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

В.С. Николаенко

БЕЗУПРЕЧНЫЙ РИСК-МЕНЕДЖМЕНТ В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Учебное пособие

Томск
Издательство ТУСУРа
2025

УДК 352:005.334(075.8)
ББК 65.050.2я73+65.290-2я73
Н634

Рецензенты:

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

Соснин В.Н., Генеральный директор ООО «КОНТЕК-СОФТ»

Николаенко, Валентин Сергеевич

Н634 Безупречный риск-менеджмент в системе государственного и муниципального управления Российской Федерации: учеб. пособие / В.С. Николаенко. – Томск: Изд-во Томск. гос. ун-та систем управления и радиоэлектроники, 2025. – 200 с.

ISBN 978-5-908033-11-4

Представлены теоретические и практические аспекты управления различными видами рисков (негативные, позитивные, проектные, комплаенс-риски, риски внешней среды и др.) в системе государственного и муниципального управления. Описан инструментарий оценки, мониторинга и контроля рисков, а также механизм воздействия на риски и их документального сопровождения.

Предназначено для государственных и муниципальных служащих, руководителей структурных подразделений организаций и учреждений, а также и студентов высших учебных заведений, обучающихся по направлениям подготовки в областях государственного и муниципального управления, экономики и менеджмента.

УДК 352:005.334(075.8)
ББК 65.050.2я73+65.290-2я73

ISBN 978-5-908033-11-4

Оглавление

Введение …… 4

1. КЛЮЧЕВЫЕ АСПЕКТЫ РИСК-МЕНЕДЖМЕНТА

1.1. Риски как объект управления …… 7

1.1.1. Формирование теории управления рисками: история развития, основные понятия, правовая и нормативная база …… 7

1.1.2. Классификация рисков …… 26

1.2. Процессы управления рисками: методы, инструменты …… 34

1.2.1. Анализ внутренней и внешней среды объектов риска 34

1.2.2. Идентификация рисков …….. 37

1.2.3. Анализ рисков ……. 43

1.2.4. Оценивание рисков ……. 47

1.2.5. Воздействие на риски ……. 57

1.3. Механизмы митигации рисков …… 63

1.3.1. Элиминирование рисков: ковенанты договора ……. 63

1.3.2. Страхование рисков …… 78

2. ОСОБЕННОСТИ РИСК-МЕНЕДЖМЕНТА В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

2.1. Оценка угроз национальной безопасности Российской Федерации ……. 86

2.2. Управление рисками при осуществлении государственного и муниципального контроля (надзора) …..... 98

2.3. Риски в сфере закупок товаров, работ и/или услуг для обеспечения государственных и муниципальных нужд 107

2.4. Риски внешней среды: риски изменения цены на нефть и газ 126

2.5. Особенности риск-менеджмента в системе государственного и муниципального управления за рубежом …… 134

Заключение …… 145

Литература …… 146

Глоссарий …….. 161

Приложение А. Риски внешней среды: 2025 год …….. 166

Приложение Б. Реестр универсальных рисков …….. 172

Приложение В. Примеры ковенантов в договоре подряда …… 184

Приложение Г. Угрозы в сферах экономической, военной и информационной безопасности …… 195

Введение

Необходимость внедрения и распространения инструментария управления рисками в системе государственного и муниципального управления Российской Федерации во многом обусловлена усиливающимся геополитическим давлением, которое создает каскад новых нежелательных рисков и негативных последствий в случаях их материализации. Яркими примерами наступления подобных последствий являются диверсии на подводных газопроводах «Северный поток-1» и «Северный поток-2», 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, Федерального закона США «О противодействии противникам Америки посредством санкций» (CAATSA, Countering America's Adversaries Through Sanctions Act), принятого Правительством США 24 июля 2017 г., показывает, что геополитические противники намерены вести системную и планомерную работу, направленную против Российской Федерации и ее граждан, создавая новые угрозы для национальной безопасности [1]. Для элиминирования[1] подобных нежелательных рисков отечественным законодателем актуализируются, разрабатываются и принимаются проактивные нормативные акты, доктрины, стратегии и национальные стандарты.

Документами, закрепляющими механизм управления рисками в системе государственного и муниципального РФ, являются федеральные законы «О стратегическом планировании в Российской Федерации» и «О безопасности», Стратегия национальной безопасности, Военная доктрина РФ, Доктрина информационной безопасности РФ, Стратегия экономической безопасности России до 2030 г., Стратегия научно-технологического развития РФ, Стратегия экологической безопасности РФ на период до 2025 г. и др.

---

[1] **Элиминирование рисков** (лат. *eliminare* — устранять, ликвидировать) — изменение вероятности наступления рисков и/или их влияния в случаях материализации.

Системообразующие механизмы управления рисками, методы оценки и способы воздействия на них законодатель закрепил в национальных стандартах (например, ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» [2], ГОСТ Р 58771-2019 «Менеджмент риска. Технологии оценки риска» [3] и др.

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, структурных подразделений организаций и учреждений повысить шансы на достижение запланированных стратегических, тактических, операционных и проектных целей.

В первом разделе пособия рассмотрены теоретические аспекты управления рисками: основные понятия рисков и их классификация, нормативные и правовые документы по регулированию процессов управления рисками, особенности митигации рисков. Подробно анализируются процессы управления рисками, методы оценки и воздействия на риски. Представлен механизм страхования рисков и примеры ковенантов[1] договора, элиминирующие риски.

В приложениях к пособию продемонстрирован перечень универсальных рисков (коммерческих, комплаенс-рисков[2], проектных рисков и рисков внешней среды).

---

[1] **Ковенант** — обязательство совершить какое-либо действие или воздержаться от его совершения.

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

Во втором разделе описываются: механизм управления рисками в системе государственного и муниципального управления Российской Федерации; митигация рисков при осуществлении государственного и муниципального контроля (надзора); ключевые угрозы национальной безопасности Российской Федерации; риски в сфере закупок товаров, работ/услуг для обеспечения государственных и муниципальных нужд; риски внешней среды; особенности риск-менеджмента в системе государственного и муниципального управления за рубежом.

Автор настоящего пособия желает читателям безрисковых проектов, безопасного исполнения контрактов и успешного достижения запланированных целей.

1. КЛЮЧЕВЫЕ АСПЕКТЫ РИСК-МЕНЕДЖМЕНТА

1.1. Риски как объект управления

1.1.1. Формирование теории управления рисками: история развития, основные понятия, правовая и нормативная база

Можно с уверенностью утверждать, что истоки управления рисками берут свое начало в религиозных учениях, философии, математике и теории вероятностей (табл. 1.1) [4]. Считается, что первое формальное закрепление понятия «риск» произошло благодаря азартным играм, в которых активно применялась концепция теории вероятностей. Ведущую роль в развитии данного направления сыграл крупный алгебраист XVI в. Джироламо Кардано, посвятивший анализу игр содержательную монографию «Книга об игре в кости» (1526 г.).

В 1654 г. Паскаль Б. и Ферма П. пришли к пониманию математического ожидания, сформулировав теоремы сложения и умножения вероятностей. Их выводы легли в основу трудов Гюйгенса Х., вышедших в свет в 1657 г. под названием «О расчетах в азартной игре или рассмотренная математически стоимость всех шансов при азартных играх в карты, кости, при заключении пари, при участии в лотерее и т. д.» [5].

Конец XVII в. является новым витком в развитии теории управления рисками, который сопровождается выходом первых трудов по статистике. В 1693 г. были опубликованы научные работы Галля Э., ставшие основой для института страхования рисков, и труды страхового агента Ллойда Э., заключившего первые договоры страхования морских рисков [6].

В XVIII в. активно разрабатываются экономические теории, оказавшие влияние на понимание природы риска. Например, Смит А. в работе «Исследование о природе и причинах богатства народов» пришел к выводу, что представители рисковых профессий, таких как врач и юрист, получают более высокое вознаграждение, чем представители профессий с низким уровнем риска [7].

Таблица 1.1

Хронология развития теории управления рисками

Год издания	Наименования научных трудов, нормативных документов и разработок по управлению рисками
1526	Кардано Дж. «Книга об игре в кости»
1654	Паскаль Б. и Ферма П. «Математическое ожидание и теорема сложения и умножения вероятностей»
1657	Гюйгенс Х. «О расчетах в азартной игре или рассмотренная математически стоимость всех шансов при азартных играх в карты, кости, при заключении пари, при участии в лотерее и т. д.»
1693	Галль Э. и Ллойд Э. «Труды о страховании рисков»
1848	Милль Д. «Основы политической экономии с некоторыми приложениями их к социальной философии»
1850	Фон Тюнен И.Г. «Изолированное государство в его отношении к сельскому хозяйству и национальной экономии. Исследование о влиянии хлебных цен, богатства почвы и налогов на земледелие»
1921	Найт Ф. «Риск, неопределенность и прибыль»
1953	Нейман Дж., Моргенштерн О. «Теория игр и экономическое поведение»
1988	Соглашение «Базель I»
1992	COSO «International Control – Integrated Framework»
1996	Project Management Body of Knowledge. First Edition
1999	Разработка стандарта управления рисками AS/NZS 4360:1999
2000	Project Management Body of Knowledge. Second Edition
2002	Разработка стандартов управления рисками FERMA, IRM, AIRMIC и ALARM
2004	Соглашение «Базель II»
2004	Project Management Body of Knowledge. Third Edition
2004	Создание модели «COSO ERM»
2005	Пособие PRMIA
2008	Создание модели зрелости в плате управления рисками RIMS
2008	Project Management Body of Knowledge. Fourth Edition
2008	Руководство по передовым стандартам в области управления рисками. Австралийское правительство
2008	BS 311000:2008 «Свод практик для риск-менеджмента»
2009	ISO 31000:2009. «Risk Management – Principles and Guidelines»
2010	ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство

Окончание табл. 1.1

Год издания	Наименования научных трудов, нормативных документов и разработок по управлению рисками
2010	Management of Risk: Guidance for Practitioners (M_o_R®)
2011	Федеральный закон № 402-ФЗ от 06.12.2011 «О бухгалтерском учете» (вступил в силу с 01.01.2013 г. в РФ): ст. 19 «Экономический субъект обязан организовать и осуществлять внутренний контроль совершаемых фактов хозяйственной жизни», одним из элементов которого является оценка рисков
2013	Project Management Body of Knowledge. Firth Edition
2017	Усовершенствование модели COSO ERM «Enterprise Risk Management. Integrating with Strategy and Performance»
2017	Project Management Body of Knowledge. Sixth Edition
2017	PRojects IN Controlled Environments (PRINCE2®)
2020	О рекомендациях по организации управления рисками, внутреннего контроля, внутреннего аудита, работы комитета совета директоров (наблюдательного совета) по аудиту в публичных акционерных обществах: информационное письмо Банка России от 01.10.2020 г. № ИН-06-28/143

Английский экономист Милль Д.С. в работе «Основы политической экономии с некоторыми приложениями их к социальной философии» в 1848 г. ввел в оборот термин «плата за риск» [8].

Тюнен И.Г. в 1850 г. опубликовал труд «Изолированное государство в его отношении к сельскому хозяйству и национальной экономии. Исследование о влиянии хлебных цен, богатства почвы и налогов на земледелие», где впервые описал сущность инновационных рисков [9]. Главной идеей данной работы стала классификация рисков на страхуемые риски, под которые могут быть выделены резервы, и нестрахуемые риски, где предприниматель полностью принимает ущерб на себя.

По мере развития теории управления рисками происходило формирование и расширение понятийного аппарата риск-менеджмента. В частности, в 1921 г., развивая идеи Тюнена И. о прибыли и риске, Найт Ф. впервые **разделил понятия «риск» и «неопределенность»**. По его мнению, ***риск*** является «***измеримой неопределенностью***», которой можно управлять» [10].

Новый взгляд на риск предложил Кейнс Дж. М., добавив в деловой оборот такие понятия, как «*риск кредитора*», «*риск заемщика*», «*риск обесценивания денег*» и др. Кроме того, в своем труде «Трактат о вероятности» Кейнс использует такое понятие, как «*издержки рисков*» [11].

Важным моментом в понимании природы риска стало осознание того, что неопределенность наступает из-за неизвестных желаний и предпочтений людей. Эта концепция составила основу теории игр и нашла отражение в книге Моргенштерна О. и Неймана Дж. и «Теория игр и экономическое поведение» (1953 г.) [12].

В 1988 г. банковский сектор принял консолидированное решение о необходимости регулирования деятельности финансовых институтов в части управления рисками, в связи с чем Базельским комитетом по банковскому надзору был издан документ «Базель I», в котором рассматривались вопросы о достаточности капитала банков для покрытия расходов по кредитным рискам [13]. Данный свод правил — это первый документ, в котором зафиксирован механизм по оценке, воздействию, мониторингу и контролю рисков.

Управление рисками получило развитие и в проектной деятельности. Например, Project Management Institute (PMI) в 1996 г. был выпущен в свет свод знаний проектного управления PMBoK® Guide [14, 15, 16], который с тех пор каждые 4–6 лет корректируется, обновляется и дополняется новой информацией. С первого издания PMI уделяет управлению рисками особое внимание. Это во многом связано с тем, что элиминирование рисков значительно повышает шансы на успешное завершение проектов. По этой причине «*реестр рисков*» и «*план управления рисками*» являются важнейшими проектными документами наравне с уставом проекта, иерархической структурой работ (ИСР), планом управления стоимостью и др.

В 2004 г. частной некоммерческой организацией COSO выпущена первая версия собственного стандарта по управлению рисками «Управление рисками организации. Интеграция со стратегией и эффективностью деятельности» (COSO ERM — The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management») [17]. Затем в 2017 г. была

опубликована обновленная версия «Enterprise Risk Management. Integrating with Strategy and Performance».

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

Американская школа управления рисками. Одна из первых ссылок на термин «управление рисками» встречается в американском издании «Harvard Business Review», опубликованном в 1956 г. В этом издании впервые было высказано предположение, что в организациях необходим специальный работник *(риск-менеджер)*, в чьи обязанности должна входить минимизация величины причиненного ущерба [18].

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

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

После серии финансовых скандалов, самым ярким из которых стало банкротство в 2001 г. американской энергетической корпорации Enron Corporation, в 2002 г. был принят закон Sarnabes-Oxey (Сарбейнза-Оксли). Согласно данному закону организации, акции которых размещены на Американском фондовом рынке, обязаны предоставлять Комиссии по ценным бумагам и биржам США (U.S. Securities and Exchange Commission, SEC) подробную информацию о рисках, в том числе в годовых отчетах по форме 10-K [19].

Австралийская школа управления рисками. Первый стандарт по управлению рисками AS/NZS 4360 появился в Австралии в 1995 г. Позднее, в 1999 и 2004 гг., он был обновлен. В 2003 г. Австралийская фондовая биржа опубликовала принципы корпоративного управления, среди которых управление рисками названо одним из восьми важнейших принципов. Затем принципы обновлялись в 2007, 2010 и 2014 гг. В 2009 г. Австралийская фондовая

биржа опубликовала отдельное пособие по управлению рисками в рамках программы повышения уровня соответствия принципам корпоративного управления. Тогда же австралийский стандарт по управлению рисками был практически полностью принят за основу международного стандарта ISO 31000:2009 «Риск-менеджмент. Принципы и руководства» («Risk Management – Principles and Guidelines»).

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

В 2009 г. был выпущен международный стандарт по управлению рисками ISO 31000:2009. В некоторых европейских странах (например, в Германии) законодательно закреплено требование о раскрытии в годовых отчетах информации, касающейся системы управления рисками и проведении регулярных независимых аудитов. В 2018 г. стандарт ISO 31000 был обновлен. В рабочую группу вошли представители 63 стран, в том числе представители Российской Федерации. На сегодняшний день ISO 31000 является самым распространенным в мире стандартом по управлению рисками. Стандарт представляет собой обобщенное руководство, призванное обеспечить единообразие управления рисками во всех организациях. Управление рисками в соответствии со стандартом ISO 31000:2018 позволяет организациям:

- повышать вероятность достижения целей;
- совершенствовать процесс выявления возможностей и угроз;
- модернизировать процессы управления;
- соответствовать законодательным и другим обязательным требованиям, международным нормам;
- упорядочивать формирование обязательной и управленческой отчетность;
- укреплять и повышать лояльность заинтересованных сторон;

- эффективно распределять и использовать ресурсы для воздействия на риски;
- повышать безопасность жизни и здоровья работников;
- предотвращать материальные потери и негативные инциденты;
- способствовать повышению устойчивости организации.

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

Согласно ст. 19 Федерального закона «О бухгалтерском учете» № 402-ФЗ, вступившего в силу с 01.01.2013 г., экономический субъект обязан организовать и осуществлять ***внутренний контроль*** [20], под которым понимается процесс, направленный на получение достаточной уверенности в том, что экономический субъект обеспечивает эффективность и результативность своих действий, в том числе достижение финансовых и операционных показателей, достоверность и своевременность бухгалтерской (финансовой) отчетности и соблюдение применяемого законодательства, в том числе и в ведении бухгалтерского учета.

Основными элементами внутреннего контроля экономического субъекта являются:

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

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

В 2014 г. Банком России был разработан Кодекс корпоративного управления, продекларированными целями которого являются снижение рисков и совершенствование управления рисками [21]. Для достижения этой цели в Кодексе закреплен перечень рекомендаций, соблюдение которых позволит выстроить результативную и эффективную систему управления рисками, которая включает:

- использование при создании системы общепринятых концепций и практик, в частности COSO и ГОСТ 31000-2010;
- определение советом директоров принципов и подходов организации и утверждение политики в области управления рисками и внутреннего контроля, с последующим использованием утвержденных принципов при принятии решений;
- определение характера и периодичности пересмотра системы управления рисками и политики в области управления рисками, исходя из целей и задач общества, масштабов его деятельности, принимаемых рисков и изменений в организации деятельности;
- оценивание советом директоров как финансовых, так и нефинансовых рисков, которым подвержено общество, а также определение приемлемой величины рисков для общества;
- обеспечение оптимального баланса между рисками и доходностью с учетом требований законодательства и внутренних документов при утверждении советом директоров политики в области управления рисками, в которой должна быть предусмотрена разумная степень риска для операций и сделок, связанных с повышенным риском.

