортивный инвентарь и оборудование, необходимые для олимпийской и параолимпийской команд РФ, услуги по защите интересов РФ в судебных органах иностранных государств и международных судах, изделия народных художественных промыслов, жилых помещений для детей-сирот и детей, оставшихся без попечения родителей, запрос котировок может применяться для контрактов независимо от НМЦ (начальной максимальной цены).

Процедура запроса котировок имеет упрощенный порядок рассмотрения заявок, что значительно сокращает срок определения подрядчика (исполнителя, поставщика). В частности, согласно ст. 50 Закона № 44-ФЗ, не позднее одного часа с момента окончания подачи заявок оператор электронной площадки направляет государственному (муниципальному) заказчику поступившие заявки. Далее в течение двух рабочих дней комиссия рассматривает и присваивает каждой заявке порядковый номер. Победителю закупки присваивается первый номер. Принятое решение фиксируется в протоколе, который в течение одного часа размещается оператором в ЕИС и на электронной площадке. Если закупка работ, услуг и товаров составляет государственную тайну, касающуюся ценностей Государственного фонда драгоценных металлов и драгоценных камней РФ, музейных предметов и

музейных коллекций, создания, модернизации, поставки, ремонта вооружения, военной и специальной техники, услуг по страхованию, транспортировке и охране, а также работ по исследованию и использованию космического пространства, материалов и техники, то для этих сделок применяются *закрытые конкурентные способы* определения подрядчика (исполнителя, поставщика) (§3 Закона № 44-ФЗ).

Процедура заключения контракта по итогам проведения запроса котировок аналогична открытому конкурсу в электронной форме и открытому аукциону в электронной форме.

Закупка у единственного подрядчика (исполнителя, поставщика)

Закупка у единственного подрядчика (*исполнителя, поставщика*) осуществляется, когда закупка работы, услуги и/или товара относится к сфере деятельности субъектов естественных монополий, мобилизационной подготовке РФ, поставке российских вооружений и военной техники и др.

Рассмотрев способы определения подрядчика (исполнителя, поставщика), отметим основные проблемы, которые возникают во время их применения. В частности, А. О. Никитина отмечает, что несмотря на открытость процедуры заключения контрактов, для многих действующих экономических агентов финансовые требования становятся существенным барьером [134]. В качестве примера А. О. Никитина ссылается на случаи, которые возникали во время применения постановления Правительства РФ от 10.05.2018 № 564, а именно на случаи взимания оплаты операторами ЕИС за проведение электронных процедур [135].

С. А. Евграфов раскрывает проблему большого количества изменений, которые активно вносятся законодателем в Закон № 44-ФЗ [136]. По итогу проведенного исследования С. А. Евграфов пришел к выводу, что частое обновление норм влечет негативные последствия как для государственных (муниципальных) заказчиков, так и для участников закупок. В качестве примера ученый обращается к решению № 04-50/483-2018 Управления Федеральной антимонопольной службы по Республике Бурятия, согласно которому заказчик был привлечен к административной ответственности за нарушение требований, которые вступили в силу.

Чрезмерную регулированность сферы государственных закупок в своих трудах также отмечает М. В. Шмелева [137]. Ее исследования показывают, что общее количество опубликованных нормативно-правовых актов, которые касаются государственных (муниципальных) закупок, уже превысило тысячу наиме-

нований. В качестве примера ученый приводит дело № А73-6308/2022, где Прокуратура Хабаровского края потребовала признать заключенные государственные контракты недействительными, поскольку порядок проведения закупки был не соблюден [138].

Отдельно стоит отметить проблему смещения акцентов во время оценивания заявок в сторону экономности бюджетных средств. А. А. Науразбаева отмечает, что в международной практике цена не является единственным критерием при определении подрядчиков, исполнителей и/или поставщиков [139]. В частности, в Директиве Европейского парламента и Совета Европейского Союза 2014/24/ЕС сказано, что помимо цены обязательно должны быть учтены полезный эффект и срок службы создаваемого результата (поставляемого товара) [140].

В отечественном законодательстве также имеются указания на установление баланса между экономностью и результативностью. Так, в норме ст. 34 БК РФ говорится о том, что при составлении и исполнении бюджетов необходимо исходить из необходимости достижения заданных результатов с использованием наименьшего объема средств (экономность) и достижения наилучшего результата с использованием определенного объема средств (результативность) [141]. Баланс между экономностью и результативностью согласно нормам бюджетного законодательства называется *экономической эффективностью использования бюджетных средств*.

Смещение акцентов в сторону экономности вызвано практикой применения законов, регулирующих закупку работ, услуг и товаров для государственных и муниципальных нужд. Например, закупка лекарств по торговому названию запрещена Федеральной антимонопольной службой, поэтому заказчики были обязаны осуществлять закупку по международному непатентованному названию. Это привело к тому, что качественные препараты стали проигрывать дешевым и сомнительным лекарствам [140].

Логично предположить, что принцип экономической эффективности использования бюджетных средств должен стать ведущим при определении победителя, особенно при выполнении работ по созданию и/или развитию государственных (муниципальных) ИТ-продуктов, где квалификация подрядчика (исполнителя, поставщика) играет решающую роль. Это означает, что применение данного принципа должно выражаться в соблюдении баланса между возможностью достижения запланированных результатов и эффективным использованием ограниченных ресурсов.

Таким образом, на основании проведенного анализа судебной практики и легальных механизмов оценки контрагентов можно заключить, что принцип экономической эффективности использования бюджетных средств должен стать ведущим для объектов закупки, где планируется выполнение работ по созданию и/или развитию государственных (муниципальных) ИТ-продуктов. Это означает, что для соблюдения баланса между экономностью и результативностью, увеличения вероятности заключения контрактов с добросовестными, надежными и квалифицированными подрядчиками (исполнителями, поставщиками), а также повышения шансов на успешное закрытие государственных (муниципальных) контрактов требуется усовершенствовать способы определения подрядчиков (исполнителей, поставщиков).