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

В 2019 г. Некоммерческим партнерством «Русское общество управления рисками» (НП «РусРиск») опубликован обновленный национальный стандарт ГОСТ 31000-2019 «Менеджмент риска. Принципы и руководство». На сегодняшний день современное семейство национальных стандартов по управлению рисками насчитывает более 20 наименований (табл. 1.2).

Таблица 1.2

Семейство национальных стандартов по управлению рисками

Код стандарта	Название стандарта
ГОСТ Р 14.09-2005	Экологический менеджмент. Руководство по оценке риска в области экологического менеджмента
ГОСТ Р 27.012-2019	Надежность в технике. Анализ опасности и работоспособности (HAZOP)
ГОСТ Р 51901.3-2007	Менеджмент риска. Руководство по менеджменту надежности
ГОСТ Р 27.303-2021	Надежность в технике. Анализ видов и последствий отказов
ГОСТ Р МЭК 61078-2021	Надежность в технике. Структурная схема Надежности
ГОСТ Р ИСО/МЭК 16085-2007	Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения
ГОСТ Р ИСО 16732-1-2024	Менеджмент риска. Процедуры управления пожарным риском на предприятии
ГОСТ Р ИСО 31000-2019	Менеджмент риска. Принципы и руководство
ГОСТ Р 58771-2019	Менеджмент риска. Технологии оценки риска
ГОСТ Р 51897-2021	Менеджмент риска. Термины и определения
ГОСТ Р 54617.1-2011	Менеджмент риска в наноиндустрии. Общие положения
ГОСТ Р 54617.2-2011	Менеджмент риска в наноиндустрии. Идентификация опасностей
ГОСТ Р 51901.21-2012	Менеджмент риска. Реестр риска. Общие положения
ГОСТ Р 51901.22-2012	Менеджмент риска. Реестр риска. Правила построения
ГОСТ Р 51901.23-2012	Менеджмент риска. Руководство по оценке риска опасных событий для включения в реестр
ГОСТ Р 55059-2012	Безопасность в чрезвычайных ситуациях. Менеджмент риска чрезвычайной ситуации. Термины и определения
ГОСТ Р 55234.2-2013	Практические аспекты менеджмента риска. Менеджмент биориска
ГОСТ Р 55914-2013	Менеджмент риска. Руководство по менеджменту психосоциального риска на рабочем месте
ГОСТ Р ИСО 11231–2024	Менеджмент риска. Метод вероятностной оценки риска на примере космических систем
ГОСТ Р ИСО 15743-2012	Практические аспекты менеджмента риска. Менеджмент и оценка риска для холодных сред
ГОСТ Р МЭК 62502-2014	Менеджмент риска. Анализ дерева событий
ГОСТ Р МЭК 62508-2014	Менеджмент риска. Анализ влияния на надежность человеческого фактора

Результаты исследований основных понятий теории управления рисками показали, что в литературе нет общепринятого толкования термина «риск». Данное обстоятельство создает проблему интерпретации и использования понятия «риск» на практике. Примеры интерпретации понятия риска в литературных источниках представлены в табл. 1.3. Следует отметить, что и 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» [22]. 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». В азиатской культуре понятие «риск» включает два иероглифа 风 险, означающие опасность и позитивную возможность.

Современные позиции толкования понятия «риск» закреплены в отечественных и международных стандартах (см. табл. 1.2). В частности, в отечественном стандарте ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» [2] **риск** характеризуется как влияние неопределенности на запланированные цели.

В своде знаний управления проектами Project Management Body of Knowledge (PMBoK® Guide) **риск** понимается как неопределенное событие (ситуация), которое при наступлении оказывает негативное или позитивное влияние на проектные цели, такие как содержание, длительность, стоимость и/или качество проекта [15–17].

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

Таблица 1.3

Интерпретация понятия «риск» в литературных источниках

Содержание понятия «риск»	Источник
1. Влияние неопределенности на цели	ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство [2]
2. Неопределенное событие или совокупность неопределенных событий	Свод знаний управления рисками (Management of Risk: Guidance for Practitioners – M_o_R®) [23]
3. Неопределенное событие или набор событий, которые в случае наступления способны оказать влияние на процесс достижения целей	Свод знаний управления проектами (PRojects IN Controlled Environments – PRINCE2®) [24]
4. Угроза и/или опасность	Балабанов И.Т. [25]; Машков Д.М. [26]
5. Неопределенность	Филимонов Д.И. [27]; Бурков В.Н. и др. [28]; Мазур И.И. и др. [29]
6. 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) [15–17]
7. Угроза или возможность	Сангхира П. [30]
8. Событие, несущее одновременно угрозу, опасность, неопределенность и возможность	PricewaterhouseCoopers (PwC) [17]
9. Вероятность недополучения доходов и/или вероятность возникновения убытков	Грабовый П.Г. и др. [31]

Окончание табл. 1.3

10. Мера опасности	Шохин Е.И. [32]
11. Совокупность значений возможного	Королев В.Ю. и др. [33]
12. Возможность получения убытков от предпринимательской деятельности	Гражданский кодекс РФ (ст. 926 ГК РФ, ст. 933 ГК РФ) [34]
13. Действия, сделанные наудачу	Даль В. [35]
14. Искусственная экономическая категория, совокупно отражающая меру реальности нежелательного отклонения от цели хозяйственной деятельности предприятия и размер обусловленного этим отклонением ущерба	Качалов Р.М. [36]
15. Негативная часть неопределенного события, наступление которого может принести организации ущерб либо выгоду	Свод знаний управления рисками организаций (The Committee of Sponsoring Organizations of the Treadway Commission «Enterprise Risk Management» – COSO ERM) [17]
16. Вероятный неблагоприятный исход для субъекта	Мадера А.Г. [37, 38]

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

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

В отечественных и международных стандартах понятия «неопределенность» и «риск» часто воспринимаются как синонимы, однако между ними есть существенные различия, а именно:

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

Таким образом, из 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. 1.1).

СТРУКТУРА РИСКА включает:

- **причины риска** — условия, имеющие потенциал для создания событий, способных оказать влияние на достижения целей;
- **источники риска** — объекты, имеющие потенциал для создания событий, способных оказать влияние на достижение целей;
- **последствия от наступления риска** — новые обстоятельства, возникающие в результате материализации риска.

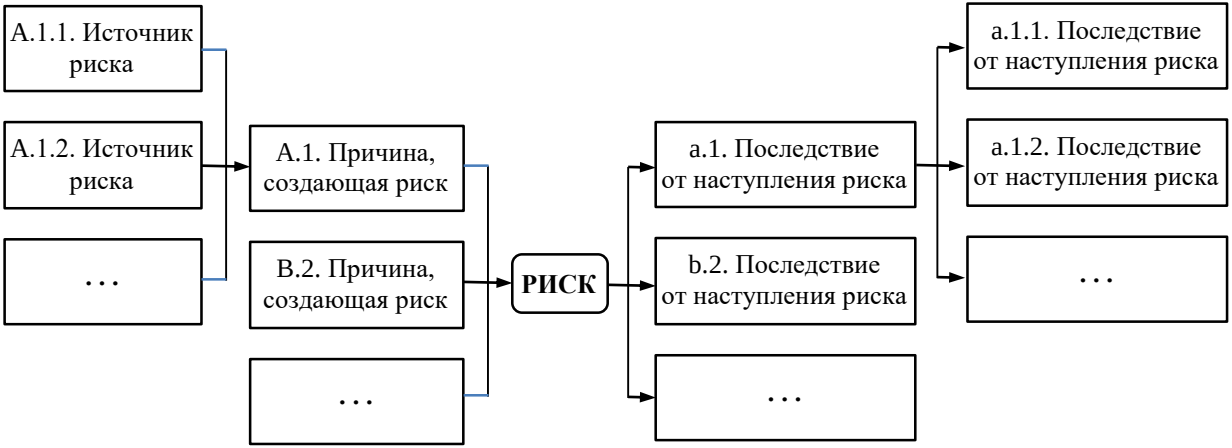

Рис. 1.1. Структура риска

Необходимо отметить, что представленная на рис. 1.1 структура риска позволяет сделать важные практико-ориентированные выводы относительно последствий от наступления риска:

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

2) для нейтральных и смешанных рисков необходимо блокировать наступление проблемных последствий, усиливая 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.

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

Согласно ГОСТ Р ИСО 31000-2019[1] **управление рисками** — это совокупность принципов, скоординированных действий и процессов по оценке, воздействию, мониторингу и контролю рисков [2] (рис. 1.2).

ПРИНЦИПЫ УПРАВЛЕНИЯ РИСКАМИ (*Principle*)

Стандарт ГОСТ Р ИСО 31000-2019 [2] содержит 11 принципов, которых должны придерживаться сотрудники при организации менеджмента для результативного и эффективного управления рисками.

[1] Отечественный ГОСТ Р ИСО 31000-2010 является локализованной версией международного ISO 31000:2009 «Risk Management – Principles and Guidelines».

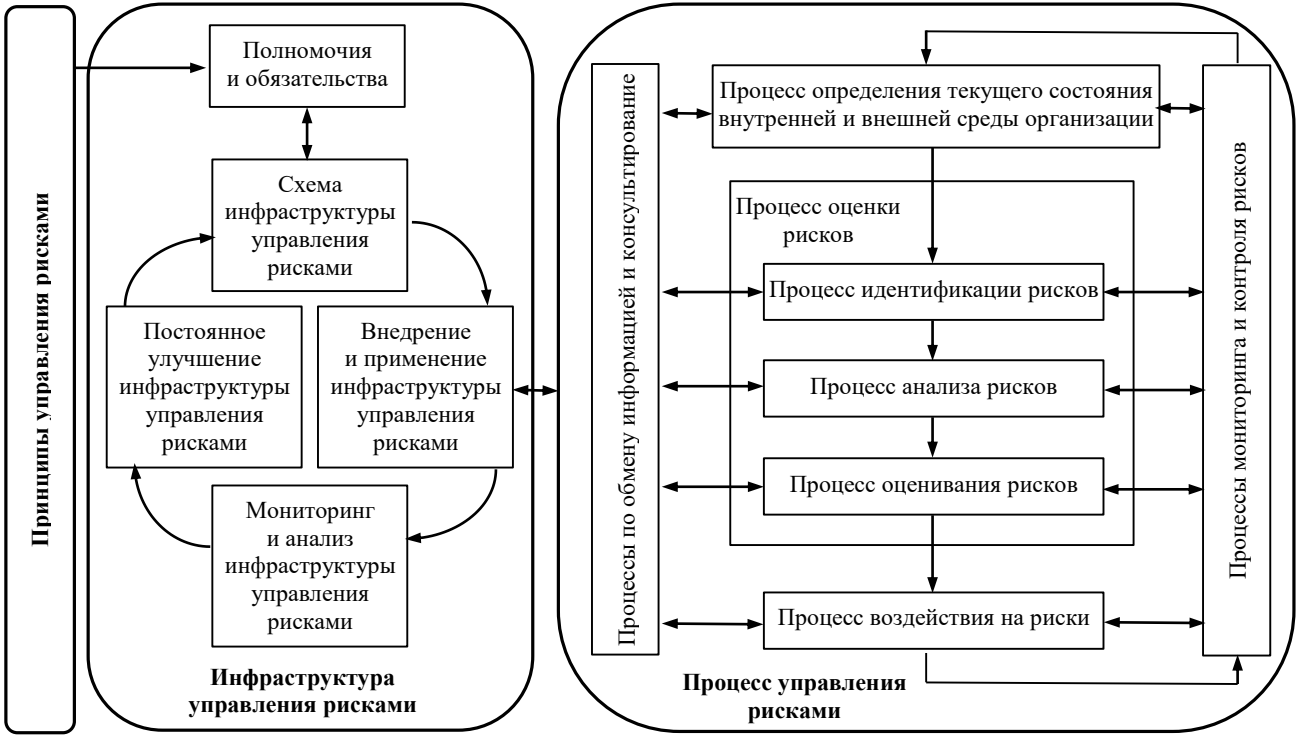

Рис. 1.2. Взаимосвязь между принципами, инфраструктурой и процессами управления рисками согласно ГОСТ Р ИСО 31000-2019

Принципы управления рисками состоят в следующем:

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

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

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

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

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

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

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

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

9) ***прозрачность принимаемых решений с учетом позиции заинтересованных сторон*** (*transparent and inclusive*), гарантирующая, что управление рисками будет отвечать интересам и требованиям всех заинтересованных;

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

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

ИНФРАСТРУКТУРА УПРАВЛЕНИЯ РИСКАМИ (*Framework*)

Согласно ГОСТ Р ИСО 31000-2019 [2] реализация перечисленных принципов обеспечивается включением в инфраструктуру управления рисками пяти нижеприведенных 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 процессов управления рисками организации возможно лишь при наличии зрелой инфраструктуры организации (работники, ответственные за управление рисками, их трудовые договоры и должностные инструкции, рабочие места, специализированное программное обеспечение и др.

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

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

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

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

ПРОЦЕССЫ УПРАВЛЕНИЯ РИСКАМИ

Управление рисками согласно ГОСТ Р ИСО 31000-2019 включает семь процессов [2]:

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

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

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

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

5) **оценивание рисков** (*risk evaluation*): количественное измерение вероятности наступления рисков и их возможного влияния в случае материализации. В ГОСТ Р ИСО 31000-2019 ***вероятность*** понимается как возможность наступления какого-либо события, ***влияние*** — как отклонение (отрицательное или положительное) от ожидаемого результата [2]. Документ, в котором фиксируются результаты изменения характеристик рисков, называется ***матрицей рисков***. Отметим, что процессы идентификации, анализа и оценивания рисков также принято называть **оценкой рисков**;

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

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

1.1.2. 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.

1. В зависимости от причин возникновения выделяют следующие группы рисков:

- ***экономические риски*** — вероятные события, природа которых имеет экономический характер. К экономическим рискам относятся:

– изменение цен на нефть, газ и металлы;

– дефицит (профицит) консолидированного федерального бюджета Российской Федерации;

– изменения курса национальной валюты, темпов инфляции, ключевой ставки Банком России, темпов роста экономики, уровня безработицы, уровня жизни населения, фондовых индексов;

– дефолт;
– экономический кризис и др.;

- ***общественные риски*** — возможные события, природа которых имеет социально-общественный характер. Яркими примерами общественных рисков являются отсутствие на рынке труда квалифицированных кадров, социальная напряженность, изменение уровня медицины, преступности, миграции и вероятность наступления голода;
- ***политические риски*** — вероятные события, которые связаны с деятельностью органов государственной власти. К политическим рискам относятся изменение геополитического давления, норм действующего законодательства, возможность террористического акта и др.
- ***природно-естественные риски*** (***экологические риски***) — риски, связанные с силами природы (например, землетрясение, наводнение, ураган, пожар, экстремально высокие или низкие температуры и др.). Кроме того, к природно-естественным рискам можно отнести нехватку природных ресурсов, загрязнение окружающей среды, изменение климата и пандемии;
- ***технологические риски*** — риски внешней среды, природа которых имеет технологический характер. К данным рискам относятся атака искусственного интеллекта (ИИ), отключение электричества и интернета, атака на критическую инфраструктуру и информационную инфраструктуру (КИИ) и др., в качестве примера которой можно назвать наиболее опасные хакерские атаки, которые произошли в 2021 г., в частности:

– нападение на компьютерные системы «*Colonial Pipeline*» (9 мая 2021 г.). Атака поставила под угрозу поставки горючего сразу в нескольких густонаселенных штатах США. В итоге компания была вынуждена отключить часть своих систем и заплатить хакерам выкуп в криптовалюте [39];

– 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 [40];

– масштабная компьютерная атака на информационные сети МВД Бельгии (26 мая 2021 г.) [41];

– многочисленные кибератаки на североамериканские и австралийские филиалы предприятия по производству мяса «JBS S.A.» (3 июня 2021 г.). В итоге компания была вынуждена заплатить выкуп в размере $11 млн [42];

– 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 [43];

– хакерская атака на компьютерные сети округа Анхальт-Биттерфельд (Германия) (11 июля 2021 г.), повлекшая введение режима чрезвычайной ситуации. Администрация округа была вынуждена приостановить работу почти на две недели. Вследствие отключения критических информационных систем от сети 157 тыс. чел. временно не смогли получить социальные пособия [44].

2. По масштабу воздействия выделяются следующие группы рисков:

- ***макориски*** — глобальные риски, последствия от материализации которых отражаются на всех экономических агентах. Например, экономический кризис 2007–2009 гг., начавшийся с ипотечного кризиса в США отразился в итоге на экономике РФ вызвав одно их самых глубоких падений ВВП (–7,8 % в 2009 г.);
- ***мезориски*** — риски, последствия от наступления которых влияют на определенный регион или отрасль экономики;
- ***микориски (предпринимательские риски)*** — вероятные события, наступление которых оказывает влияние на экономическую деятельность конкретных экономических агентов. Например, алмазодобывающий холдинг «Алроса» 26 июня 2022 г. не смог выплатить купонный доход по еврооблигациям на сумму $7,75 млн из-за рестрикций США, ЕС и Великобритании [45]. Стоит отметить, что согласно ст. 933 ГК РФ риск убытков от предпринимательской деятельности вследствие нарушения своих обязательств контрагентами или изменения условий этой деятельности по независящим от предпринимателя обстоятельствам, в т. ч. риск неполучения ожидаемых доходов, может быть застрахован [34].