Возможным решением по усовершенствованию способов определения подрядчиков (исполнителей, поставщиков) в области ИТ может стать включение в критерий «квалификация участников закупки» показателя, учитывающего зрелости управления ИТ-проектами. Зарубежный опыт показывает, что при поиске лучшего контрагента заказчики часто прибегают к оценке уровня зрелости управления ИТ-проектами потенциальных подрядчиков (исполнителей, поставщиков) [142]. Под *зрелостью управления проектами понимается определенный уровень развития подрядчика* (*исполнителя, поставщика*), *который выражается в способности успешно достигать предусмотренных контрактом существенных условий*. Накопленные лучшие практики решения проблем, возникших во время выполнения контрактов, наличие опыта и работников определенного уровня квалификации, обеспеченность финансовыми и материальными ресурсами, управленческая и комплаенс-чистота проектной документации, качественное исполнение ключевых процессов и высокий рейтинг деловой репутации обуславливают зрелость подрядчика (исполнителя, поставщика) в области управления проектами, которая выражается в гарантированном выполнении обязательств, предусмотренных условиями контракта. Отсутствие соответствующего опыта либо незрелость в области проектного управления создает угрозу ненадлежащего выполнения данных обязательств.

Контрольные вопросы по главе 3

1. Как можно элиминировать риск того, что заказчик откажется принимать выполненную работу (оказанную услугу, поставленный товар)?

2. Назовите и охарактеризуйте составляющие элементы национальной безопасности Российской Федерации.
3. Какие риски угрозы в сфере экономической безопасности пересекают границу толерантности и находятся в «критической области»?
4. Какие риски угрозы в сфере информационной безопасности пересекают границу толерантности и находятся в «критической области»?
5. Какие риски угрозы в сфере военной безопасности пересекают границу толерантности и находятся в «критической области»?
6. Опишите суть риск-ориентированного подхода согласно Постановлению Правительства РФ от 17 августа 2016 г. № 806 «О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации».
7. Назовите основные риски в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд и способы их элиминирования.

Заключение

Анализ доктринальных документов недружественных стран показал, что США, Канада и Великобритания в системе государственного управления придерживаются политики нулевой терпимости к угрозам, которые пересекают границу толерантности. Оценка же угроз национальной безопасности Российской Федерации показала, что угрозы в экономической, военной и информационных сферах находятся в «критической области» (81% от общего количества угроз) и пересекают границу толерантности. Причем важно отметить, что многие угрозы носят экзистенциальный характер, что требует оперативной реализации мер, направленных на их элиминирование.

В этой связи важно подчеркнуть, что изложенные в настоящем учебном пособии основные теоретические аспекты риск-ориентированного управления и описанные инструменты по элиминированию угроз в государственном и муниципальном управлении являются базовыми знаниями, которые необходимы для создания мер по элиминированию угроз, в том числе и экзистенциального характера. Эффективное и результативное управление рисками в системе публичного управления во многом же зависит от индивидуального роста профессиональной подготовки каждого государственного (муниципального) служащего, руководителя департамента, подразделения, отдела, проекта, который на своем рабочем месте ежедневно вносит свой вклад в развитие культуры управления рисками.

Список использованных источников и литературы

1. Фадейкина Н. Эволюция взглядов на категории «риск» и «неопределенность» в экономической науке // Риск: ресурсы, информация, снабжение, конкуренция, 2013. – № 3. – С. 202–208.
2. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство. ISO 31000:2009. Risk management – Principles and guidelines (IDT). – М. : Стандартинформ, 2012. – 19 с.
3. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. ISO 31000:2018. Riskmanagement – Guidelines (IDT). – М. : Стандартинформ, 2020. – 19 с.
4. Балабанов И. Т. Риск-менеджмент. – М. : Финансы и статистика, 1996. – 192 с.
5. Машков Д. М. Научные подходы к управлению рисками промышленных предприятий // Инженерный вестник Дона. – 2014. – Том 31. – № 4-1. – С. 65.
6. Филимонов Д. И. Классификация рисков кадровой безопасности в деятельности IT-структур // Экономика и предпринимательство. – 2017. – № 5-1 (82-1). – С. 682–685.
7. Бурков В. Н., Новиков Д. А. Как управлять проектами. – М. : Синтег, 1997. – 188 с.
8. Мазур И. И., Шапиро В. Д. Управление проектами. – М. : Высшая школа, 2001. – 502 с.
9. Project management body of knowledge. Guide 4th edition (PMBOK-4). – Project Management Institute (PMI), 2008. – 506 p.
10. Project management body of knowledge. Guide 5th edition (PMBOK-5). – Project Management Institute (PMI), 2013. – 616 p.
11. Project management body of knowledge. Guide 6th edition (PMBOK-6). – Project Management Institute (PMI), 2017. – 756 p.
12. 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.
13. Enterprise Risk Management. Integrating with Strategy and Performance. – Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017. – 16 p.

14. Грабовый П. Г., Петрова С. Н. и др. Риски в современном бизнесе. – М. : Издательство «Алане», 1994 г. – 200 с.
15. Шохин Е. И. Финансовый менеджмент. – М. : ИД ФБК-ПРЕСС, 2002. – 408 с.
16. Королев В. Ю., Бенинг В. Е., Шоргин С. Я. Математические основы теории риска. – М. : Физматлит, 2011. – 620 с.
17. Гражданский кодекс Российской Федерации (ГК РФ). Комментарии к последним изменениям. – М.: АБАК, 2019. – 752 с.
18. Даль В. И. Толковый словарь живого великорусского языка. – М. : Цитадель, 1998. – 11465 с.
19. Management of Risk: Guidance for Practitioners (M_o_R®). – The Office of Government Commerce, 2010. – 160 p.
20. Managing Successful Projects with PRINCE2 (PRINCE2®). – TSO, 2017. – 412 p.
21. Качалов Р. М. Управление хозяйственным риском. – М. : Наука, 2002. – 192 с.
22. Мадера А. Г. Риски и шансы. Неопределенность, прогнозирование и оценка. – М. : Красанд, 2014. – 448 с.
23. Мадера А. Г. Принятие решений в условиях неопределенности при актуализации в будущем множества возможных шансов и рисков // Экономические науки. – 2014. – № 4. – С. 136–140.
24. Вигерс К., Битти Д. Разработка требований к программному обеспечению. 3-е изд., дополненное. – СПб. : БХВ, 2022. – 736 с.
25. США вернули Colonial Pipeline большую часть от уплаченного хакерам выкупа. – URL: https://clck.ru/VMkiJ (дата обращения: 04.04.2023).
26. Американская страховая компания заплатила хакерам $40 млн. Это крупнейший выкуп из известных. – URL: https://clck.ru/V2hpQ (дата обращения: 04.04.2023 г.).
27. Бельгия заявила о масштабной кибератаке со «шпионскими» целями. – URL: https://clck.ru/V5sbS (дата обращения: 04.04.2023).
28. All of JBS’s U.S. Beef Plants Were Forced Shut by Cyberattack. – URL: https://clck.ru/VFrq5 (дата обращения: 04.04.2023).
29. McDonald's сообщил об утечке данных из-за хакерской атаки. – URL: https://clck.ru/VU2P6 (дата обращения: 04.04.2023).
30. В одном из регионов ФРГ впервые ввели режим ЧС из-за кибератаки. – URL: https://clck.ru/W4qKF (дата обращения: 04.04.2023).