3. По функциональной области организации различают:

- ***внутренние и внешние риски*** — риски, находящиеся внутри либо за пределами организации;
- ***коммерческие риски*** — непредвиденные расходы (доходы), которые могут быть получены во время ведения финансово-хозяйственной деятельности организаций;
- ***имущественные риски*** — вероятность потери имущества по причине пожара, кражи, диверсии, халатности и др.;
- ***производственные риски*** — возможный ущерб от остановки производства, гибели или повреждения оборудования, полученного брака продукции и др.;
- ***торговые риски*** — возможные убытки из-за задержки или отказа от оплаты товара, непоставки товара, потери имущества во время транспортировки и др.;
- ***транспортные риски*** — вероятность повреждения или потери товара во время перевозки автомобильным, морским, речным, железнодорожным и/или воздушным транспортом;
- ***финансовые риски*** — вероятность получения убытков (прибыли);
- ***инвестиционные риски*** — вероятность неполучения (получения) ожидаемого коммерческого эффекта. При рассмотрении инвестиционных рисков в негативном ключе выявляются следующие их подвиды:

– *риски упущенной выгоды* — возможность получения финансового ущерба в результате неосуществления какой-либо превентивной меры (например, страхование, хеджирование и др.);

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

– *риски прямых финансовых потерь*.

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

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

4. К рискам, связанным с покупательной способностью денег, относятся:

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

5. По степени контролируемости риски классифицируются на следующие виды:

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

6. В зависимости от наступивших последствий риски могут быть:

- ***негативные***— вероятные события, которые могут привести к наступлению проблемных последствий;
- ***позитивные*** — вероятные события, которые могут привести к наступлению благоприятных последствий;
- ***смешанные***— вероятные события, которые приводят одновременно к проблемным и благоприятным последствиям;
- ***нейтральные*** — вероятные события, которое не приводят к проблемным и (или) благоприятным последствиям.

В качестве примера воздействия негативного и позитивного рисков на план проекта в случае их материализации рассмотрим рис. 1.3, где *t* — это длительность проекта.

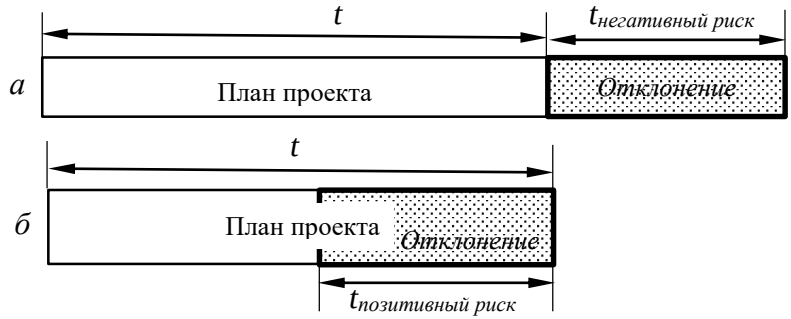

Рис. 1.3. Влияние наступившего негативного риска (*а*) и позитивного риска (*б)* на план проекта

В случае материализации негативного риска происходит увеличение длительности проекта на величину $t_{негативный\ риск}$, так как руководителю и участникам проекта требуется дополнительное время для устранения возникшей проблемы.

В случае наступления позитивного риска также происходит отклонение от запланированной длительности. Однако при материализации позитивного риска проект можно завершить быстрее, сократив время выполнения на величину $t_{позитивный\ риск}$.

Влияние материализовавшихся рисков можно охарактеризовать следующими формулами:

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

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

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

C_1 — прямой материальный ущерб;

C_2 — ресурсы, направляемые на ликвидацию последствий;

C_3 — ресурсы, которые будут направлены на восстановление;

C_4 — материальный ущерб, вызванный отклонением от запланированных целей;

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

C_5 — материальная польза, вызванная отклонением от запланированных целей.

В качестве примера наступившего негативного риска можно рассмотреть ситуацию потери сервера жестких дисков в ИТ-организации в результате пожара C_1. Для ликвидации последствий ИТ-организации нужно приобрести новый сервер C_2, провести пуско-наладочные работы C_3 и оплатить простой трудовых ресурсов C_4, спровоцированный потерей информационных данных.

Наглядным примером положительного эффекта от материализации позитивного риска являются привлечение в ИТ-проект программиста более высокого квалификационного уровня или проведение 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, обойдутся ИТ-организации в $4200 [46].

7. 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.

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

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

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

- ***текущие риски*** — потери, которые могли бы возникнуть сегодня, например, по контракту или нескольким контрактам, если бы контрагент не выполнил свои обязательства;
- ***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.

10. В зависимости от возможности передачи риска другому лицу выделяют:

- ***страхуемый риск*** — риск, в отношении которого может быть заключен договор страхования;
- ***нестрахуемый риск*** — риск, в отношении которого не может быть заключен договор страхования.

1.2. Процессы управления рисками: методы и инструменты

1.2.1. Анализ внутренней и внешней среды объектов риска

Эффективное и результативное управление рисками возможно, когда ясны и понятны цели организации, проекта, сделки, контракта и др., которые требуется достичь. В связи с этим рассмотрим пример достижения цели.

Предположим, что субъект желает совершить переход из состояния A в состояние B. Достичь желаемого состояния субъект планирует спустя время T_1. Желаемое состояние B является для субъекта его целью (рис. 1.4).

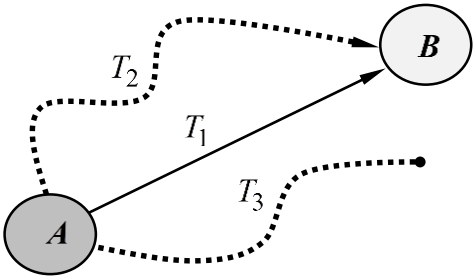

Рис. 1.4. Переход субъекта
из состояния A в состояние B

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

сценарий 1. При достижении цели ничего не произойдет и субъект благополучно спустя запланированное время T_1 ее достигнет. Этот сценарий маловероятен, потому что на процесс достижения цели будут влиять различные штатные и нештатные ситуации. Например, цель изменится, будут отсутствовать необходимые компетенции, ключевой работник будет занят на других проектах и др. Если подобные ситуации наступят, тогда для субъекта будут актуальны иные сценарии;

сценарий 2. При достижении цели наступили события, повлиявшие на процесс достижения целей и запланированное время. В результате субъект достигнет цели через время T_2. Если наступившие события были негативными, то $T_2 > T_1$, если позитивными — $T_2 < T_1$. Подобный сценарий может считаться допустимым, если *риск-аппетит* и *толерантность к риску* приемлемы для субъекта. Однако если материализовавшиеся события окажут значительный материальный ущерб, то субъект не достигнет запланированной цели;

сценарий 3. При достижении цели наступили события, не позволившие субъекту достичь запланированной цели. Для субъекта подобный сценарий является неприемлемым и недопустимым. В связи с этим логично предположить, что прежде чем приступить к достижению цели, субъекту необходимо заранее выявить события, которые могут оказать воздействие на данный процесс.

сценарий 4. Прежде чем приступать к достижению цели, субъект продумал наиболее безопасное движение и заблаговременно выявил события, которые могут повлиять на данный процесс. Кроме того, для повышения шансов на успех субъект сделал запасы дополнительных ресурсов на случай, если наступят непредвиденные события (рис. 1.5). Стоит отметить, что возможно достижение цели в рамках сценария 4 потребует б*о*льших временных затрат времени T_4, однако субъект гарантированно достигнет желаемой цели. Подобный процесс достижения целей называют ***риск-ориентированным***.

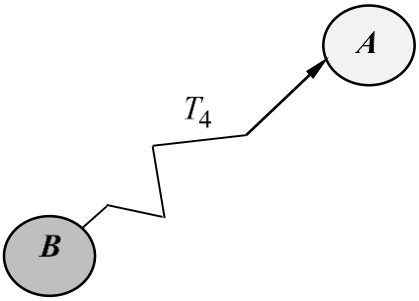

Рис. 1.5. Риск-ориентированный переход субъекта из состояния *A* в состояние *B*

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

Далее требуется провести анализ внутренней среды. Для проектов и организаций этот процесс различен. В частности, для того чтобы провести анализ внутренней среды проекта, достаточно сравнить текущий статус выполненных работ (оказанных услуг, поставленных товаров) с запланированным и установить, идет ли все по графику и есть ли отклонения. Организация, являясь структурно сложным объектом, требует иного подхода. Для того чтобы определить текущее внутреннее состояние организации, необходимо определить долю рынка, объемы сбыта, качество рекламы, размер прибыли, уровень компетентность работников и др.

Внешние среды для проекта и организации также различны. Например, для проведения анализа внешней среды проекта достаточно оценить текущие интересы, цели и ожидания внешних заинтересованных сторон. Согласно международному своду лучших практик управления проектами PMBOK Guide® под заинтересованными сторонами проекта понимаются физические и (или) юридические лица, активно участвующие в проекте, либо лица, интересы которых могут быть затронуты в ходе выполнения проекта или по его завершению [14–16].

Определение текущего состояния внешней среды организации является более трудоемким, так как требует выявления и анализа экономических, политических, социально-общественных, природно-естественных и технологических факторов, которые способны влиять на ее деятельность (рис. 1.6).

Прямое и косвенное воздействие факторов внешней среды на деятельность организации создают **риски внешней среды**, к которым могут быть отнесены риск изменения действующего законодательства, темпов инфляции, ключевой ставки ЦБ, курса

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

национальной валюты, рестрикции, риск отсутствия на рынке труда квалифицированные кадров и др.

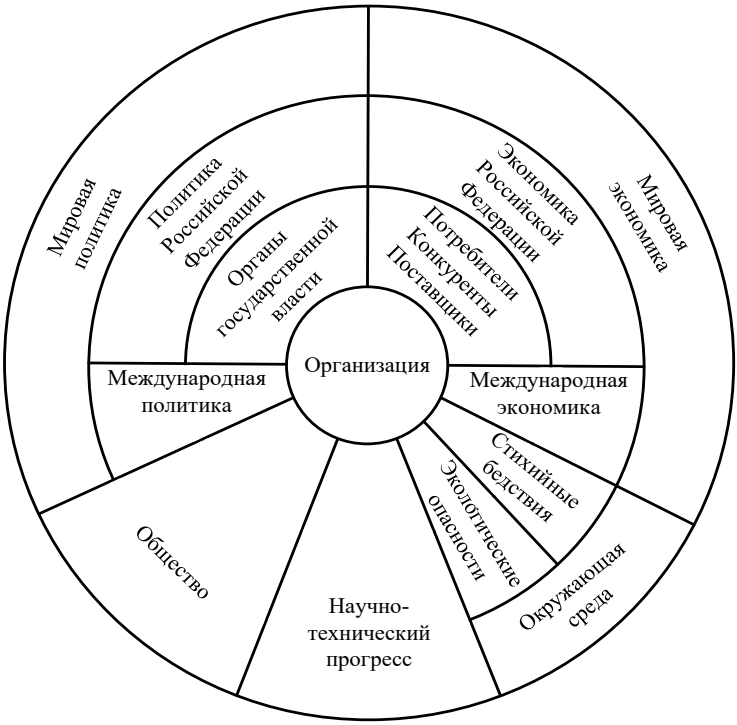

Рис. 1.6. Модель влияния факторов внешней среды на деятельность организации

Примеры рисков внешней среды представлены в приложении А.

1.2.2. Идентификация рисков

Согласно ГОСТ 31000-2019 **целью идентификации рисков** является составление всеобъемлющего перечня вероятных событий, которые в случае наступления могут оказать влияние на процесс достижения целей [2]. Документ, в котором фиксируются выявленные риски, называется ***реестром рисков***.

Идентификация рисков является одним из наиболее кропотливых процессов управления рисками. По мнению Ключникова В.О., сложность выявления рисков вызвана уникальностью бизнес-процессов [47–49]. Ученый в своих трудах отмечает, что время, затраченное на выявление рисков, представляет собой инвестицию в успех, так как неучтенные риски при материализации помешают достижению запланированных целей. Для выявления рисков отечественные и зарубежные ученые рекомендуют применять различные методы и их комбинации в зависимости от специфики бизнес-процессов. Методы идентификации рисков представлены в табл. 1.4.

Таблица 1.4

Методы идентификации рисков

Название метода		Разработчики
Оригинал (англ.)	В переводе на русский	
1. Retrospective	Ретроспективный анализ документов	Никонов В.А. [50]
2. Brainstorming	Мозговой штурм	Осборн А. [51]
3. Delhi	Метод «Делфи»	Хелмер О. [51]
4. SWOT matrix	SWOT-анализ	Эндрюс К. [51]
5. Structured What-If Technique (SWIFT)	Структурированный анализ сценариев методом «Что, если?»	Лавли Ф. [52]

Ретроспективный анализ документов (*Retrospective*). Ретроспективный анализ представляет собой детальный разбор данных, изменяющихся в рамках конкретного временного интервала, в виде сравнения плановых результатов с достигнутыми итогами, результатом которого является определение количественных и качественных изменений анализируемых процессов.

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 197 универсальных рисков, выявленных

при анализе 192 судебных решений и изучении бизнес-деятельности 495 ИТ-организаций Томской области (ОКВЭД 62.0), представлен в приложении Б.

Метод «Мозговой штурм» (*Brainstorming*) — метод коллективного генерирования максимального количества креативных идей и нестандартных решений проблем с последующим выбором наиболее эффективных. Основы техники мозгового штурма разработаны в 1942 г. американский журналистом (рекламщик, психолог) Алексом Осборном. Для работы по данному методу создается группа экспертов, состоящая из членов команды по исследуемому процессу/проекту и специалистов из рассматриваемой области. Выявляются и идентифицируются *любые* важные по мнению участников группы возможные риски, которые оформляются в список рисков. Ключевой особенностью метода мозгового штурма *является запрет на обсуждение* выдвинутых идей.

Применение метода мозгового штурма в системе государственного управления характеризуется некоторыми особенностями:

1) высокая важность задач, поставленных перед органами государственной власти, решение которых оказывает существенное влияние в целом на управление государством. Это диктует необходимость квалифицированной всесторонней и взвешенной экспертной оценки рисков, возникающих при реализации государственных программ, проектов, разработке нормативных правовых документов и др.;

2) высокий уровень общественной значимости проблем и задач, вызывающих большой общественный резонанс в силу актуальности обсуждаемых вопросов. Анализ и идентификация рисков, сопровождающих реализацию таких задач, требуют проведения учета результатов социологических исследований, опросов общественного мнения, рейтингов должностных лиц и конкретных органов власти и управления;

3) необходимость определенной организации рабочей группы экспертов, в состав которой следует включать максимально широкий круг специалистов в целях исключения ситуаций навязывания и диктата мнений наиболее известных и авторитетных участников группы;

4) специфическое содержание идентифицированных рисков, основу которых составляет неэффективность государственного управления в рассматриваемой сфере, создающая опасность утраты доверия к власти со стороны общества, ослабление ее легитимности.

Преимущества метода мозгового штурма:

- возможность найти неожиданные идеи, разбить сложную проблему на мелкие задачи;
- инициация критического мышления участников экспертной группы;
- создание условий для сплочения команды;
- выявление специальных рисков, легкость применения, а также коллаборация[1] участников мозгового штурма.

К недостаткам метода мозгового штурма можно отнести:

- низкое качество процесса идентификации рисков (которое выражается в невозможности либо недостаточности выявления специальных рисков);
- опасность доминирования наиболее авторитетного эксперта или экспертов [53];
- вероятность смещения акцента на отдельных аспектах обсуждения, что может привести к отклонению от главной темы мозгового штурма [53];
- недостаточная квалификация или отсутствие организаторских способностей у ведущего [53].

Метод «Делфи» (Delphi)

Метод «Делфи», созданный в 1960-е гг. сотрудниками RAND Corporation, изначально разрабатывался как метод прогнозирования трендов развития различных технологий, в частности военных технологий. Однако по прошествии времени метод показал свою результативность во время выявления рисков.

[1] **Коллаборация** — сотрудничество, направленное на достижение общей цели посредством объединения знаний, опыта и ресурсов для решения сложных задач и достижения лучших результатов как в рамках одной организации, так и между разными компаниями или группами специалистов из разных областей.

Метод «Делфи» представляет собой процедуру, направленную на получение согласованного мнения группы экспертов для получения качественного и достоверного результата, не зависящего от субъективного мнения отдельного специалиста. При этом *экспертная оценка* в данном случае представляет собой не частное мнение профессионала в конкретной области, а результат проведения нескольких этапов (раундов) опроса, что позволяет не только получить единое коллективное решение, но и определить степень согласованности отдельных точек зрения.

К особенностям метода можно отнести:

- независимость мнений экспертов, обеспечиваемая проведением анкетирования в заочной форме;
- постепенное согласование индивидуальных мнений экспертов посредством многоэтапной процедуры опросов;
- возможность свободного высказывания точек зрения, которая обеспечивается анонимностью ответов экспертов;
- исключение проблемы доминирования мнения наиболее авторитетных экспертов, достигаемое за счет одинакового «веса» ответа каждого эксперта;
- высокая вероятность выявления специальных рисков, которые в открытом обсуждении не всегда будут озвучены;
- отсутствие необходимости сбора экспертов одновременно и в одном месте.

Наряду с определенными достоинствами метода следует отметить высокую трудоемкость проведения многораундового анкетирования, большие временные затраты, а также необходимый уровень участников экспертной группы в умении четко и профессионально излагать свое мнение в письменной форме.