31. «Алроса» не сможет заплатить по евробондам $7,75 млн из-за санкций. – URL: https://clck.ru/rdwnT (дата обращения: 04.04.2023).
32. Ключников В. О. Идентификация рисков ИТ-проектов // Государственное управление. Электронный вестник, 2009. – № 20. – С. 1−7.
33. Ключников В. О. Опционный метод управления рисками в инвестиционных ИТ-проектах // Вестник Московского университета. Серия 21: Управление (государство и общество), 2010. – № 1. – С. 69–78.
34. Ключников В. О. Реальные опционы в проектах информационных технологий // Российское предпринимательство, 2011. – № 12–2. – С. 118–124.
35. Никонов В. А. Управление рисками. Как больше зарабатывать и меньше тратить. – М. : Альпина Паблишер, 2009. – 285 с.
36. Ефимов В. В. Сборник методов поиска новых идей и решений управления качеством. – Ульяновск: УлГТУ, 2011. – 194 с.
37. Crawley F., Tyler B. Hazard identification methods. Institute of Chemical Engineers, 2003. – 98 p.
38. Card A., Ward J., Clarkson P. Beyond FMEA: the structured what-if technique (SWIFT) // Healthcare Risk Manage, 2012. – Vol. 31. – P. 23–29.
39. Авдошин С. М., Песоцкая Е. Ю. Информатизация бизнеса. Управление рисками, 2011. – М. : ДМК Пресс. – 176 с.
40. Песоцкая Е. Ю. Управление рисками в ИТ-проектах // Альманах современной науки и образования, 2008. – № 1 (8). – С. 157−159.
41. Песоцкая Е. Ю. Управление рисками при внедрении ИТ-проектов // Успехи современного естествознания, 2008. − № 1. – С. 11−13.
42. 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.
43. Wijayanti D., Sukwika T., Ramli S. AnalisisInsidenFatali-ty Akibat Covid-19 MenggunakanMetode 5 Why, SCAT, BowTie, dan ISM // JurnalMigasian, 2022. – 6 (1). – P. 84–92.
44. ГОСТ Р 31010-2011 Методы оценки риска. ISO/IEC 31010:2009. Risk management – Risk assessment techniques (IDT). – М. : Стандартинформ, 2012. – 74 с.
45. Merna T., Al-Thani F. Corporate risk management. – John Wiley & Sons, Ltd, 2008. – 2nd ed. – 443 p.

46. The Department of Defense (DoD) United States of America. Risk Management Guide for DOD Acquisition, 2006. – Sixth Edition. – Version 1.0. – 34 p.
47. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ). – М. : Проспект, 2019. – 688 с.
48. Талеб Н. Н. Черный лебедь. Под знаком непредсказуемости. – 2-е изд. Доп. – М. : КоЛибри, Азбука-Аттикус, 2015. – 736 с.
49. Николаенко В. С. Внедрение риск-менеджмента в ИТ-проекты // Государственное управление. Электронный вестник, 2016. – № 54. – С. 63–88.
50. The CHAOS Manifesto. – The Standish Group, 2014. – 16 p.
51. 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. ст. по материалам науч.-практ. конф. с междунар. участием. – Томск, 2016. – С. 12–16.
52. Гага В. А., Козлова С. А., Тютюшев А. П., Ярославцева Е. Н. Российские системы распознавания и сопровождения лидера. – Томск : Изд-во Том. ун-та, 2011. – 196 с.
53. Селиховкин И. Управление ИТ-проектом. Эффективная система «с нуля» в любой организации. – СПб., 2010. – 90 с.
54. Никонов В. А. Управление рисками. Как больше зарабатывать и меньше тратить. – М. : Альпина Паблишер, 2009. – 285 с.
55. Поляков А. А., Ключников В. О. Опционный метод управления рисками в инвестиционных ИТ проектах // Вестник Московского университета. Серия 21: Управление (государство и общество), 2010. – № 1. – С. 69–78.
56. Решение Арбитражного суда Ямало-Ненецкого автономного округа по делу № А81-9472/2019 от 02.01.2020 г. – URL: https://clck.ru/kScgp (дата обращения: 04.04.2023).
57. Решение Арбитражного суда Томской области от 16.05.2017 г. по делу № А67-1623/2017. – URL: https://clck.ru/jec2f (дата обращения: 04.04.2023).
58. Решение Арбитражного суда города Москвы по делу № А40-248300/21-5-1672 от 09.02.2022 г. – URL: https://clck.ru/kRTqS (дата обращения: 04.04.2023).