SWOT-анализ — метод, позволяющий выявить не только сильные (*Strengths*) и слабые (*Weaknesses*) стороны исследуемого субъекта, но и рассмотреть возможности (*Opportunities*, позитивные риски) и угрозы (*Threats*, негативные риски) из внешней среды. В системе государственного управления SWOT-анализ может быть использован для выявления рисков, выступающих как проявление угрозы со стороны внешней среды.

Структурированный анализ сценариев методом «Что, если?» (*Structured What-If Technique* — **SWIFT**)**.** Анализ сценариев развития последствий в результате наступления рисков с помощью метода SWIFT является упрощенной версией метода 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, так как метод не требует предварительной подготовки,
- графическое исполнение, стимулирующее творческий процесс.

Представленные методы идентификации рисков направлены на выявление определенных рисковых событий. При решении проблемы применимости методов для выявления актуальных для организации или проекта рисков рекомендуется использовать различные методы и привлекать сторонних экспертов.

Согласно ГОСТ Р 51901.21-2012 «Менеджмент риска. Реестр риска. Общие положения» характеристики выявленных рисков необходимо заносить в раздел «Идентификация» в реестре рисков (табл. 1.5) [54].

Таблица 1.5

Пример раздела «Идентификация» реестра рисков

Название риска	Характеристики риска		
	Описание	Классификационная группа	Дата выявления
Риск изменения условий контрактов работников	Требование профсоюза о пересмотре контрактов сотрудников, в которых должно быть отражено новое распределение обязанностей	Комплаенс-риск	хх.хх.хххх

1.2.3. Анализ рисков

В соответствии с требованиями ГОСТ 31000-2019 **цель анализа рисков** состоит в выявлении причин, вызывающих наступления рисков, источников рисков, а также возможных последствий в случаях их материализации [2].

Согласно ГОСТ Р 58771-2019 [3] оптимальными для проведения анализа рисков являются представленные в табл. 1.6 методы «Галстук-бабочка» (первый этап) [55] и «Почему-почему» [56].

Таблица 1.6

Методы анализа рисков

Название метода		Разработчики
Оригинал (англ.)	В переводе на русский	
1. Bow-tie	«Галстук-бабочка» (первый этап)	Лангминд Б. [55]
2. 5Why	«Почему-почему»	Тоеда С. [56]

Метод «Галстук-бабочка» (*Bow-tie*) включает два этапа [55]:

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

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 рис. 1.7.

Метод «Почему-почему» (5Why, «Пять "почему"») [56] 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?», целью которого является определение источника риска. Если источник риска во время первой итерации не устанавливается, тогда процедура повторяется.

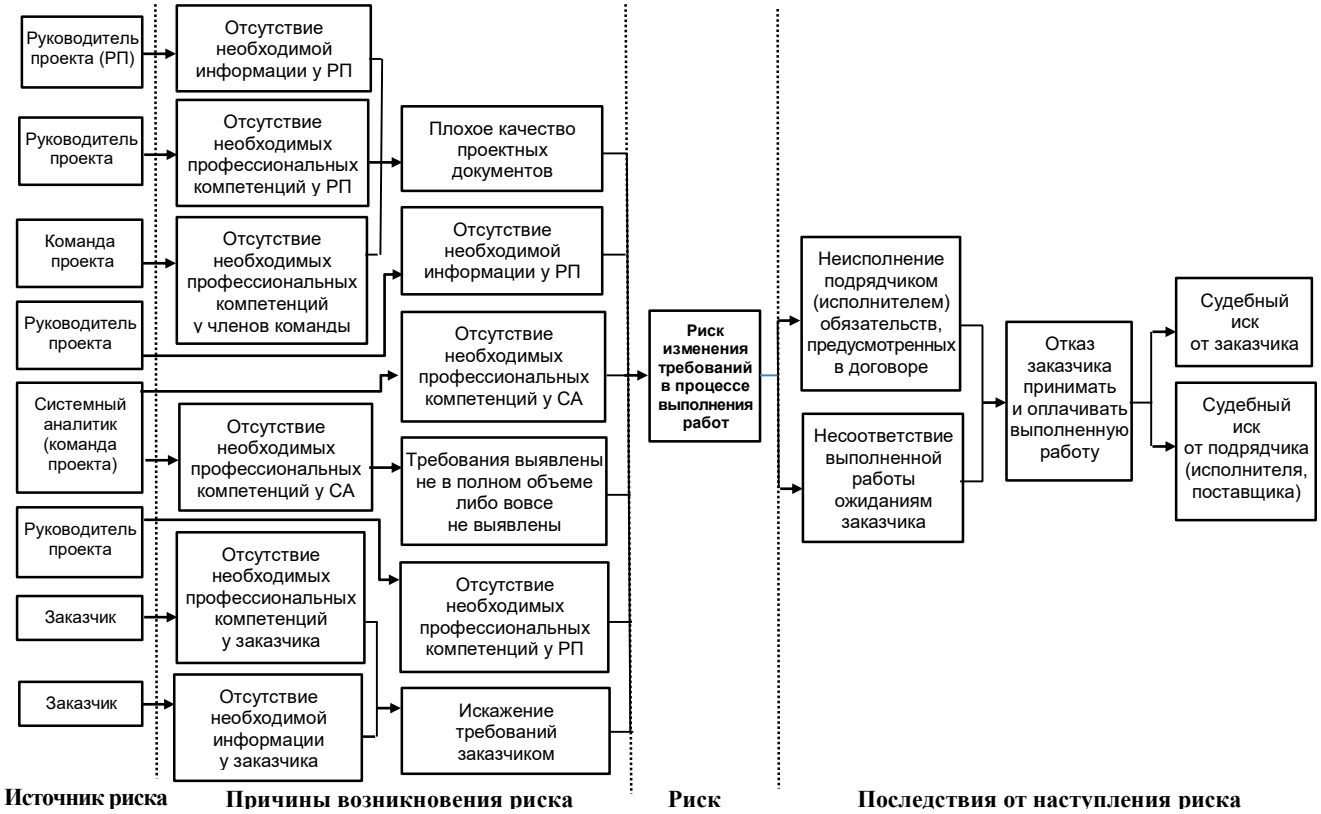

Рис. 1.7. Анализ риска «Изменение требований в процессе выполнения работ (оказания услуг)» методом Bow-tie

Пример анализа риска «По факту проектные работы окажутся значительно сложнее, чем предполагалось изначально» представлен в табл. 1.7.

Анализ коммерческих, комплаенс-рисков и проектных универсальных рисков методом «Почему-почему» (см. приложение Б) позволил установить, что источниками рисков являются заинтересованные стороны проекта (рис. 1.8): конечный пользователь, заказчик, руководитель проекта, команда проекта, субподрядчик, конкурент.

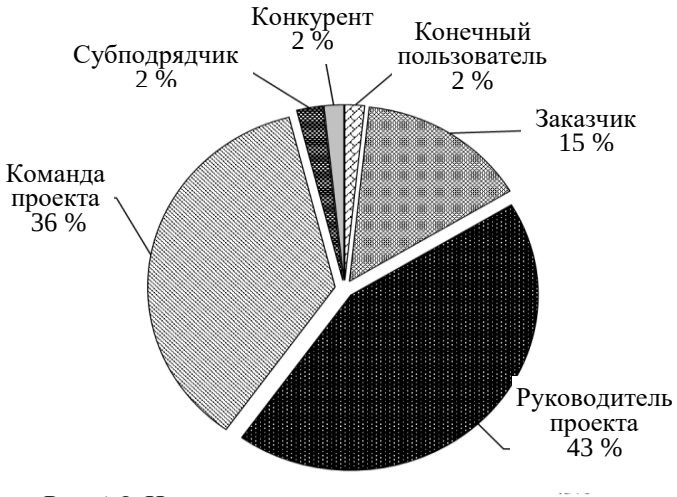

Рис. 1.8. Источники актуальных для проектов универсальных рисков

Согласно ГОСТ Р 51901.21-2012 «Менеджмент риска. Реестр риска. Общие положения» характеристики, выявленные в ходе анализа рисков, необходимо фиксировать в разделе «Анализ» реестра рисков [54]. Как правило, к данным характеристикам относятся:

- причины, создающие риск,
- источники риска
- последствия, возникающие в случае его наступления.

Таблица 1.7

Анализ риска «По факту проектные работы окажутся значительно сложнее, чем предполагалось изначально» с помощью метода «Почему-почему»

Название риска	Почему есть вероятность наступления этого риска?	Повторный вопрос: Почему есть вероятность наступления этого риска?	Источник риска
Риск повышения уровня сложности работ в процессе выполнения проекта по сравнению с первоначально запланированным	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

1.2.4. Оценивание рисков

Представим, что в процессе идентификации рисков было выявлено большое количество рисков и что после проведения анализа стало очевидно, что не все они одинаково важны. Например, риск возможного ухода ключевого сотрудника будет представлять для нас бóльший интерес, нежели отключение электричества или интернета. В связи с этим логично предположить, что выявленные риски следует определенным образом сгруппировать для того, чтобы выделить следующие группы рисков:

- наиболее опасные риски;
- риски, требующие постоянного управленческого внимания;
- незначительные риски, которые можно не учитывать и др.

Для решения данной проблемы применяется оценивание рисков. Согласно ГОСТ 31000-2019 **целью оценивания рисков** является количественное измерение следующих показателей [2]:

вероятности наступления рисков (возможность наступления какого-либо события);

возможного влияния (как отклонение от ожидаемого результата).

Документ, в котором фиксируются результаты изменения характеристик рисков, называется ***матрицей рисков***.

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

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

В частности, количественные методы оценивания рисков представляют вероятность материализации рисков как величину, которая рассчитывается по формуле

$$P(A) = \frac{m}{n}, \tag{1.3}$$

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

m — число исходов испытания, благоприятствующих событию A;

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

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 табл. 1.8 и 1.9.

Таблица 1.8

Коэффициенты оценивания вероятности материализации риска

Вероятность наступления риска	Коэффициент Харрингтона		Комментарии
	PMBOK® Guide	Merna T., [57]	
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 его 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 1.9

Коэффициенты оценивания возможного влияния в случае наступления риска

Влияние риска	Коэффициент Харрингтона		Комментарии
	PMBOK ® Guide	Merna T., [57]	
Очень высокое	0,8–1,0	5	Причинен катастрофический материальный ущерб
Высокое	0,64–0,8	4	Причинен значительный материальный ущерб
Среднее	0,37–0,64	3	Причинен приемлемый материальный ущерб
Низкое	0,2–0,37	2	Ущерб незначительный
Очень низкое	0,1–0,2	1	Есть незначительные отставания от намеченного расписания и бюджета
Нет влияния	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.

Согласно ГОСТ Р 56715.3-2015 «Системы проектного менеджмента. Часть 3. Методы» полученные с помощью коэффициента Харрингтона оптимистическая, реалистическая и пессимистическая оценки рисков используются для расчета вероятности наступления риска и уровня его влияния по следующим формулам («Метод трех точек») [58]:

$$A_{ij} = \frac{a_i^o + 4a_i^r + a_i^p}{6}, \quad (1.4)$$

$$B_{ij} = \frac{b_i^o + 4b_i^r + b_i^p}{6}, \quad (1.5)$$

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

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

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

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

i — номер риска;

j – номер эксперта.

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

$$A_i = \frac{\sum_{j=1}^{n} A_{ij}}{n}, \tag{1.6}$$

$$B_i = \frac{\sum_{j=1}^{n} B_{ij}}{n}, \tag{1.7}$$

где n — количество экспертных мнений.

Для визуализации полученных оценок используется специальный инструмент — **матрица рисков**. Пример матрицы рисков, применяемый Министерством обороны США (*The Department of Defense United States of America* — DoD), представлен на рис. 1.9 [59].

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

1) ***красная*** — самые опасные риски, способные нанести катастрофический ущерб;

2) ***желтая*** — умеренные риски, способные нанести приемлемый ущерб;

3) ***зеленая*** — безопасные риски.

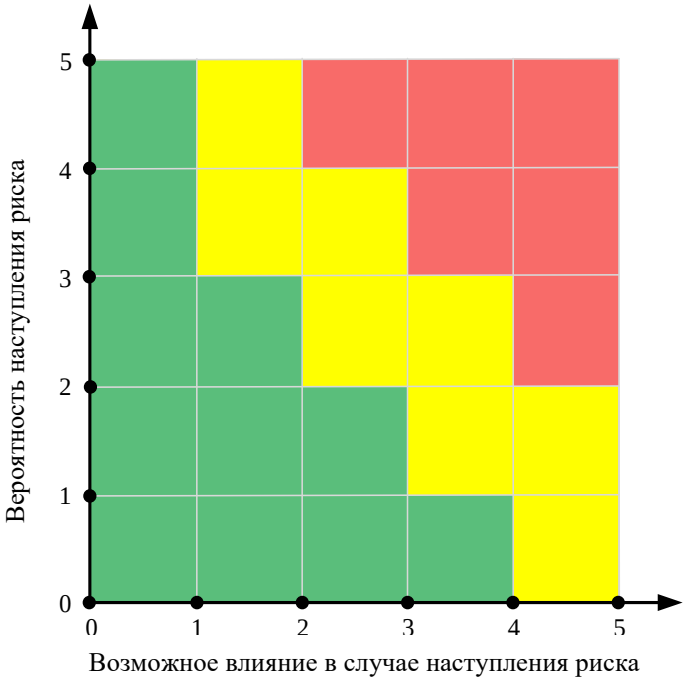

Рис. 1.9. Матрица рисков Министерства обороны США

В работах Merna T. и Al-Thani F. предлагается **распределение негативных рисков** на четыре группы [57]:

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

2) ***непредсказуемые риски,*** или **«*аллигаторы*»** (*alligator*) — негативные риски, имеющие низкую вероятность материализации, но обладающие способностью оказывать значительное негативное

влияние. Как правило, к «аллигаторам» относятся комплаенс-риски. Например, организация, реализующая проект, может получить штраф в связи с нарушением императивных норм (ч. 1 ст. 9.5 КоАП РФ; ч. 3, ст. 14.1 КоАП РФ, ст. 15.33.2 КоАП РФ) [60] и др.;

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

4) ***несущественные риски*, или «*котята*»** (*kitten*) — негативные риски, имеющие низкую вероятность материализации и при этом не обладающие способностью оказывать какое-либо значительное влияние. По мнению Merna T. и Al-Thani F., «котята» не способны хоть как-то навредить проекту, поэтому данными негативными рисками можно пренебречь [57].

Матрица вероятности и влияния представлена на рис. 1.10.

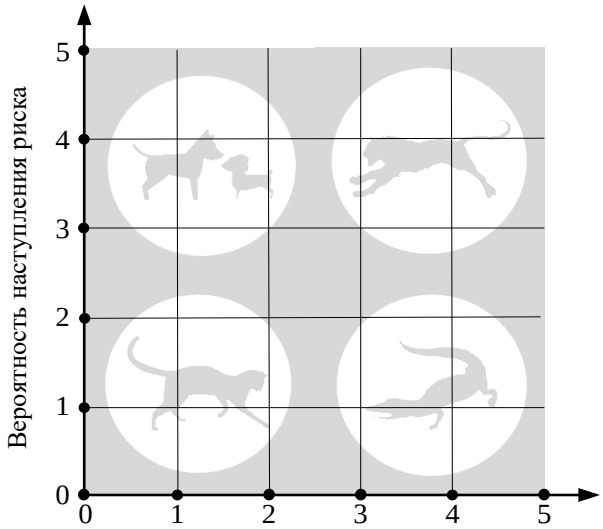

Рис. 1.10. Матрица негативных рисков Мерна Т. и Ал-Хани

Отдельно следует выделить группу маловероятных, но очень опасных рисков:

- промышленные катастрофы,
- потрясения,
- природные катаклизмы,
- пандемии,
- эпидемии.

Талеб Н.Н называет подобные риски «***черные лебеди***» [61].

Позитивные риски автором настоящего пособия рекомендуется распределять на четыре группы [62]:

1) ***созидательные риски***, или «***слоны***» — риски, имеющие высокую вероятность материализации и способные 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***» — риски, имеющие низкую вероятность материализации, но обладающие способностью оказывать значительное влияние, из чего можно заключить, что «львы» представляют собой 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***» — риски, имеющие высокую вероятность материализации, но неспособные оказывать значительное влияние. Отделение данных позитивных рисков от остальных имеет большую практическую ценность, так как провоцируя («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***» — риски, имеющие низкую вероятность материализации и не обладающие способностью оказывать значительное позитивное влияние. Рисками данной группы можно пренебречь.

Матрица вероятности и влияния позитивных рисков представлена на рис. 1.11 [62].

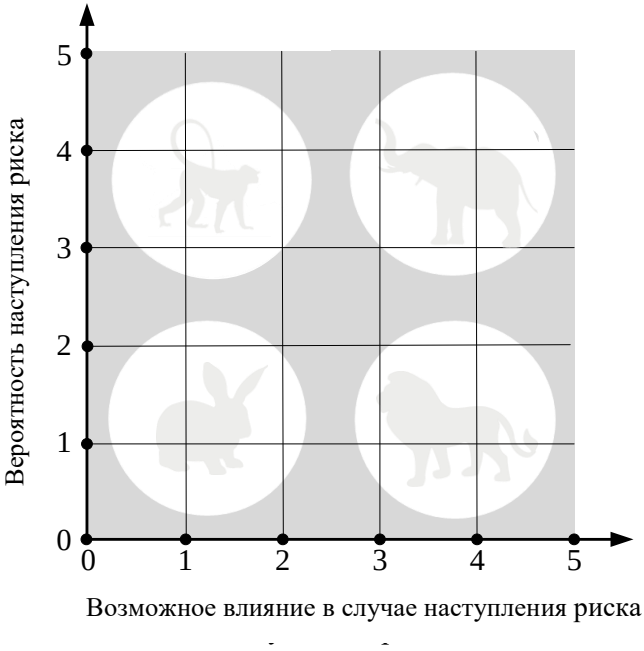

Рис. 1.11. Матрица позитивных рисков

Рассмотрим примеры позитивных рисков в проектах.