59. Решение Арбитражного суда города Москвы по делу № А40-32033/19-47-287 от 02.10.2020 г. – URL: https://clck.ru/kTCuY (дата обращения: 04.04.2023).
60. Решение Арбитражного суда города Москвы по делу № А40-81328/11 от 07.04.2014 г. – URL: https://clck.ru/nTfSN (дата обращения: 04.04.2023).
61. Решение Арбитражного суда Самарской области по делу № А55-9384/2018 от 26.09.2018. – URL: https://clck.ru/jeqZv (дата обращения: 04.04.2023).
62. Комментарий к Уголовному кодексу Российской Федерации (УК РФ). – 8-е изд., перераб. и доп. – М. : Проспект, 2019. – 800 с.
63. Решение Приморского районного суда города Санкт-Петербурга по делу № 2-38/2019 (2-4158/2018;) ~ М-608/2018 от 11.06.2019. – URL: https://clck.ru/SiN5M (дата обращения: 04.04.2023).
64. Решение Арбитражного суда города Москвы по делу № А40-202764/18-110-1552 от 01.02.2019. – URL: https://clck.ru/jfczi (дата обращения: 04.04.2023).
65. Решение Арбитражного суда Свердловской области по делу № А60-27815/2012 от 01.10.2012. – URL: https://clck.ru/jfedG (дата обращения: 04.04.2023).
66. Решение Арбитражного суда города Москвы по делу № А40-117808/10-12-740 от 30.11.2010. – URL: https://clck.ru/SiNiS (дата обращения: 04.04.2023).
67. Федеральный закон «О коммерческой тайне» от 29.07.2004 № 98-ФЗ. – URL: https://clck.ru/gLnDf (дата обращения: 04.04.2023).
68. Швеция отказалась передать России итоги расследования взрывов Nord Stream. – URL: https://clck.ru/355Tk4 (дата обращения: 06.08.2023).
69. Путин назвал спецслужбы Украины исполнителями теракта на Крымском мосту. – URL: https://clck.ru/355xG6 (дата обращения: 06.08.2023).
70. ЕС ввел потолок цен на российскую нефть: что будет с акциями и рублем. – URL: https://clck.ru/355Tcc (дата обращения: 06.08.2023).
71. Bloomberg узнал об обсуждении почти полного запрета на экспорт в Россию. – URL: https://clck.ru/355xTc (дата обращения: 06.08.2023).
72. Британия запретит импорт российских алмазов и никеля. – URL: https://clck.ru/355xPM (дата обращения: 06.08.2023).
73. Акции золотодобытчиков упали после их включения в SDN-лист США. – URL: https://clck.ru/355xKc (дата обращения: 06.08.2023).

74. Эксперты оценили случаи изъятия автомобилей россиян в Германии. – URL: https://clck.ru/355Thd (дата обращения: 06.08.2023).
75. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). – URL: https://clck.ru/MsKLk (дата обращения: 06.08.2023).
76. Федеральный закон от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации». – URL: https://clck.ru/34sdcd (дата обращения: 06.08.2023).
77. Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ. – URL: https://clck.ru/333aRp (дата обращения: 06.08.2023).
78. Военная доктрина Российской Федерации (утв. Президентом РФ 25.12.2014 № Пр-2976). – URL: https://clck.ru/34su4N (дата обращения: 06.08.2023).
79. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». – URL: https://clck.ru/34MhxC (дата обращения: 06.08.2023).
80. Указ Президента РФ от 13.05.2017 № 208 «О Стратегии экономической безопасности Российской Федерации на период до 2030 года». – URL: https://clck.ru/34YTms (дата обращения: 06.08.2023).
81. Указ Президента РФ от 01.12.2016 № 642 «О Стратегии научно-технологического развития Российской Федерации». – URL: https://clck.ru/34sxVt (дата обращения: 06.08.2023).
82. Указ Президента РФ от 19.04.2017 № 176 «О Стратегии экологической безопасности Российской Федерации на период до 2025 года». – URL: https://clck.ru/34szRF (дата обращения: 06.08.2023).
83. Распоряжение Правительства РФ от 09.06.2020 № 1523-р «Об утверждении Энергетической стратегии Российской Федерации на период до 2035 года». – URL: https://clck.ru/34XEga (дата обращения: 06.08.2023).
84. Концепция общественной безопасности в Российской Федерации (утв. Президентом РФ 14.11.2013 № Пр-2685). – URL: https://clck.ru/34svF5 (дата обращения: 06.08.2023).
85. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ. – URL: https://clck.ru/hS8Je (дата обращения: 06.08.2023).

86. Указ Президента РФ от 21.07.2020 № 474 «О национальных целях развития Российской Федерации на период до 2030 года». – URL: https://clck.ru/34swts (дата обращения: 06.08.2023).
87. Раздел I. Понятие международного права, его сущность и роль в международных отношениях, политике и дипломатии. 1. Устав Организации Объединенных Наций (Принят в г. Сан-Франциско 26.06.1945) (с изм. и доп. от 20.12.1971). – URL: https://clck.ru/34t2Sf (дата обращения: 06.08.2023).
88. Countering America’s Adversaries Through Sanctions Act. – URL: https://clck.ru/qjFCv (дата обращения: 02.07.2023).
89. Военная доктрина Союзного государства. – URL: https://clck.ru/35BSss (дата обращения: 02.07.2023).
90. МИД заявил о моделировании НАТО кибератак по энергосистеме Москвы. – URL: https://clck.ru/35BUYr (дата обращения: 06.08.2023).
91. Власти сообщили о хакерском взломе радиостанций в нескольких регионах. – URL: https://clck.ru/35BUmb (дата обращения: 06.08.2023).
92. РЖД сообщили о массированной хакерской атаке на свой сайт и приложение. – URL: https://clck.ru/35BUdd (дата обращения: 06.08.2023).
93. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ. – URL: https://clck.ru/33sX2n (дата обращения: 18.05.2023).
94. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации от 04.12.2014. – URL: https://clck.ru/34sKk8 (дата обращения: 18.05.2023).
95. Федеральный закон от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». – URL: https://clck.ru/34Y4DM (дата обращения: 18.05.2023).
96. Статья 8.1. «Применение риск-ориентированного подхода при организации государственного контроля (надзора)» Федерального закона от 26.12.2008 № 294-ФЗ (ред. от 08.08.2024) «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». – URL: https://clck.ru/35FZmV (дата обращения: 18.05.2023).
97. Постановление Правительства РФ от 17 августа 2016 г. № 806 «О применении риск-ориентированного подхода при организации отдельных

видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации». – URL: https://clck.ru/34sLb5 (дата обращения: 18.05.2023).

98. Паспорт приоритетной программы «Реформа контрольной и надзорной деятельности» от 21 декабря 2016 г. № 12. – URL: https://clck.ru/34sLmg (дата обращения: 18.05.2023).
99. Федеральный закон от 31 июля 2020 г. № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации». – URL: https://clck.ru/345MHP (дата обращения: 18.05.2023).
100. Глава 5 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FZyn (дата обращения: 18.05.2023).
101. Статья 22 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FZzu (дата обращения: 18.05.2023).
102. Статья 8.1 Федерального закона от 26 декабря 2008 г. № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля». – URL: https://clck.ru/35FZmV (дата обращения: 18.05.2023).
103. Статья 22 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FZzu (дата обращения: 18.05.2023).
104. Часть 6 статьи 22 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FZzu (дата обращения: 18.05.2023).
105. Часть 1 статьи 23 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FaAR (дата обращения: 18.05.2023).
106. Часть 9 статьи 25 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном

контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024) – URL: https://clck.ru/35FaEt (дата обращения: 18.05.2023).

107. Часть 10 статьи 23 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FaAR (дата обращения: 18.05.2023).
108. Постановление Администрации Томской области от 08.07.2022 № 315а «Об утверждении перечней индикаторов риска нарушения обязательных требований при осуществлении регионального государственного контроля (надзора) за применением цен на лекарственные препараты, включенные в перечень жизненно необходимых и важнейших лекарственных препаратов, регионального государственного контроля (надзора) в сфере перевозок пассажиров и багажа легковым такси, регионального государственного контроля (надзора) в области розничной продажи алкогольной и спиртосодержащей продукции на территории Томской области». – URL: https://clck.ru/34sNmf (дата обращения: 18.05.2023).
109. Часть 1 статьи 24 Федерального закона от 31.07.2020 № 248-ФЗ (ред. от 08.08.2024) «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» (с изм. и доп., вступ. в силу с 01.09.2024). – URL: https://clck.ru/35FaUP (дата обращения: 18.05.2023).
110. Аналитический центр при Правительстве Российской Федерации. Высокая доля расторжения контрактов в рамках закона о контрактной системе. – URL: https://clck.ru/gfMiA (дата обращения: 18.05.2023).
111. Приказ Минкомсвязи России от 22.09.2020 № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных». – URL: https://clck.ru/34Pa7P (дата обращения: 18.05.2023).
112. Решение Арбитражного суда города Москвы по делу № А40-263677/21-51-1834 от 27.07.2022. – URL: https://clck.ru/32Rowo (дата обращения: 18.05.2023).
113. Решение Арбитражного суда Алтайского края по делу № А03-5595/2021 от 04.08.2022. – URL: https://clck.ru/32RsSP (дата обращения: 18.05.2023).
114. Решение Арбитражного суда Санкт-Петербурга и Ленинградской области по делу № А56-107933/2019 от 31.03.2021. – URL: https://clck.ru/32S4yT (дата обращения: 18.05.2023).

115. Приказ Минцифры России от 17.12.2020 № 715 «Об утверждении типовых условий контрактов на выполнение работ по созданию и (или) развитию (модернизации) государственных (муниципальных) и (или) иных информационных систем». – URL: https://clck.ru/34PZuq (дата обращения: 18.05.2023).
116. Решение Арбитражного суда Алтайского края по делу № А03-14616/2020 от 21.10.2021. – URL: https://clck.ru/32RtCX (дата обращения: 18.05.2023).
117. Департамент государственного заказа Томской области. – URL: https://dgz.tomsk.gov.ru/ (дата обращения: 18.05.2023).
118. Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ. – URL: https://clck.ru/Nh6GG (дата обращения: 18.05.2023).
119. Федеральный закон «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 № 223-ФЗ. – URL: https://clck.ru/339idK (дата обращения: 18.05.2023).
120. Постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд». – URL: https://clck.ru/34N4xx (дата обращения: 18.05.2023).
121. Официальный сайт единого реестра российских программ для электронных вычислительных машин и баз данных. – URL: https://reestr.digital.gov.ru/ (дата обращения: 18.05.2023).
122. Постановление Правительства РФ от 31.12.2021 № 2604 «Об оценке заявок на участие в закупке товаров, работ, услуг для обеспечения государственных и муниципальных нужд». – URL: https://clck.ru/33D86G (дата обращения: 18.05.2023).
123. ГОСТ Р 66.0.01-2017. Национальный стандарт Российской Федерации. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Общие положения, требования и руководящие принципы. – 2018. – 34 с.
124. Официальный сайт Технического комитета по стандартизации. Оценка опыта и деловой репутации предприятий. – URL: https://tk066.ru/ (дата обращения: 18.05.2023).

125. Национальный стандарт Российской Федерации ГОСТ Р 66.1.01-2015. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации лиц, осуществляющих архитектурно-строительное проектирование. – М. : Стандартинформ, 2015. – 12 с.
126. Национальный стандарт Российской Федерации ГОСТ Р 66.1.02-2015. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации лиц, осуществляющих инженерные изыскания. – М. : Стандартинформ, 2020. – 12 с.
127. Национальный стандарт Российской Федерации ГОСТ Р 66.1.03-2016. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации строительных организаций. – М. : Стандартинформ, 2020. – 16 с.
128. Национальный стандарт Российской Федерации ГОСТ Р 66.9.01-2015. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации лиц, производящих и реализующих пожарно-техническую продукцию. – М. : Стандартинформ, 2016. – 19 с.
129. Национальный стандарт Российской Федерации ГОСТ Р 66.9.02-2015. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации лиц, выполняющих работы (оказывающих услуги) в области обеспечения пожарной безопасности объектов защиты. – М. : Стандартинформ, 2020. – 12 с.
130. Национальный стандарт Российской Федерации ГОСТ Р 66.9.03-2016. Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации организаций, выполняющих перевозки крупногабаритных тяжеловесных грузов. – М. : Стандартинформ, 2020. – 16 с.
131. Национальный стандарт Российской Федерации ГОСТ Р 66.9.04-2017 Оценка опыта и деловой репутации субъектов предпринимательской деятельности. Национальная система стандартов. Оценка опыта и деловой репутации охранных организаций. – М. : Стандартинформ, 2020. – 14 с.

132. Распоряжение Правительства РФ от 21.03.2016 № 471-р «О перечне товаров, работ, услуг, в случае осуществления закупок которых заказчик обязан проводить аукцион в электронной форме (электронный аукцион)». – URL: https://clck.ru/33D8K3 (дата обращения: 18.05.2023).
133. Федеральный закон от 28.04.2023 № 154-ФЗ «О внесении изменений в Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд». – URL: https://clck.ru/34PdQ5 (дата обращения: 18.05.2023).
134. Никитина А. О. Проблемы при проведении закупочных процедур в соответствии с Федеральным законом № 44-ФЗ // Право и правопорядок в фокусе научных исследований, 2022. – С. 183–186.
135. Постановление Правительства РФ от 10.05.2018 № 564 «О взимании операторами электронных площадок, операторами специализированных электронных площадок платы при проведении электронной процедуры, закрытой электронной процедуры и установлении ее предельных размеров». – URL: https://clck.ru/33D8Zw (дата обращения: 18.05.2023).
136. Евграфов С. А. Проблемы реализации Федерального закона от 05.04.2013 № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» на муниципальном уровне // Актуальные вопросы местного самоуправления в Российской Федерации, 2021. – С. 21–26.
137. Шмелева М. В. Проблемы понятийного наполнения сферы государственных закупок и пути их решения // Журнал предпринимательского и корпоративного права, 2020. – № 1. – С. 12–15.
138. Решение Арбитражного суда Хабаровского края по делу № А73-6308/2022 от 28.06.2022. – URL: https://clck.ru/32RZZe (дата обращения: 18.05.2023).
139. Науразбаева А. А. Некоторые проблемы нормативно-правового регулирования государственных и муниципальных закупок на современном этапе // Тенденции развития науки и образования, 2022. – № 86-7. – С. 93–96.
140. Директива № 2014/24/ЕС Европейского парламента и Совета Европейского Союза «О государственных закупках и об отмене Директивы 2004/18/ЕС». – URL: https://clck.ru/32U2Mf (дата обращения: 18.05.2023).