***Риск изменения числа участников проекта* (*менее шести*).** В аналитических докладах The CHAOS Manifesto приводятся статистические данные, показывающие, что проекты, в составе которых менее шести участников, значительно успешнее, чем проекты, в которых состав участников более шести человек (табл. 1.10) [63].

Таблица 1.10

Проекты, в которых менее 6 участников (50 тыс. проектов)

Статус проекта	Распределение, %
Успешные проекты	67
Незавершенные проекты	5
Проекты с изменением целей вследствие проблем	28

Риск привлечения в проект высококвалифицированного работника. Результаты исследований показывают, что материализация данного позитивного риска повышает вероятность успешного достижения запланированных целей до 70 % [64].

Риск привлечения в проект руководителя проекта, имеющего профессиональное образование в области управления проектами и 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 проведенных исследований показали, что на эффективность и результативность рабочих групп значительно влияет эмоциональный интеллект руководителя [65]. Например, его негативные эмоции быстро передаются участникам проекта, что отражается на их координации, мотивации и энтузиазме.

Риск декомпозиции большого проекта на малые проекты с продолжительностью не более четырех месяцев. Согласно данным The CHAOS Manifesto доля краткосрочных проектов, трудоемкость которых составляет не более 700 чел.-ч., равна 76 %, в то время как доля среднесрочных (700–2500 чел.-ч.) — 14 %, долгосрочных ИТ-проектов (более 2500 чел.-ч.) — 10 % [64].

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 уровня влияния риска, оказываемого на одну или несколько стратегических, тактических, операционных или проектных целей;
- ***срочность*** — период, в течение которого должны быть проведены меры воздействия на риск;

- ***выявляемость*** — способность обнаружения и распознавания приближения риска. Для представления близости, выявляемости и величины влияния может быть использована пузырьковая диаграмма (*bubble chart*);
- ***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».

Согласно ГОСТ Р 51901.21-2012 «Менеджмент риска. Реестр риска. Общие положения» характеристики вероятности наступления рисков и их возможного влияния в случаях материализации необходимо заносить в раздел «Оценивание» в реестре рисков [54].

Пример заполнения раздела представлен в табл. 1.11.

Таблица 1.11

Пример раздела «Оценивание» в реестре рисков

Название риска	Вероятность наступления риска, (0÷1)	Влияние в случае наступления риска, (0÷10)	Группа риска
Риск изменения условий контрактов сотрудников	0,6	3	Зеленая
Риск отказа партнеров от сотрудничества	0,3	3	Зеленая
Риск несоответствия результатов выполненной работы (оказанной услуги) ожиданиям конечного пользователя	0,5	6	Желтая

1.2.5. Воздействие на риски

После того как среди выявленных рисков установлены наиболее важные и опасные риски, требующие постоянного управленческого внимания, и риски, которыми можно пренебречь, необходимо разработать точечные меры воздействия на данные риски. Согласно ГОСТ 31000-2019 **воздействие на риски** включает разработку мер превентивного воздействия на риски (план А) и разработку мер принятия рисков (план Б). Документ, в котором фиксируются разработанные меры воздействия на риски, называется ***планом управления рисками***.

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 обнаруженные во время идентификации. Опасность данных рисков заключается в их неожиданном наступлении.

В качестве примера реализации мер плана Б можно рассмотреть ситуацию, связанную с риском возможного ухода из проекта 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 достаточно часто можно встретить в производстве фильмов. Например, в картине 1994 г. «Побег из Шоушенка» главный герой Энди Дюфрейн смог уйти в побег только потому, что заранее подготовил «тайный ход» и спрятал на счетах $370 000.

Для увеличения качества разрабатываемых мер планов А и Б рекомендуется вести их разработку, 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 табл. 1.12.

Таблица 1.12

Стратегии воздействия на риски

Тип риска	Стратегия воздействия	Описание стратегии воздействия
Негативный риск	Нивелирование	Выявление источников риска с их последующей ликвидацией
	Ослабление	Изменение вероятности материализации риска и/или возможного влияния в случае его наступления
	Передача (страхование, хеджирование)	Передача риска третьему лицу
	Эскалация	Передача риска компетентному лицу
	Наблюдение	Выполнение процесса мониторинга без каких-либо активных действий в отношении риска
	Принятие	Отсутствие активных действий в отношении риска
Позитивный риск	Масштабирование	Увеличение масштаба возможного благоприятного эффекта
	Усиление	Изменение вероятности материализации риска и/или возможного влияния в случае его наступления
	Передача	Передача риска третьему лицу
	Эскалация	Передача риска компетентному лицу
	Наблюдение	Выполнение процесса мониторинга без каких-либо активных действий в отношении риска
	Принятие	Отсутствие активных действий в отношении риска

Самой результативной стратегией воздействия на негативные риски, по мнению Селиховкина И., является ***стратегия нивелирования***, суть которой заключается в ликвидации источников рисков [66]: не будет источника риска, 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.

Стратегия диверсификации рисков — это перераспределение капитала между несколькими, несвязанными между собой инвестиционными инструментами: акциями, облигациями, валютой, недвижимостью, криптовалютой и др. ***Стратегия хеджирования рисков*** — это перенос рисковых событий на субъектов, готовых их принять.

После определения для каждого идентифицированного риска стратегии воздействия с помощью специальных методов, представленных в табл. 1.13. разрабатываются непосредственно меры планов А и Б.

Таблица 1.13

Методы разработки мер воздействия на риски

Название	Название (перевод на русский)	Разработчики
Retrospective	Ретроспективный анализ документов	Никонов В.А. [50]
Delhi	Метод «Делфи»	Хелмер О. и др. [51]
Brainstorming	Метод «Мозговой штурм»	Осборн А. [51]
Bow-tie	Метод «Галстук-бабочка» (2-й этап)	Лангминд Б. [55]
Method of Walt Disney	Метод Уолта Диснея	Дисней У. [51]

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 «Делфи» (*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 «Делфи» (рис. 1.12).

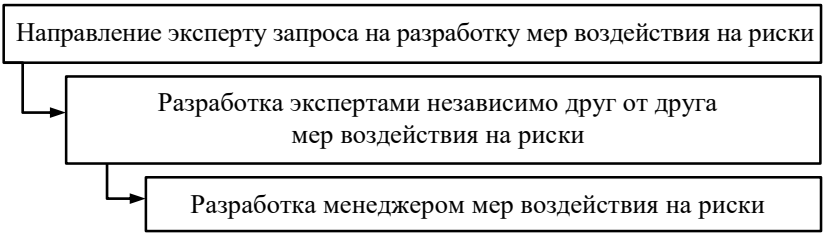

Рис. 1.12. Разработка мер воздействия на риски с помощью метода «Делфи»

Метод «Мозговой штурм» (*Brainstorming*). Результативно проявляет себя метод мозгового штурма при работе в малых группах до шести человек (рис. 1.13).

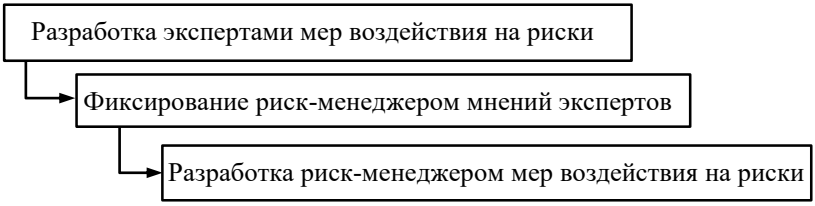

Рис. 1.13. Разработка мер воздействия на риски с помощью метода «Мозговой штурм»

Творческая свобода и отсутствие критики дают возможность экспертам создать большое количество разнообразных мер воздействия не только для специальных рисков, но и для пересмотра механизма воздействия на универсальные риски.

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)», назначение которых в оперативной локализации причиненного ущерба (усиление благоприятного эффекта).

Метод Уолта Диснея (*Method of Walt Disney*). Суть метода заключается в условном выделении ролей «фантазера», «критика» и «реалиста». «Фантазер» отвечает за поиск творческих идей, в том числе и на первый взгляд нереальных (фантастические), «критик» ищет слабые места в предложенных мерах, а «реалист» оценивает достижимость и целесообразность разработанных мер воздействия на риски.

Помимо разработки мер планов А и Б, в процессе воздействия на риски также рекомендуется выявлять триггерные условия. В управлении рисками ***триггерными***[1] ***условиями*** называют условия, события или ситуации, указывающие на скорую материализацию рисков. Например, если в процессе общения заказчик произнес, например, фразы «Мне это не нравится» или «Чего-то тут не хватает», то эта фраза будет триггерным условием, которое предупреждает, 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 информацию, представленную в табл. 1.14: тип и название риска; стратегия воздействия; меры превентивного воздействия; владелец риска (конкретное лицо (группа лиц), которое будет управлять риском; триггерные условия; меры принятия рисков.

---

[1] **Триггер** (англ. *trigger,* «спусковой крючок») — любой стимул, вызывающий у человека автоматическую эмоциональную или поведенческую реакцию.

Таблица 1.14

Пример плана управления рисками

Название риска	Стратегия воздействия	Меры превентивного воздействия	Владелец Риска	Триггерные условия	Меры принятия рисков
1. Риск изменения условий контрактов сотрудников	Ослабление	Проведение переговоров с представителями профсоюза для выявления их целей и интересов	ФИО	Требования от профсоюза о пересмотре контрактов сотрудников кафетерия	Привлечение юриста
2. Риск отсутствия ожидаемого коммерческого эффекта от выполненной работы (оказанной услуги)	Ослабление	Организация обучения сотрудников	ФИО	Обратная связь от работников	Подготовка руководства пользователя программы для ЭВМ
3. Риск отказа партнеров от сотрудничества	Ослабление	Заключение контрактов с партнерами	ФИО	Непредо-ставление скидки	Привлечение юриста

1.3. Механизмы митигации[1] рисков

1.3.1. Элиминирование рисков: ковенанты договора

Несмотря на устоявшуюся деловую практику и закрепленные нормы права, регулирующие ход реализации проектов, направленных на обеспечение государственных (муниципальных) нужд, 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.

Наступление комплаенс-рисков, как отмечают в своей работе Merna T. и Al-Thani F. [57], довольно редкое событие, однако материализация одного подобного риска является достаточным условием для причинения существенного материального ущерба. Например, в рамках судебного разбирательства по делу № А81-9472/2019 одна из ИТ-организаций в г. Томске проиграла спор на общую сумму, равную 1 744 615,65 руб. [67]; по делу № А67-1623/2017 — 2 850 107,39 руб. [68]; по делу № А40-248300/21-5-1672 — 2 000 000,00 руб. [69]; по делу № А40-32033/19-47-287 — 15 830 400,00 руб. [70] и др.

Рассмотрим способы элиминирования универсальных комплаенс-рисков, представляющих собой вероятные события в любой сфере деятельности, актуальные для сделки (проекта) независимо от масштаба, сложности, длительности, типа, способов управления и численности участников команды. Примеры мер элиминирования и ковенанты, позволяющие осуществлять митигацию универсальных комплаенс-рисков, представлены в приложении В.

---

[1] **Митигация** (англ. mitigation) — «смягчение» или «смягчение последствий». В управлении рисками митигация означает усилия, направленные не только на уменьшение тяжести последствий реализации риска, но также и на снижение вероятности реализации рискового события.

Риск несоответствия выполненной работы (оказанная услуга, поставленный товар) ожиданиям заказчика. В качестве примера наступления данного комплаенс-риска можно рассмотреть судебное дело № А67-1623/ 2017, в котором, несмотря на то что истец создал программу для ЭВМ по разработке системы управления проектно-изыскательскими работами на сумму 2850107,39 руб., ответчик все же отказался от оплаты, потому что полученный результат не соответствовал его ожиданиям [68].

Согласно PMBOK Guide® сторона Заказчика ожидает, что проектные работы будут выполнены в полном объеме к определенной дате в рамках согласованного бюджета и на требуемом уровне качества. Логично предположить, что для получения релевантного результата работ (оказанных услуг), ожидаемого заказчиком, в тексте договора должны быть точно сформулированы и корректно формализованы объем, дата окончания, цена и качество выполняемых проектных работ.

При этом необходимо отметить, что согласно действующему гражданскому законодательству существенными условиями договора подряда являются предмет договора, даты начала и 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*) [34].

Риск отказа Заказчика от приемки выполненной работы (оказанная услуга, 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) [34].

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 излагает имеющиеся 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 отказа Заказчика от оплаты выполненной работы (оказанная услуга, поставленный товар). Согласно ст. 702 ГК РФ Заказчик обязуется принять результат выполненных работ и оплатить его [34]. Следовательно, основанием для оплаты выполненных работ является факт приемки работ без претензий и замечаний. Таким образом, для нивелирования комплаенс-риска рекомендуется зафиксировать в тексте договора следующие условия:

1) Подрядчик обязан в течение 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 неполучения от Заказчика 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 нарушения Заказчиком сроков оплаты за выполненную подрядчиком работу (оказанная исполнителем услуга, поставленный поставщиком товар). Для уменьшения негативного влияния данного комплаенс-риска в тексте договора рекомендуется зафиксировать порядок применения мер санкционирования в случае нарушения порядка и сроков оплаты, зафиксировав в тексте договора следующие условия:

1) в случае просрочки Заказчиком оплаты подрядчик вправе потребовать с Заказчика неустойку в размере 0,1 % от договорной 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 заказчику об отказе 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 получения судебного иска от Заказчика (Подрядчик, исполнитель, поставщик). 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 ситуацию, когда договор об отчуждении исключительного права на программу для ЭВМ не был заключен и оформлен в письменной форме согласно п. 2 ст. 1234 ГК РФ [34].

В этом случае сделка считается незаключенной, а исключительное право — не переданным от правообладателя к правоприобретателю. Последствия от нарушения необходимого условия относительно письменного оформления договора об отчуждении исключительного права на программный продукт представлены в деле № А40-81328/2011 [71], 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 [34]. Следовательно, для нивелирования данного комплаенс-риска необходимо, чтобы в тексте договора существенные условия были точно сформулированы и корректно формализованы.

Риск невозможности досрочного расторжения сделки в одностороннем порядке. 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 неточной формулировки и/или некорректной формализации предмета договора. Уменьшение вероятности наступления данного комплаенс-риска возможно при повышении уровня зрелости управления коммуникациями и 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 управления коммуникациями проекта, так как выработка корректных и точных формулировок возможна при согласованных действиях заинтересованных сторон.

Риск отсутствия предусмотренного порядка распределения экономии, которая возможна по факту выполненных работ (оказанные услуги, поставленные товары) между договаривающимися сторонами. В соответствии со ст. 710 ГК РФ в случаях, когда фактические расходы Подрядчика оказались меньше зафиксированных в тексте договора, Подрядчик сохраняет право на оплату работ по цене, предусмотренной договором [34].

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 нарушения Заказчиком сроков предоставления информации, необходимой для выполнения работ (оказание услуг, поставка товаров), либо отсутствия данной информации по вине Заказчика. 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 необходимости изменения требований (появление новых и/или существенное уточнение ранее согласованных требований) в процессе выполнения работ (оказание услуг, поставка товаров). В качестве примера можно рассмотреть дело № А55-9384/2018 [72], где внесение Заказчиком частых корректировок в ранее согласованное техническое задание привело к тому, что новые требования Подрядчику пришлось реализовывать за свой счет. Уменьшение вероятности материализации комплаенс-риска и его возможного негативного влияния зависит от методического инструментария, используемого Подрядчиком для выполнения работ (оказания услуг), — Agile или Waterfall (гибкая или каскадная методики разработки и управления проектами).

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 и прочие работы, не поименованные в договоре и приложениях к нему, не входят в объем работ по договору и выполняются Подрядчиком исключительно на основании заключенных сторонами дополнительных соглашений либо самостоятельных договоров».

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

а) изменения не вносятся в утвержденные подрядные работы;

б) изменения вносятся в утвержденные подрядные работы;

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

Сроки реализации и стоимость изменений требований определяются подрядчиком».

Риск несоответствия спецификации (устав, техническое задание и/или другая документация) требованиям национальных стандартов либо недостоверности и предоставленной в неполном объеме содержащейся в ней информации. Уменьшить вероятность материализации комплаенс-риска можно, 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 (оказание услуги). Согласно ст. 715 ГК РФ Заказчик вправе в любое время проверять ход и качество выполняемой

работы [34]. Уменьшение вероятности материализации комплаенс-риска возможно при использовании инструментария управления проектами PMBOK Guide®, PRINCE2®, SCRUM и др.

Риск отсутствия у Заказчика корпоративной культуры, квалифицированных специалистов и опыта ведения деятельности в едином информационном пространстве с использованием информационных систем (ИС). 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 отсутствия у Заказчика отлаженных корпоративных процедур 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 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 пренебрежения условием о необходимости включения в процесс работы над созданием и согласованием проектных документов ВСЕХ заинтересованных лиц со стороны Заказчика, участвующих в бизнес-процессах, автоматизируемых информационной системой. Уменьшение вероятности материализации данного комплаенс-риска требует определенной зрелости управления коммуникациями проекта, а именно — наличия механизмов управления по своевременному созданию, сбору, распространению, хранению, получению и использованию информации.

Риск возможной реструктуризации организации Заказчика (изменения организационной структуры, функциональных обязанностей, бизнес-процессов, локальных актов, финансово-экономической модели и др.). Для нивелирования комплаенс-риска рекомендуется включить реестр рисков в качестве приложения к договору, 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 неисполнения Подрядчиком (исполнитель, поставщик) обязательств, предусмотренных договором (например, невыполнение заявленных требований в срок либо невыполнение в полном объеме и др.). Для увеличения лояльности Заказчика и уменьшения вероятности материализации комплаенс-риска в части невыполнения Подрядчиком заявленных требований в срок или работ в полном объеме в тексте договора рекомендуется зафиксировать порядок санкционирования посредством добавления 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 [34].

Риск сокрытия и/или искажения Подрядчиком (исполнитель, поставщик) информации о реальном положении дел по договорным обязательствам перед Заказчиком. 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 [34]. Информирование заказчика о реальном положении дел в ИТ-проекте является обязательством подрядчика, которое закреплено в действующем гражданском законодательстве.

Риск отсутствия у заинтересованных сторон общего видения конечного создаваемого продукта. Уменьшение вероятности материализации комплаенс-риска требует определенного уровня зрелости в части управления коммуникациями проекта, а именно — наличия механизма управления, включающего структурные и инфраструктурные элементы, предоставляющие возможность своевременного создания, сбора, распространения, хранения, получения и использования информации.

Риск невозможности Подрядчиком (исполнитель, поставщик) в процессе выполнения работ (оказание услуг, поставка товаров) исполнения заявленных в договоре обязательств собственными силами. Согласно ст. 706 ГК РФ, если сделка требует от Подрядчика выполнить работу лично, то Подрядчик вправе привлечь к исполнению своих обязательств других лиц (субподрядчиков) [34].

Риск выявления Подрядчиком (исполнитель, поставщик) скрытых, не обнаруженных на этапе планирования, источников дополнительных затрат. В силу ст. 709 ГК РФ цена работы может быть твердой или приблизительной [34]. 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 (исполнитель, поставщик). Согласно ст. 152 ГК РФ деловая репутация признается нематериальным благом, защита которого гарантирована действующим законодательством. За распространение информации, которая порочит честь и достоинство, законодателем установлена гражданско-правовая, административная и уголовная ответственность [34]. Административным законом предусмотрена ответственность за оскорбление,

т. е. унижение чести и достоинства, выраженное в неприличной форме (ст. 5.61 КоАП РФ) [60]. Совершение указанного правонарушения влечет наложение административного штрафа. Уголовным кодексом предусмотрено понятие «клевета», т. е. распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию (ст. 128.1 УК РФ) [73].

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. Примером материализации комплаенс-риска является дело № 2-38/2019 (2-4158/2018) ~ М-608/2018, в котором рассматривался спор между программистом, создавшим программу «eLearning Metadata Manager», с одной стороны, и ООО «Интервим» и Veeam Software Group GmpH, с другой стороны. Согласно материалам дела после увольнения программист обнаружил, что в созданной им программе исчез знак охраны авторского права «©», что стало основанием для обращения в суд [74]. 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, договорами отчуждения исключительного права, передачи исключительного права на основании лицензии, авторского заказа, трудового договора и др.

Риск запрещения правообладателем (автором) использования результатов интеллектуальной деятельности. В качестве примера материализации данного комплаенс-риска можно рассмотреть материалы дела № А40-202764/18-110-1552 [75], 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) [76], 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».

Показательно и дело № А40-117808/10-12-740 [77], 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 [34]. 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 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 [34].

Риск несоответствия полученного субподрядчиком результата (оказанной услуги, поставленного товара) 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 (компьютеры, серверы 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 [34]).

Риск гибели и/или повреждения электронного оборудования (компьютеры, серверы 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 [34]).

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» понятие «***коммерческая тайна***» трактуется как 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 [78]. 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 следующее:

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 при условии добросовестного исполнения предусмотренных договором обязательства, а также обеспечения «правовой чистоты» 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 (оказание услуг, поставка 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. Обстоятельствами непреодолимой силы являются стихийные бедствия, военные действия любого характера, блокады, эмбарго, забастовки, запрет на экспорт/импорт, эпидемия, антитеррористические мероприятия, розыскные и оперативные мероприятия правоохранительных органов».

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

1.3.2. Страхование рисков

Согласно ст. 2 Закона РФ № 4015-1 «Об организации страхового дела в Российской Федерации» **страхование** определяется как отношения по защите интересов физических и юридических лиц при наступлении определенных страховых случаев за счет денежных фондов, формируемых страховщиками из уплаченных страховых премий (страховых взносов) и иных средств страховщиков [79].

В соответствии с нормами гл. 48 ГК РФ одна сторона ***(страховщик)*** обязуется в течение известного срока нести риск, который в случае своей материализации может причинить ущерб объекту страхования, и при наступлении ***страхового случая*** уплатить другой стороне ***(страхователю)*** или третьему лицу ***(выгодоприобретателю)*** страховое вознаграждение ***(страховую сумму)***. Другая же сторона (страхователь), обязуется уплатить страховщику за это известный взнос ***(страховую премию)*** [34] (рис. 1.14).

Законодатель согласно ст. 927 ГК РФ в зависимости от способа вовлечения субъектов в страховые правоотношения разделяет страхование на следующие виды [34]:

1) добровольное страхование;
2) обязательное страхование.

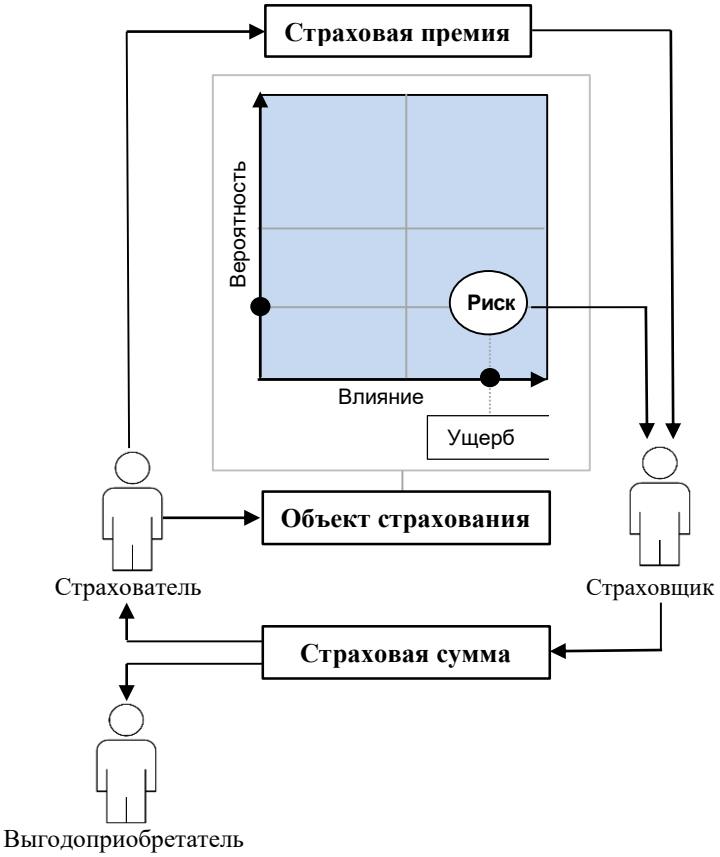

Рис. 1.14. Страховые правоотношения

Добровольное страхование осуществляется на основании договоров страхования, заключаемых гражданином или юридическим лицом (*страхователем*), со страховой организацией (*страховщиком*). При добровольном страховании отношения основаны

на ***принципе свободы договора*** (ст. 421 ГК РФ): стороны свободны в принятии решения о заключении договора, объект и иные условия страхования определяются соглашением сторон [34].

Обязательное страхование — вид страхования, при котором обязанность страхователя заключить договор страхования устанавливается законом. Обязательное страхование предусматривает [34]:

- установление в законе для определенных в нем субъектов обязанности страховать жизнь, здоровье, имущество и другое на случай причинения им вреда (ущерба);
- риск гражданской ответственности, которая может наступить вследствие причинения вреда жизни, здоровью и (или) имуществу других лиц (ст. 931 ГК РФ);
- предпринимательский риск, который может реализоваться в случае нарушения договоров с другими лицами (ст. 933 ГК РФ).

Обязательное страхование осуществляется путем заключения договоров страхования (ст. 936 ГК РФ) [34]. Законом определяются: объекты, подлежащие обязательному страхованию; *риски*, от которых они должны быть застрахованы; минимальные размеры страховых сумм.

С точки зрения риск-менеджмента в страхование могут и должны передаваться риски, имеющие низкую вероятность реализации и влекущие высокие (катастрофические) последствия для организации-страхователя.

В зависимости от объекта страхования выделяются:

1) ***имущественное страхование***, в котором объектом страхования являются интересы, связанные с имуществом. Согласно ст. 929 ГК РФ выделяются следующие подвиды [34]:

- риск утраты (гибели), недостачи или повреждения определенного имущества (ст. 930 ГК РФ);
- риск ответственности по обязательствам, возникающим вследствие причинения вреда жизни, здоровью или имуществу других лиц, а также ответственности по договорам — риск гражданской ответственности (ст. 931, ст. 932 ГК РФ);
- риск убытков от предпринимательской деятельности из-за нарушения своих обязательств контрагентами предпринимателя

или изменения условий этой деятельности по не зависящим от предпринимателя обстоятельствам, в том числе риск неполучения ожидаемых доходов (*предпринимательский риск*) (ст. 933 ГК РФ);

2) ***личное страхование***, в котором объектом страхования являются интересы, связанные с личностью, принадлежащими ей неотчуждаемыми нематериальными благами, такими как жизнь и здоровье. В соответствии со ст. 934 ГК РФ к личному страхованию относится страхование имущественных отношений, связанных со следующими событиями [34]:

- причинение вреда жизни или здоровью самого страхователя или другого названного в договоре гражданина (застрахованного лица);
- достижение страхователем определенного возраста или наступление в его жизни иного предусмотренного договором события (страхового случая).

В зависимости от объекта страхования различаются страховые риски, порядок и условия определения страховой суммы и размера страховых выплат.

ГК РФ не содержит единого определения договора страхования: приводится два понятия — «договор имущественного страхования» (ст. 929 ГК РФ) и «договор личного страхования» (ст. 934 ГК РФ) [34].

Сторонами, возникающего из договора страхования правоотношения, являются:

1) ***страхователь*** — физическое или юридическое лицо, заключившее со страховой организацией договор страхования (ст. 927 ГК РФ). Страхователь может заключать договор в пользу третьего лица — ***выгодоприобретателя***. Хотя выгодоприобретатель не является стороной сделки, на него возлагаются определенные обязанности (ст. 939 ГК РФ) [34];

2) ***страховщик*** — юридическое лицо, созданное в соответствии с законодательством РФ для осуществления страхования, перестрахования, взаимного страхования, и получившее лицензии в установленном Законе РФ № 4015-1 «Об организации стра-

хового дела в Российской Федерации» порядке [79]. Страховщики осуществляют связанные с исполнением обязательств по договору страхования действия:

- производят оценку страхового риска;
- получают страховые премии (страховые взносы);
- формируют страховые резервы;
- инвестируют активы;
- определяют размер убытков и ущерба;
- производят страховые выплаты.

Существенные условия договора страхования, т. е. условия по которым должно быть достигнуто соглашение при заключении сделки, определяются ст. 942 ГК РФ отдельно применительно к имущественному и личному страхованию [34]. Следует отметить, что круг этих существенных условий для договоров имущественного и личного страхования сходен. ***Существенными условиями*** являются условия об объекте страхования, страховом риске, страховой сумме и сроке действия договора. Однако содержание этих условий применительно к имущественному и личному страхованию различно по объектам страхования, страховым рискам, порядку определения страховой суммы.

Объектом имущественного страхования согласно ст. 942 ГК РФ является определенное имущество или иной имущественный интерес; в договоре личного страхования должно быть обозначено застрахованное лицо [34].

Договор страхования является ***алеаторной (рисковой) сделкой***, рисковой характер которой выражается в неопределенности результатов сделки: страховой случай может наступить, а может не наступить; неизвестен размер ущерба от страхового случая.

В Законе РФ № 4015-1 «Об организации страхового дела в Российской Федерации» ***«страховым риском»*** признается предполагаемое событие, на случай наступления которого производится страхование [79]. Событие, которое предусматривается сторонами договора страхования в качестве риска, должно иметь признаки *возможности (вероятности), неизвестности, определенности во времени*.

Наступление риска не должно вызываться поведением лица, его волей. Вредоносное событие не должно, по общему правилу, быть неизбежным либо, если оно таковым является (например, смерть человека), неизвестным должно быть время его наступления.

Определенность во времени означает будущность предполагаемого события. Кроме того, определенность во времени означает, что страховщик принимает на себя соответствующий риск на период времени, предусмотренный договором страхования.

По общему правилу, договор страхования, заключенный при отсутствии страхового риска, ***ничтожен*** (ст. 168 ГК РФ) [34]. Если страховой риск — это угрожающая объекту страхового интереса опасность, то страховой случай — это реализованный страховой риск. **Страховой случай** — совершившееся событие, предусмотренное договором страхования, с наступлением которого возникает обязанность страховщика произвести страховую выплату страхователю, застрахованному лицу, выгодоприобретателю или иным третьим лицам. Важно отметить, что страховой случай имеет сложный состав, включающий не только само событие, но и причиненный объектам страхового интереса ущерб.

Согласно Закону РФ № 4015-1 «Об организации страхового дела в Российской Федерации» признаками страхового случая являются *вероятность* и *случайность* его наступления [79]. Представляется, что признак вероятности наступления следует относить к категории страхового риска, так как страховой случай — уже свершившиеся событие.

Случайность наступления события, отнесенного к страховому риску, означает отсутствие вины в этом сторон договора, а также выгодоприобретателя или застрахованного лица. Страховщик освобождается от страховой выплаты, если страховой случай наступил вследствие умысла страхователя, выгодоприобретателя или застрахованного лица.

Для договора страхования существенным является условие о размере страховой суммы. В силу ст. 947 ГК РФ ***«страховая сумма»*** определяется как сумма, в пределах которой страховщик

обязуется выплатить страховое возмещение по договору имущественного страхования или которую он обязуется выплатить по договору личного страхования [34]. Эта сумма определяется соглашением страхователя со страховщиком.

Еще одно существенное условие договора страхования — **срок**. Срок оперяется соглашением сторон, однако в отношении отдельных видов обязательного страхования он устанавливается законодательством. Так, по общему правилу, срок действия договора страхования гражданской ответственности владельца транспортного средства — один год.

К существенным условиям договора страхования помимо перечисленных в ст. 942 ГК РФ, относится ***размер страховой премии*** [34]. Страховая премия, хотя и именуется платой за страхование, с экономической точки зрения неоднородна и включает себестоимость страхования для страховщика, а также определенную надбавку, которую можно рассматривать непосредственно как вознаграждение страховщика за принятый на себя риск. Страховая премия без указания надбавки именуется ***нетто-премией***, а с учетом надбавки — ***брутто-премией***.

В договоре страхования могут содержаться и иные условия. Например, условия о франшизе. ***Франшиза*** — освобождение страховщика от страховой выплаты, если размер ущерба не превышает в договоре величины причиненного ущерба. Франшиза бывает:

условная, подразумевающая освобождение страховщика от возмещения ущерба, не превышающего установленную договором величину, и его полное покрытие, если размер ущерба эту величину превысил;

безусловная, применяемая в любом случае, так как ущерб, независимо от его размера, подлежит возмещению за вычетом франшизы.

Договор страхования заключается в письменной форме (ст. 940 ГК РФ) [34]. Несоблюдение этого требования влечет недействительность договора. Также договор страхования может быть заключен путем составления одного документа либо вручением страховщиком страхователю на его основании *страхового полиса*, подписанного страховщиком.

Контрольные вопросы для раздела 1

1. Чем различаются понятия «неопределенность» и «риск»?
2. Назовите и охарактеризуйте основные принципы управления рисками согласно ГОСТ Р ИСО 31000-2019.
3. Перечислите основные элементы инфраструктуры управления рисками согласно ГОСТ Р ИСО 31000-2019. Каковы их функции?
4. Перечислите и охарактеризуйте процессы управления рисками согласно ГОСТ Р ИСО 31000-2019.
5. На какие классификационные группы распределяются риски?
6. Назовите и охарактеризуйте методы, которые используются для идентификации рисков.
7. Назовите и охарактеризуйте методы, которые используются для анализа рисков.
8. Чем отличаются количественные и качественные методы оценки рисков?
9. Опишите механизм качественной оценки рисков с использованием коэффициентов вербально-числовой шкалы Харрингтона.
10. Перечислите и охарактеризуйте стратегии управления рисками.

2. ОСОБЕННОСТИ РИСК-МЕНЕДЖМЕНТА В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ

2.1. 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 газопроводах «Северный поток-1» и «Северный поток-2», 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 [80–86].

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 политики в области обеспечения национальной безопасности России, является Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» [87], где под **угрозой национальной безопасности** понимается совокупность условий и факторов, создающих прямую или косвенную возможность причинения ущерба ***национальным интересам России***.

Проведенный анализ правовых документов[1], регулирующих формирование государственной политики в области обеспечения национальной безопасности, а также доктринальных[2] стратегических актов, показал, что понятие «**риск**» определяется как некая совокупность факторов, запускающих процесс трансформации вызовов в угрозы, где **вызовы** — это совокупность факторов, способных при определенных условиях приводить к возникновению угроз. Связи между вызовами, рисками, угрозами и национальными интересами России представлены на рис. 2.1.