141. Бюджетный кодекс Российской Федерации от 31.07.1998 № 145-ФЗ. – URL: https://clck.ru/Z3dQB (дата обращения: 18.05.2023).
142. Bay A. F., Skitmore M. Project Management Maturity: Some Results from Indonesia // Journal of Building and Construction Management, 2006. – Vol. 10. – P. 2–15.

Глоссарий

Аукцион – способ определения подрядчика (исполнителя, поставщика), где победителем признается тот участник закупки, который предлагает наиболее низкую цену контракта.

Валютные риски – вероятность денежных потерь при конвертации одной валюты в другую валюту.

Вторичные риски – вероятные события, которые могут наступить несмотря на проведение профилактических мер плана А.

Дефляционные риски – вероятность усиления реальной покупательной способности денег.

Запрос котировок в электронной форме – это способ определения подрядчика (исполнителя, поставщика), где победителем признается тот участник закупки, который предлагает наиболее низкую цену контракта.

Имущественные риски – вероятность потери имущества по причине пожара, кражи, диверсии, халатности и др.

Инвестиционные риски – вероятность неполучения (получения) ожидаемого коммерческого эффекта.

Инфляционные риски – вероятность обесценивания реальной покупательной способности денег.

Источники риска – объекты, имеющие потенциал создавать события, способные оказывать влияние на процесс достижения целей.

Качественные методы – методы, в которых используются экспертные мнения для оценивания характеристик вероятностей и влияний рисков.

Количественные методы – методы, использующие математический аппарат для прогнозирования вероятности материализации рисков и возможного влияния в случае их наступления.

Коммерческие риски – непредвиденные расходы (доходы), которые могут быть получены во время ведения финансово-хозяйственной деятельности организаций.

Коммерческая тайна – 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.

Конкурс – способ определения подрядчика (исполнителя, поставщика), где победителем признается тот участник закупки, который предлагает лучшие условия контракта.

Макрориски – глобальные риски, последствия от материализации которых отражаются на всех экономических агентах.

Мезориски – риски, последствия от наступления которых влияют на определенный регион или отрасль экономики.

Микрориски (*предпринимательские риски*) – вероятные события, наступление которых оказывает влияние на экономическую деятельность конкретных экономических агентов.

Негативный риск – вероятное событие, которое может привести к наступлению проблемных последствий.

Нейтральный риск – вероятное событие, которое не приводит к проблемным и/или благоприятным последствиям.

Общественные риски – возможные события, природа которых имеет социально-общественный характер.

Оценка риска причинения вреда (*ущерба*) – деятельность контрольного (надзорного) органа по определению вероятности возникновения риска и масштаба вреда (ущерба) для охраняемых законом ценностей.

Позитивный риск – вероятное событие, которое может привести к наступлению благоприятных последствий.

Политические риски – вероятные события, которые связаны с деятельностью органов государственной власти.

Последствия от наступления риска – новые обстоятельства, возникающие в результате материализации риска.

Природно-естественные риски (*экологические риски*) – риски, связанные с силами природы (например, землетрясение, наводнение, ураган, пожар, экстремально высокие или низкие температуры и др.).

Причины риска – условия, имеющие потенциал создавать события, которые способны оказывать влияние на процесс достижения целей.

Производственные риски – возможный ущерб от остановки производства, гибели или повреждения оборудования, полученного брака продукции и др.

Риск – это вероятное событие, проистекающее из конкретных источников, материализация которого может привести к наступлению благоприятных/проблемных последствий.

Риски ликвидности – вероятность неисполнения денежных обязательств в установленном объеме и в согласованный срок.

Риски-невидимки – скрытые риски, которые не были обнаружены во время идентификации. Опасность данных рисков заключается в их неожиданном наступлении.

Риск причинения вреда (*ущерба*) – вероятность наступления событий, следствием которых может стать причинение вреда (ущерба) различного масштаба и тяжести охраняемым законом ценностям.

Рыночные риски – риски снижения денежной стоимости капитала, ценных бумаг или портфеля вследствие изменения цен и ставок на рынке.

Смешанный риск – вероятное событие, наступление которого приводит одновременно к проблемным и благоприятным последствиям.

Спекулятивные риски – вероятные события, которые могут привести к наступлению как проблемных, так и благоприятных последствий.

Технологические риски – риски внешней среды, природа которых имеет технологический характер.

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.

Триггерные условия (*триггеры*) – в управлении рисками это условия, события или ситуации, которые указывают на скорую материализацию рисков.

Универсальные риски – вероятные события, которые актуальны для любой сделки и проекта независимо от его масштаба, сложности, длительности, типа, способов управления и численности участников команды.

Управление рисками – совокупность принципов, скоординированных действий и процессов по оценке, воздействию, мониторингу и контролю рисков.

Управление риском причинения вреда (*ущерба*) – осуществление на основе оценки рисков причинения вреда (ущерба) профилактических мероприятий и контрольных (надзорных) мероприятий в целях обеспечения допустимого уровня риска причинения вреда (ущерба) в соответствующей сфере деятельности.

Управленческий резерв – 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).

Финансовые риски – вероятность получения убытков (прибыли).

Чистые риски – вероятные события, которые могут привести к наступлению проблемных последствий.

Экономические риски – вероятные события, природа которых имеет экономический характер.

Приложение А
Реестр 170 универсальных рисков

№	Название риска
Коммерческие риски (бизнес-риски)	
Риски, связанные с пользователем (*клиентом*)	
1	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям пользователя (клиента)
2	Риск низкой вовлеченности пользователя (клиента) в процесс выполнения работы (оказания услуги, поставки товара)
Риски, связанные с коммерческим эффектом	
3	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не принесет ожидаемый коммерческий эффект
Риски, связанные с конкурентами	
4	Риск того, что конкуренты будут оказывать влияние на ход выполнения работы (оказания услуги, поставки товара)
Риски, связанные с товарами-субститутами	
5	Риск того, что товары-субституты будут оказывать влияние на ход выполнения работы (оказания услуги, поставки товара)
Комплаенс-риски	
Риски, связанные с заказчиком	
6	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям заказчика
7	Риск того, что заказчик откажется принимать и/или оплачивать выполненную работу (оказанную услугу, поставленный товар)
8	Риск того, что будет просрочка оплаты за выполненную подрядчиком работу (оказанную исполнителем услугу, поставленный поставщиком товар)
9	Риск судебного иска от заказчика
10	Риск признания сделки недействительной
11	Риск того, что будет невозможно досрочно и в одностороннем порядке расторгнуть сделку
12	Риск того, что существенные условия сделки будут сформулированы и формализованы в тексте договора неточно и/или некорректно
13	Риск неверной квалификации вида сделки
14	Риск допущения неточных и/или некорректных формулировок в тексте договора
15	Риск того, что между сторонами будет не учтен порядок распределения экономии, которая может быть получена по факту выполненной работы (оказанной услуги, поставленного товара)
16	Риск отсутствия связи с заказчиком
17	Риск того, что заказчик не предоставит и/или будет предоставлять с большой задержкой информацию, необходимую для выполнения работы (оказания услуги, поставки товара)
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
19	Риск того, что спецификация (устав, техническое задание и/или другая документация) будет неполной, недостоверной и/или не соответствовать требованиям национальных стандартов

№	Название риска
20	Риск низкой вовлеченности заказчика в процесс выполнения работы (оказания услуги, поставки товара)
21	Риск отсутствия у заказчика корпоративной культуры, работников и опыта ведения деятельности в едином информационном пространстве с использованием информационных систем
22	Риск того, что у заказчика будут отсутствовать отлаженные корпоративные процедуры по информационному взаимодействию и совместной работе его подразделений
23	Риск отсутствия ключевых и квалифицированных специалистов на стороне заказчика (например, отсутствие лиц, которые могут определить требования к информационным системам)
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
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*)	
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.)
27	Риск того, что подрядчик (исполнитель, поставщик) будет утаивать информацию о реальном положении дел от заказчика и/или искажать ее
28	Риск отсутствия общего виденья конечного продукта у заинтересованных сторон
29	Риск того, что в процессе выполнения работы (оказания услуги, поставки товара) подрядчик (исполнитель, поставщик) не сможет своими силами исполнить заявленные в договоре обязательства
30	Риск выявления подрядчиком (исполнителем, поставщиком) скрытых, не обнаруженных на этапе планирования источников дополнительных затрат
31	Риск распространения сведений, порочащих деловую репутацию подрядчика (исполнителя, поставщика)
32	Риск судебного иска от подрядчика (исполнителя, поставщика)
Риски, связанные с исключительным правом на результат интеллектуальной деятельности (*РИД*)	
33	Риск нарушения исключительных прав (авторских прав) на РИД
34	Риск взыскания правообладателем (автором) вознаграждения за нарушение исключительных прав (авторских прав) на РИД
35	Риск того, что правообладатель (автор) запретит использовать РИД
36	Риск невозможности признания исключительного права (авторского права) на РИД за правообладателем (автором)
37	Риск создания нежелательного производного произведения
38	Риск ограничения для последующих сублицензионных договоров
39	Риск расторжения договора в «сублицензионной цепочке» договоров
Риски, связанные с субподрядчиком (*субисполнителем*, *субпоставщиком*)	
40	Риск отсутствия связи с субподрядчиком (субисполнителем, субпоставщиком)
41	Риск того, что полученный субподрядчиком (субисполнителем, субпоставщиком) результат (оказанная услуга, поставленный товар) не будет соответствовать ожиданиям заинтересованных сторон
42	Риск судебного иска от субподрядчика (субисполнителя, субпоставщика)

№	Название риска
Риски, связанные с имуществом	
43	Риск гибели и/или повреждения электронного оборудования (компьютеров, серверов и др.) и другого имущества в результате пожара, затопления водой и др.
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	
45	Риск промышленного шпионажа
46	Риск утечки конфиденциальных данных
47	Риск ограбления
Риски государственных (*муниципальных*) *контрактов*	
48	Риск признания недействительными государственного (муниципального) контракта (доступ к исполнению контракта без конкурентной борьбы)
49	Риск отказа от заключения государственного (муниципального) контракта
50	Риск того, что государственный (муниципальный) заказчик откажется принимать и (или) оплачивать выполненную работу (оказанную услугу, поставленный товар)
51	Риск того, что выполненная работа (оказанная услуга, поставленный товар) не будет соответствовать требованиям государственного (муниципального) контракта
52	Риск того, что государственный (муниципальный) заказчик в одностороннем порядке откажется от исполнения государственного (муниципального) контракта
Проектные риски	
Риски, связанные с руководителем проекта	
53	Риск того, что руководитель проекта допустит ошибку при оценивании стоимости проектных работ
54	Риск того, что руководитель проекта допустит ошибку при оценивании длительности проектных работ
55	Риск неучета отпусков и государственных праздников при создании плана проекта
56	Риск того, что руководитель проекта допустит ошибку при оценивании ресурсов, которые необходимы для выполнения проектных работ
57	Риск нерационального расходования ограниченных ресурсов проекта
58	Риск отсутствия знаний, навыков и опыта у руководителя проекта
59	Риск ухода руководителя проекта из проекта
60	Риск низкой производительности труда у руководителя проекта
61	Риск отсутствия заинтересованности руководителя проекта в успешном завершении проекта
62	Риск занятости руководителя проекта в других проектах
63	Риск неправильного ранжирования задач руководителем проекта
64	Риск завышения качества руководителем проекта
65	Риск отсутствия в проекте инструментария управления проектом (например, PRINCE2, SCRUM и др.)
66	Риск отсутствия ресурсов, необходимых для выполнения проектных работ
67	Риск того, что по факту проектные работы окажутся значительно сложнее, чем предполагалось изначально
68	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений
69	Риск отсутствия резервов, необходимых для принятия материализовавшихся рисков
70	Риск потери и/или отсутствия контроля руководителем проекта