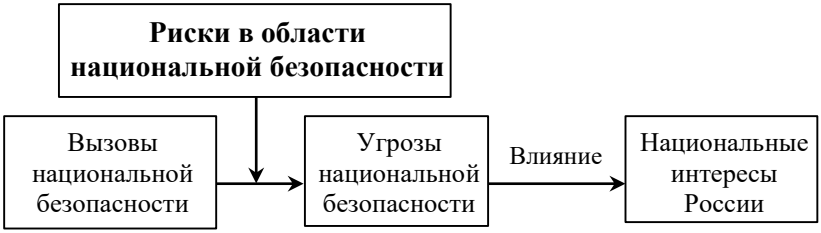

Рис. 2.1. Связь между вызовами, рисками и угрозами в области национальной безопасности

В соответствии со ст. 23 Федерального закона от 28.06.2014 № 172-ФЗ «О стратегическом планировании в Российской Федерации» основу обеспечения национальной безопасности России составляет ***стратегический прогноз***, который должен включать [88]:

---

[1] Конституция Российской Федерации); Федеральный закон № 172-ФЗ «О стратегическом планировании в Российской Федерации»; Федеральный закон «О безопасности» № 390-ФЗ; 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.

[2] Доктринальный — *юр*. относящийся к сфере научно-правового знания, а не установленный нормативно (законом или иными источниками права). В группу чисто доктринальных источников права относятся комментарии отдельных нормативно-правовых актов, послания, выступления и иные высказывания Президента РФ, определяющие направления общественного развития и правового регулирования; имеющий общепризнанный научный характер.

- оценку рисков социально-экономического развития и угроз национальной безопасности;
- оптимальный сценарий преодоления рисков и угроз национальной безопасности;
- поэтапные прогнозные оценки вероятного состояния социально-экономического потенциала и национальной безопасности.

Согласно Федеральному закону от 28.12.2010 № 390-ФЗ «О безопасности» понятие **«безопасность»** — это состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз [89].

В Стратегии национальной безопасности понятие «**национальная безопасность»** трактуется как состояние защищенности национальных интересов России от внешних и внутренних угроз, при котором обеспечивается [87]:

- реализация конституционных прав и свобод граждан;
- достойные качество и уровень жизни;
- гражданский мир и согласие в стране;
- охрана государственного суверенитета России;
- независимость и государственная целостность России;
- социально-экономическое развитие страны.

Согласно вышеупомянутой Стратегии структура национальной безопасности включает восемь основных звеньев, представленных на рис. 2.2.

Рис. 2.2. Структура национальной безопасности России

Экономическая безопасность. Механизмы обеспечения экономической безопасности закреплены в Стратегии экономической безопасности, утвержденной Указом Президента Российской Федерации от 13.05.2017 № 208 [90]. Важно отметить, что ключевое место в обеспечении экономической безопасности России занимает топливно-энергетический комплекс (ТЭК), что обуславливает включение в сферу экономической безопасности механизмов обеспечения энергетической безопасности.

Военная безопасность. Механизмы обеспечения военной безопасности закреплены в Военной доктрине, утвержденной Президентом Российской Федерации 25.12.2014 № Пр-2976 [91], согласно которой для реализации военной безопасности необходимо выполнение следующих условий:

- элиминирование угроз, связанных с применением военной силы;
- способность противостоять враждебной военной силе.

Государственная и общественная безопасность. В соответствии с поправками к Конституции от 14.03.2020 в части ст. 67 [92] 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 на период до 2025 года, утвержденной Президентом РФ 14.11.2013 № Пр-2685) [93] 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) [73] и др. Основными показателями общественной безопасности являются ***уровень преступности*** и ***уровень правонарушений***.

Информационная безопасность. Механизмы обеспечения информационной безопасности закреплены в Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ от 05.12.2016 № 646 [94]. Важно отметить,

что Информационная доктрина направлена 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. (см. ч. III Информационной доктрины).

Безопасность в сфере науки, технологий и образования. Президентом Российской Федерации 13.05.2017 был утвержден Указ «О Стратегии экономической безопасности Российской Федерации на период до 2030 года» [90], в рамках которого 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.

Также следует отметить, что механизмы обеспечения безопасности в сфере науки, технологий и образования закреплены в Стратегии научно-технологического развития, утвержденной Указом Президента Российской Федерации от 01.12.2016 № 642 [95]. Согласно Стратегии научно-технологического развития такие понятия, как «проблема», «угроза» и «возможность» объединены в одно понятие «***большие вызовы***», означающее совокупность проблем, угроз и возможностей, сложность и масштаб которых таковы, что они не могут быть решены исключительно за счет увеличения материальных ресурсов.

Экологическая безопасность. Указом Президента Российской Федерации от 19.04.2017 № 176 утверждена «Стратегия экологической безопасности Российской Федерации на период до 2025 года», целями которой являются [96]:

- 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 в Стратегии экологической безопасности определяются следующие понятия:

- ***глобальные* (*внешние*) *вызовы*** — последствия изменения климата на планете, рост потребления природных ресурсов при сокращении их запасов, сокращение биологического разнообразия и пр.;
- ***внутренние вызовы*** — следствие увеличения объема образования отходов производства и потребления при низком уровне их утилизации, усиления деградации земель и почв, сокращения количества видов растений, криминализация и наличия теневого рынка в сфере природопользования и др.;
- ***внешние угрозы*** — 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.

Безопасность в духовно-нравственной и культурной сферах. В соответствии с поправками к Конституции от 14.03.2020 в части ст. 67.1 [92] 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, что обуславливает ее поддержку и охрану 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 создают угрозу естественному продолжению жизни [87].

Международная безопасность. Основополагающим международно-правовым актом, который заложил основы существующего международного порядка, является Устав Организации Объединенных Наций (ООН), принятый 26.06.1945 [97]. Собы-

тия XX в. показали, 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 Стратегии экономической безопасности понятие ***«экономическая безопасность»*** трактуется как 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 [90].

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 Федеральный закон США «О противодействии противникам Америки посредством санкций», принятые Правительством США [98]. 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 действий недружественных стран в Стратегии экономической безопасности закрепляется перечень 25 угроз экономической безопасности (приложение Г) [90]. Для оценки этих угроз применялись качественные методы, методология которых закреплена в ГОСТ Р ИСО 31000-2019 [2] и ГОСТ Р 58771-2019 [3].

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 десять респондентов, имеющих научные степени кандидатов (восемь респондентов) и докторов экономических наук (два респондента).

Численность экспертной группы обусловлена двумя факторами:

1) возможностью верификации экспертных оценок;

2) возможностью получения более достоверных оценок при большем количестве экспертных мнений.

Оценка значений вероятностей и влияний включала следующие этапы:

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

Оценка значений вероятностей и влияний осуществлялась с использованием коэффициентов вербально-числовой шкалы Харрингтона (рис. 2.3).

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

Наиболее опасными угрозами 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).

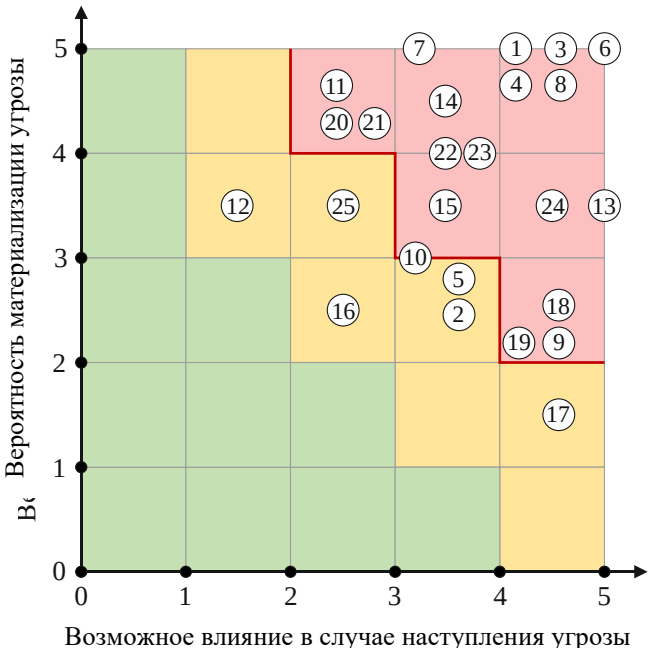

Рис. 2.3. Матрица угроз в сфере экономической безопасности

Высокая концентрация угроз в «критической области» указывает на агрессивное поведение недружественных стран, которое направлено на дестабилизацию экономики России и ухудшение уровня жизни населения. Данное обстоятельство позволяет заключить, что концентрация фокуса государственного внимания должна быть сосредоточена на развитии системы стратегического планирования в сфере экономики, создании условий для разработки и внедрения современных технологий, развитии финансовой системы, повышении региональной зрелости России и эффективности внешнеэкономического сотрудничества, обеспечении безопасности экономической деятельности и развитии человеческого потенциала.

Оценка угроз военной безопасности

В Военной доктрине разделяются понятия «военная опасность» и «военная угроза» [91]. Под ***военной опасностью*** понимаются межгосударственные (внутригосударственные) отношения, которые способны при определенных условиях привести к возникновению военной угрозы**.** ***Военная угроза*** определяется как состояние межгосударственных (внутригосударственных) отношений, для которого характерна реальная возможность возникновения военного конфликта (рис. 2.4).

Рис. 2.4. Влияние категорий военной опасности и военной угрозы на национальные интересы России

В Военной доктрине зафиксированы пять основных военных угроз (рис. 2.5), перечень которых представлен в приложении Г.

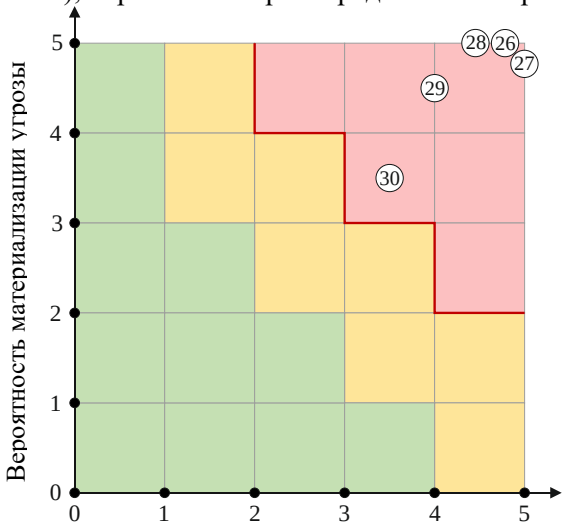

Рис. 2.5. Матрица угроз в сфере военной безопасности

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 назвать новую редакцию Военной доктрины Союзного государства, принятой 04.11.2021 Россией и Республикой Беларусь [99]. 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 Вооруженных сил России в заданной степени готовности к боевому применению, расширение взаимодействия с государствами-участниками БРИКС[1], а также укрепление системы коллективной безопасности в рамках ОДКБ[2].

Оценка угроз информационной безопасности

Расширение областей применения информационных технологий 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 исследований экспертно-аналитического центра Info-Watch[3]. Согласно

---

[1] БРИКС — (англ. BRICS — сокращение от Brazil, Russia, India, China, South Africa) — межгосударственное объединение Федеративной Республики Бразилии, Российской Федерации, Республики Индии, Китайской Народной Республики и Южно-Африканской Республики. С 1 января 2024 г. к БРИКС присоединились Египет, Иран, ОАЭ, Саудовская Аравия и Эфиопия.

[2] ОДКБ — Организация Договора о коллективной безопасности — региональная международная организация в области коллективной безопасности с участием нескольких постсоветских государств (государства, раннее входившие в состав Советского союза).

[3] InfoWatch — ведущий российский разработчик технологий и продуктов для снижения рисков информационной безопасности, защиты и анализа корпоративных данных для компаний.

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 можно отметить доклад замминистра иностранных дел России Сыромолотова О., в котором сообщалось, что НАТО отрабатывает кибердары по российским сетям и моделирует поражение госучреждений в Калининградской области и энергосистемы Москвы [100]. Яркими примерами подобных кибердаров являются атаки в июне 2023 г. на радиостанции России, в результате чего в нескольких регионах были озвучены фейковые сообщения [101]. В качестве другого примера кибердара можно привести предпринятую 05.07.2023 атаку на сайт и мобильное приложение ОАО «Российские железные дороги» [102].

Для элиминирования подобных угроз в Информационной доктрине (раздел III) закрепляются основные информационные угрозы и состояние информационной безопасности России [94]. Перечень основных угроз в сфере информационной безопасности, оценки их вероятностей и влияний представлен в приложении Г. Анализ матрицы угроз в сфере информационной безопасности показывает их высокую концентрацию в «критической области», что свидетельствует об их экзистенциальном характере (рис. 2.6).

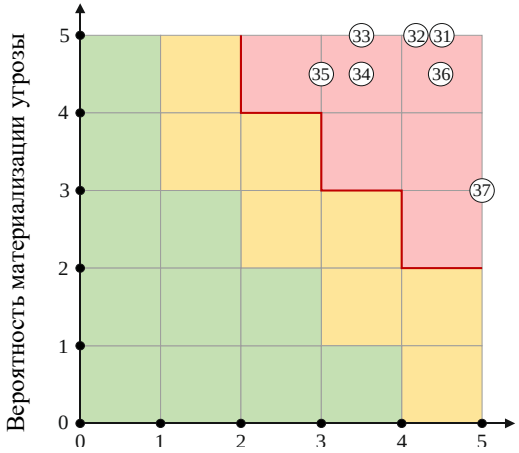

Рис. 2.6. Матрица угроз в сфере информационной безопасности

Например, если в зимний период будет совершена кибератака на критические информационные инфраструктуры энергетики и Топливно-энергетический комплекс (ТЭК) Сибирского федерального округа, то данная атака подвергнет опасности жизни и здоровье более 17 млн чел. В качестве примера мер элиминирования кибератак на отечественные КИИ можно привести закрепленные в Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [103] императивные механизмы, направленные на поддержание информационного суверенитета России в ключевых областях, таких как банковский сектор, государственное управление, медицина, образование и др.

2.2. Управление рисками при осуществлении государственного и муниципального контроля (надзора)

Риск-ориентированный подход

В послании Федеральному Собранию от 04.12.2014 [104] Президент Российской Федерации обозначил необходимость изменения подходов к 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, создает проблемы и закрывает 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.

На уровне федерального законодательства в Федеральный закон № 294-ФЗ «О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля» в новой редакции

от 13 июля 2015 г. были внесены первые упоминания о риск-ориентированном подходе, в частности, в Закон № 294-ФЗ была включена ст. 8.1. «Применение риск-ориентированного подхода при организации государственного контроля (надзора)» [105].

Новая норма предусматривала при организации отдельных видов госконтроля органами государственного контроля (надзора) с 1 января 2018 г. **применение 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 юридического лица и/или индивидуального предпринимателя 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» [106]. В частности, предусматривалась апробация до 2018 г нового механизма, включающего три вида госнадзора:

1) федеральный государственный надзор в сфере связи;

2) федеральный государственный пожарный надзор;

3) федеральный государственный санитарно-эпидемиологический надзор.

Постепенно перечень видов федерального государственного контроля (надзора), в отношении которых применялся риск-ориентированный подход, расширялся, и в 2021 г. данный перечень насчитывал 34 позиции. В дальнейшем планировалось 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 [107].

Согласно данной 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:

1) 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;

2) 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;

3) переоценка на регулярной основе рисков в зависимости от фактического распределения ущерба по категориям риска (классам опасности), в том числе с использованием массивов «больших данных»;

4) 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, что закреплено в Федеральном законе от 31.07.2020 № 248-ФЗ «О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации» [108]. Собственно, понятие «риск-ориентированный подход» в документе не приведено, 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 [108]. 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) и 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 [108] 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.

Следует отметить, что систему управления рисками причинения вреда (ущерба) планировалось распространить только на государственный контроль (надзор) в Российской Федерации.

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.

В ст. 22 Закона № 248-ФЗ [108] содержатся определения следующих 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 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).

Категории и индикаторы риска

В Законе № 248-ФЗ в ч. 1 выделено шесть категорий риска причинения вреда (ущерба) [108]:

1) чрезвычайно высокий риск;
2) высокий риск;
3) значительный риск;
4) средний риск;
5) умеренный риск;
6) низкий риск.

В зависимости от принадлежности объектов контроля к определенным категориям риска будут зависеть виды и периодичность проведения в отношении них плановых контрольных (надзорных) мероприятий (табл. 2.1).

Таблица 2.1

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

Категории риска	Периодичность проведения плановых контрольных (надзорных)мероприятий
Чрезвычайно высокий риск	Максимальная частота проведения — не менее одного, но не более двух контрольных (надзорных) мероприятий в год
Высокий риск	Средняя частота проведения — 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 — не менее одного контрольного (надзорного) мероприятия в шесть лет и не более одного контрольного (надзорного) мероприятия в три года
Умеренный Риск	
Низкий риск	Не проводятся

Следует отметить, что в первоначальной версии Законопроекта о госконтроле была предусмотрена иная периодичность плановых проверок для объектов контроля различный категорий риска:

- 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);
- категорий 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;
- категорий среднего и умеренного риска — не менее одного контрольно-надзорного мероприятия в шесть лет и не более одного мероприятия в два года.

Но многие эксперты указывали на несовершенство исходного текста норм, приведенных в первоначальной версии Законопроекта о госконтроле. 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» [109]. 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 [108]).