№	Название риска
71	Риск конфликта между руководителем проекта и заинтересованными сторонами (например, заказчиком, участниками команды и др.)
72	Риск того, что будет потеряна информация о материализовавшихся рисках, которая может потребоваться руководителю проекта в последующих проектах
73	Риск привлечения в проект руководителя проекта, который имеет профессиональное образование в области управления проектами
74	Риск привлечения в проект руководителя проекта, который имеет опыт управления проектами более двух лет
75	Риск того, что руководитель проекта будет самостоятельно формировать команду проекта
76	Риск изменения содержания проекта
77	Риск изменения длительности проекта
78	Риск изменения стоимости проекта
79	Риск изменения качества проекта
80	Риск декомпозиции большого проекта на малые проекты (длительностью не более четырех месяцев)
Риски, связанные с участниками проекта	
81	Риск простоя трудовых ресурсов
82	Риск конфликта интересов между заинтересованными сторонами
83	Риск того, что не все заинтересованные стороны будут выявлены
84	Риск ухода на больничный участника проекта
85	Риск допущения ошибок участниками проекта при реализации проекта
86	Риск значительной временной задержки в получении ответов на задаваемые вопросы между участниками проекта
87	Риск эффекта Кассандры, т. е. будет наблюдаться переизбыток каналов коммуникации, доносящих актуальную информацию
88	Риск того, что фактическое время работы участников проектов будет менее 8 ч. в день
89	Риск отсутствия знаний, навыков и опыта у участников проекта, необходимых для реализации требований
90	Риск ухода ключевого участника проекта из проекта
91	Риск перегрузки трудовых ресурсов (например, из-за переработки, работы сверхурочно и др.)
92	Риск того, что участники проекта будут неправильно оценивать трудозатраты, которые необходимы для выполнения проектных работ
93	Риск того, что участники проекта будут неправильно декомпозировать проектные работы
94	Риск занятости участников проекта в других проектах
95	Риск изменения состава участников проекта в процессе реализации проекта
96	Риск непонимания участниками проекта того, какой результат должен быть получен по завершении проекта
97	Риск нескоординированных действий участников проекта
98	Риск низкой производительности труда у участников проекта
99	Риск отсутствия заинтересованности у участников проекта в успешном завершении проекта
100	Риск негативной социально-психологической атмосферы
101	Риск недостатка коммуникации между участниками проекта
102	Риск использования устаревших технологий участниками проекта
103	Риск привлечения в проект высококвалифицированного работника
104	Риск того, что численность участников проекта не будет превышать 6 человек

№	Название риска
105	Риск коллаборации между руководителем и участниками проекта (групповая выработка решений, реализация индивидуальных идей и др.)
106	Риск привлечения в проект сторонних экспертов и советников
107	Риск того, что согласованные заинтересованными сторонами изменения будут утеряны
108	Риск того, что запрошенная функциональность программы для ЭВМ будет реализована, но никто не будет ее использовать
Риски, связанные с оборудованием	
109	Риск отключения электричества
110	Риск отключения интернета
111	Риск применения ранее не используемых технологий участниками проекта
112	Риск поломки оборудования
Риски внешней среды	
Риски, связанные с экономикой	
113	Риск изменения цен на нефть
114	Риск изменения цен на газ
115	Риск изменения цен на металлы
116	Риск изменения цен на уголь
117	Риск изменения цен на зерно
118	Риск дефицита (профицита) федерального бюджета
119	Риск изменения курса валют
120	Риск внесения изменений в Федеральный закон «О федеральном бюджете»
121	Риск изменения размера государственного долга
122	Риск изменения темпов инфляции
123	Риск изменения ключевой ставки Банка России
124	Риск изменения процентов кредитных и депозитных ставок
125	Риск изменения темпов роста экономики
126	Риск изменения уровня жизни населения
127	Риск изменения фондовых индексов
128	Риск дефолта
129	Риск экономического кризиса
Риски, связанные с обществом	
130	Риск изменения уровня смертности
131	Риск изменения уровня рождаемости
132	Риск изменения численности населения
133	Риск того, что на рынке труда будут отсутствовать квалифицированные кадры
134	Риск социальной напряженности
135	Риск изменения уровня образования
136	Риск изменения уровня медицины
137	Риск изменения уровня преступности
138	Риск изменения уровня миграции
139	Риск голода
Риски, связанные с политикой	
140	Риск изменения геополитического давления
141	Риск расширения альянса НАТО
142	Риск военного конфликта
143	Риск террористического акта
144	Риск изменения норм действующего законодательства
145	Риск нарушения норм действующего законодательства

№	Название риска
146	Риск материализации обстоятельств непреодолимой силы, которые окажут значительное влияние на ход выполнения работ (оказания услуг, поставки товаров)
147	Риск интеграции РФ с внешними субъектами
148	Риск государственного переворота
149	Риск национализации и экспроприации имущества
150	Риск массовых беспорядков
Риски, связанные с окружающей средой	
151	Риск нехватки природных ресурсов
152	Риск изменения климата
153	Риск загрязнения окружающей среды
154	Риск пандемии
155	Риск наводнения
156	Риск радиоактивного заражения
157	Риск тайфуна
158	Риск землетрясения
Риски, связанные с техникой и технологиями	
159	Риск атаки искусственного интеллекта (ИИ)
160	Риск отключения глобальной компьютерной сети Интернет
161	Риск атаки на критическую инфраструктуру
162	Риск атаки на критическую информационную инфраструктуру (КИИ)
163	Риск заражения КИИ вредоносным программным обеспечением
164	Риск частичного и/или полного отказа в обслуживании КИИ
165	Риск использования новой технологии
166	Риск неправомерного доступа, копирования, предоставления и/или распространения конфиденциальной информации
167	Риск неправомерного уничтожения и/или модификации конфиденциальной информации
168	Риск неправомерного блокирования конфиденциальной информации
169	Риск поломки оборудования из-за отсутствия импортных комплектующих
170	Риск нехватки электроэнергии

Учебное издание

Валентин Сергеевич Николаенко

РИСК-МЕНЕДЖМЕНТ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Учебное пособие

Корректор А. Н. Миронова
Оригинал-макет Т. Н. Мосуновой

Подписано к публикации 05.11.2024.

Издательство «Эль Контент»
634061, г. Томск, ул. Киевская, д. 57, оф. 27

ISBN 978-5-4332-0311-2