В первоначальной редакции Законопроекта о госконтроле страхованию рисков причинения вреда (ущерба) была отведена отдельная статья [109], 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;

– о 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 разной частотой случаев фактического причинения вреда (ущерба);

- ***добросовестность контролируемых лиц,*** оцениваемая по сведениям о выполненных контролируемыми лицами действиях:

– реализация мероприятий по снижению риска причинения вреда и его предотвращению;

– внедрение сертифицированных систем внутреннего контроля;

– предоставление доступа контрольному (надзорному) органу к своим информационным ресурсам;

– независимая оценка соблюдения обязательных требований;

– добровольная сертификация, подтверждающая повышенный необходимый уровень безопасности охраняемых законом ценностей;

– заключение 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 федерального контроля утверждается федеральным органом исполнительной власти: для регионального контроля — высшим исполнительным органом государственной власти субъекта Российской Федерации; для муниципального контроля — представительным органом муниципального образования (ч. 10 ст. 23 Закона № 248-ФЗ [108]).

В качестве примера индикаторов риска для регионального контроля можно привести перечень индикаторов риска, утвержденный Постановлением Администрации Томской области от 08.07.2022 № 315а [110]. 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. Примером таких сведений могут быть:

- сведения, собранные в ходе проведения профилактических мероприятий, контрольных (надзорных) мероприятий;
- результаты использования специальных режимов госконтроля (надзора);

- сведения, полученные от госорганов, органов местного самоуправления и организаций в рамках межведомственного информационного взаимодействия при реализации полномочий по лицензированию и иной разрешительной деятельности, из отчетности по результатам предоставления государственных и муниципальных услуг;
- сведения из обращений граждан и организаций (включая контролируемые лица) и сообщений СМИ;
- сведения, содержащиеся в информационных ресурсах, в том числе обеспечивающих маркировку, прослеживаемость, учет, автоматическую фиксацию информации.

Перечень таких сведений об объектах контроля является открытым и приведен в ч. 1 ст. 24 Закона 248-ФЗ [108]).

2.3. Риски в сфере закупок товаров, работ и/или услуг для обеспечения государственных и муниципальных нужд

Универсальными проблемами как для коммерческих, так и государственных (муниципальных) заказчиков являются:

- 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;
- низкие шансы на успешное закрытие сделок.

В частности, согласно данным АИС «Мониторинг» средний уровень исполнения государственных контрактов до их расторжения за 2017–2019 гг. составил 66 % [111]. Среди основных причин прекращения отношений Аналитический центр при Правительстве РФ называет ***существенное неисполнение подрядчиками (исполнителями, поставщиками) своих обязательств***, в которых особенно остро их недобросовестность и недостаточная квалификация проявлялись во время выполнения работ по созданию ИТ-продуктов. 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 [112].

Примеры

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 [113]. Вследствие 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 [114]. Недобросовестность подрядчика явилась причиной обращения государственного заказчика в суд.

Дело № А56-107933/2019. Государственный заказчик отказался от исполнения контракта на сумму 9 982 051,75 руб. в одностороннем порядке [115]. Причиной конфликта между сторонами стало отсутствие у подрядчика документов, подтверждающих его исключительные права на медицинскую ИС «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) [116].

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 ИС АРМ «Поликлиника» [117].

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

Пример

Согласно отчету Департамента госзаказа Томской области общая стоимость заключенных контрактов в 2022 г. по сравнению с 2018 г. увеличилась на 34,8 %, с 6879,50 млн руб. до 19756,74 млн руб. (табл. 2.2) [118]. За 2019–2022 гг. 52 ИТ-организации Томской области, занятые разработкой ПО и консультационными услугами в данной области, заключили 1067 контрактов, в 2019 г. число заключенных контрактов составило 528 млн руб., в 2020 г. — 522 млн руб., в 2021 г. — 519 млн руб., в 2022 г. — 288 млн руб. Средняя цена 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 2.2

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.	5757	5133	4908	5031	5422
Общая стоимость заключенных контрактов, млн руб.	6879,5	9102,37	14310,99	14873,78	19756,74

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. Данные механизмы закреплены, в частности, в специальных нормах Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ [119] и Федерального закона «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 № 223-ФЗ [120].

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.

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, представлены на рис. 2.7.

Согласно ст. 24 Закона № 44-ФЗ государственные (муниципальные) заказчики обязаны использовать конкурентные способы определения контрагента либо осуществлять закупки у единственного подрядчика (исполнителя, поставщика) (рис. 2.8).

Рис. 2.7.Этапы проведения закупок согласно Закону № 44-ФЗ

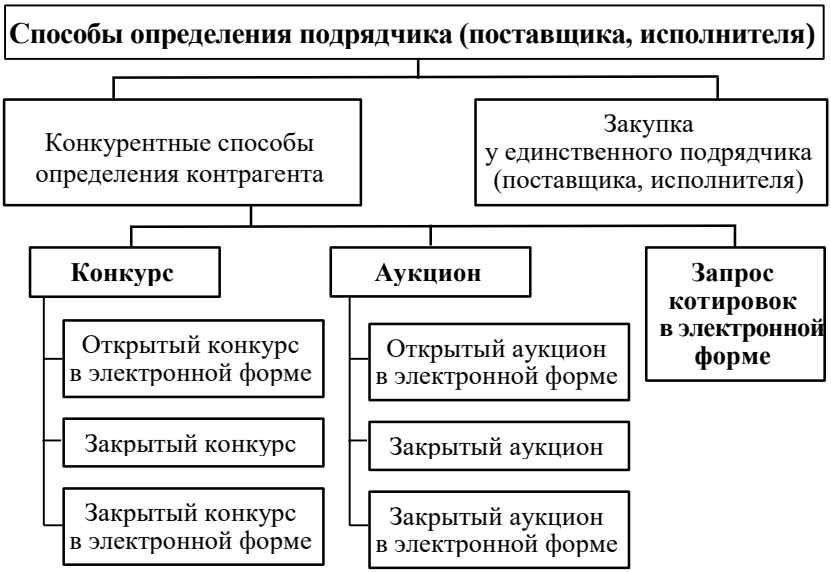

Рис. 2.8. Способы определения подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ

Законодатель дифференцирует конкурентные способы на следующие виды:

1) ***открытые конкурентные способы*** — порядок, при котором информация о закупке сообщается неограниченному кругу лиц;

2) ***закрытые конкурентные способы*** — порядок, при котором информация сообщается ограниченному кругу лиц, способных осуществить выполнение работ, оказание услуг и/или поставку товаров.

Способами определения подрядчика (исполнителя, поставщика) согласно Закону № 44-ФЗ являются конкурс, аукцион и запрос котировок в электронной форме.

Конкурс (согласно общему правилу, уставленному Законом № 44-ФЗ) — это способ определения подрядчика (исполнителя, поставщика), где победителем признается 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 (ЕИС) извещения об осуществлении закупки, после которого участники закупки могут приступить к процедуре подачи заявок.

Открытый конкурс предусматривает ***разбиение заявки на три части***:

1) информация о характеристиках работы, услуги и/или товара;

2) информация о документах, подтверждающих соответствие участника закупки единым и дополнительным требованиям, которые предъявляются ко всем участникам закупки (ст. 31 Закона № 44-ФЗ) (табл. 2.3);

3) информация о цене контракта.

Согласно требованиям 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.

Таблица 2.3

Перечень единых и дополнительных требований,
предъявляемых к участникам закупки
согласно ст. 31 Закона № 44-ФЗ

Наименование 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 участником 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

Продолжение табл. 2.3

Наименование требования	Описание требования
5. Отсутствие у участника закупки судимости за преступления в сфере экономики	Если участник закупки имеет 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
7. Обладание участником закупки исключительными правами на результаты интеллектуальной деятельности	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, которые являются либо выгодоприобретателями, либо близкими родственниками
9. Участник закупки не является офшорной компанией	Под офшорной компанией понимается иностранная компания, правовой статус которой определяется по законодательству места ее регистрации

Окончание таблицы 2.3

Наименование Требования	Описание требования
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, не исполнивших либо исполнивших ненадлежащим образом свои обязательства. Участник закупки, внесенный в реестр недобросовестных подрядчиков (исполнителей, поставщиков), 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, необходимые 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

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 [121].

В силу закрепленных требований ***заказчик обязан указывать используемые критерии и величины их значимости***, причем количество критериев должно быть не менее двух и один из критериев — это 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 рис. 2.9.

Порядок оценки заявок, предельные величины значимости критериев оценки заявок, а также требования к форме документа закреплены в Постановлении № 2604 [121]. Согласно данному постановлению для оценки заявок могут применяться следующие ***критерии оценки***:

- цена контракта;
- сумма цен единиц товара, работы, услуги;
- расходы;
- характеристики объекта закупки;
- квалификация участников закупки, для оценивания которой используются 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;
  - наличие специалистов и иных работников определенного уровня квалификации.

Рис. 2.9. Перечень критериев оценки заявок участников закупки
согласно Закону № 44-ФЗ и Постановлению № 2604

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;
- наличие специалистов и иных работников определенного уровня квалификации.

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. 2.4).

Показатели, связанные с деловой репутацией, могут применяться исключительно для юридических лиц и/или индивидуальных предпринимателей в силу п. 29 Постановления № 2604. В случае применения этого показателя осуществляется оценка индекса деловой репутации в соответствии с национальными стандартами по оценке деловой репутации субъектов предпринимательской деятельности.

Анализ методических рекомендаций Технического комитета по стандартизации «Оценка опыта и деловой репутации предприятий» [122] 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 66.0.01-2017 «Оценка опыта и деловой репутации субъектов предпринимательской деятельности» [123].

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).

Таблица 2.4

Перечень показателей критерия оценки «Квалификация участников закупки» согласно Постановлению № 2604

Показатель	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 производит путем изучения подтверждающих документов (инвентаризационные карточки учета объектов основных средств; договоры аренды (лизинга); выписки из ЕГРН; договоры аренды объектов недвижимого имущества и др.)
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., имеющихся у участника закупки. Эти 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 договоров
4. Наличие деловой репутации	Оценка деловой репутации учитывается как ***индекс деловой репутации участника закупки*** (целое числовое значение в интервале от 0 до 100, присваиваемое субъекту предпринимательской деятельности по результатам работы согласно ГОСТ Р 66.0.01-2017 [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, подтверждающих профессиональную квалификацию специалистов и работников участника закупки

Участники закупки, первые части заявок которых были одобрены комиссией, могут подать предложение о цене контракта в течение одного часа. Если участник закупки не делает предложений по цене, то учитывается 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, поступившие от участников закупки.

В течение одного рабочего дня, рассмотрев ценовые предложения и результаты обеих частей заявок, комиссия присваивает порядковые номера участникам закупки, прошедшим конкурсный отбор. Согласно ст. 48 Закона № 44-ФЗ порядковый номер уменьшается по степени выгодности, т. е. первый номер присваивается участнику закупки, предложившему 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. 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 данного протокола, государственный (муниципальный) заказчик формирует в ЕИС проект контракта без подписи.

Победитель закупки в течение пяти рабочих дней может подписать проект контракта, подготовить протокол разногласий либо отказаться от заключения контракта. Если победитель 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 рис. 2.10.

Рис. 2.10. Проведение открытого конкурса в электронной форме по определению подрядчика (исполнителя, поставщика)

Аукцион — способ определения подрядчика (исполнителя, поставщика), где победителем признается участник закупки, предлагающий наиболее низкую цену контракта. Согласно ст. 24 Закона № 44-ФЗ и распоряжению Правительства РФ от 21.03.2016 № 471-р государственные (муниципальные) заказчики обязаны проводить *аукцион в электронной форме только для определенных работ, услуг и товаров* [124].

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 до наступления даты окончания подачи заявок, подавать свои ценовые предложения, предусматривающие снижение начальной (максимальной) цены (НМЦ) контракта 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 рис. 2.11.

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

Рис. 2.11. Проведение открытого аукциона по определению подрядчика (исполнителя, поставщика) в электронной форме

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. [124].

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 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 [125].

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; жилые помещения для детей-сирот и детей, оставшихся без попечения родителей) запрос котировок может применяться для контрактов независимо от НМЦ.

Процедура запроса котировок имеет упрощенный порядок рассмотрения заявок, что значительно сокращает срок определения подрядчика (исполнителя, поставщика). В частности, согласно ст. 50 Закона № 44-ФЗ оператор электронной площадки не позднее одного часа с момента окончания подачи заявок 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.

Для сделок, в которых закупка работ, услуг и товаров составляет государственную тайну, применяются ***закрытые конкурентные способы*** определения подрядчика (исполнителя, поставщика).

Например, к закупкам работ, услуг и товаров, составляющих государственную тайну, относятся приобретение ценностей Государственного фонда (драгоценных металлов и драгоценных камней РФ, музейных предметов и музейных коллекций), создание, модернизация, поставки, ремонт вооружения, военной и специальной техники и др.

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) осуществляется в случаях, 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.

Отметим основные проблемы, которые возникают при использовании рассмотренных выше способов определения подрядчика (исполнителя, поставщика). В частности, Никитина А.О отмечает, что несмотря на открытость процедуры заключения контрактов, для многих действующих экономических агентов финансовые требования становятся существенным барьером [126]. В качестве примера Никитина А.О. ссылается на случаи, которые возникали во время применения постановления Правительства РФ от10.05.2018 № 564, а именно на случаи взимания оплаты операторами ЕИС за проведение электронных процедур [127].

Евграфов С.А. раскрывает проблему большого количества изменений, которые активно вносятся законодателем в Закон № 44-ФЗ [128]. По итогам проведенного исследования ученый пришел к выводу, что частое обновление норм влечет негативные последствия как для государственных (муниципальных) заказчиков, так и для участников закупок.

Также чрезмерную формализацию сферы государственных закупок в своих трудах отмечает Шмелева М.В. [129]. Ее исследования показывают, что общее количество опубликованных нормативно-правовых актов, касающихся государственных (муниципальных) закупок, уже превысило тысячу наименований.

В качестве примера автор приводит дело № А73-6308/2022, где Прокуратура Хабаровского края потребовала признать заключенные государственные контракты недействительными, поскольку порядок проведения закупки был не соблюден [130].

Отдельно стоит отметить проблему смещения акцентов во время оценивания заявок в сторону экономности бюджетных средств. Науразбаева А.А. отмечает, что в международной практике цена не является единственным критерием при определении подрядчиков, исполнителей и/или поставщиков [131]. 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) [132].

В отечественном законодательстве также имеются указания на установление баланса между экономностью и результативностью. Так, в норме ст. 34 Бюджетного кодекса 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) [133]. Баланс между экономностью и результативностью согласно нормам бюджетного законодательства называется *экономической эффективностью использования бюджетных средств*.

2.4. Риски внешней среды: риски изменения цены на нефть и газ

Материализация риска изменения цен на нефть и газ оказывает значительное влияние на функционирование национальной экономики, отраслей, регионов и конкретных экономических агентов, что позволяет классифицировать этот риск как макро-, мезо- и микориск. Подобное влияние на деятельность экономических агентов может быть объяснено важной ролью топливно-энергетического комплекса (ТЭК) в формировании доходов в отечественной бюджетной системе России (табл. 2.5) [134, 135].

Таблица 2.5

Структура доходов федерального бюджета за 2018–2023 гг.

Вид доходов	Удельный вес доходов в федеральном бюджете за период 2018–2023 гг., %					
	2018	2019	2020	2021	2022	2023
Нефтегазовые	46,4	39,3	28,0	35,8	41,6	30,3
Ненефтегазовые	53,6	60,7	72,0	64,2	58,4	69,7

Из табл. 2.5 следует, что средний объем нефтегазовых доходов в федеральном бюджете составляет порядка 36,9 %. Это обстоятельство указывает на большую зависимость федерального бюджета от изменения цен на нефть и газ, объемов их добычи и экспорта, что влияет на экономическую, энергетическую и национальную безопасность России.

В частности, согласно Энергетической стратегии на период до 2035 г., утвержденной распоряжением Правительства РФ от 09.06.2020 № 1523-р [136], объемы добычи нефти и газа в период до 2024 г. должны составлять соответственно 556–560 млн т и 795,1–820,6 млрд куб. м, а в период до 2035 г. — 490–555 млн т и 859,7–1000,7 млрд куб. м. Фактические показатели добычи нефти и газа показывают, что отечественным институтам удалось достичь запланированных значений и обеспечить стабильность функционирования национальной экономики, отраслей, регионов и экономических агентов (табл. 2.6).

Таблица 2.6

Фактическая добыча нефти и газа в 2018–2023 гг.

Наименование показателя	Объем добычи за период 2018–2023 гг.					
	2018	2019	2020	2021	2022	2023
Добыча нефти, млн т	555,8	560,2	512,7	524,0	534,0	527,0
Добыча газа, млрд куб. м	725,4	738,0	692,3	762,3	672,0	642,0

Особого внимания с учетом рассмотренных выше фактов заслуживают показатели нефтегазовых и ненефтегазовых доходов, представленные в Федеральном законе № 540-ФЗ «О федеральном бюджете на 2024 год и на плановый период 2025 и 2026 годов» [135].

Согласно ст. 1 Закона № 540-ФЗ доходы федерального бюджета в 2024 г. должны составить 35062,5 млрд руб., в которых объем нефтегазовых доходов прогнозируется на уровне 1053,6 млрд руб., т. е. 3 % от общего объема доходов. Совокупный объем доходов на 2025 г. прогнозируется в размере 33552,3 млрд руб., из которых 1835,6 млрд руб. — доходы от реализации нефтегазового сырья и нефтепродуктов (5,4 % от общего объема доходов). В 2026 г. планируется обеспечить федеральный бюджет доходами на уровне 34050,9 млрд руб., в которых 1844,8 млрд руб. — нефтегазовые доходы (5,4 % от общего объема доходов). Подобное уменьшение доли нефтегазовых доходов в федеральном бюджете России может негативно сказаться на устойчивости национальной экономики.

В 2022 г. на процесс достижения запланированных показателей по добыче нефти и газа значительное влияние оказало беспрецедентные рестрикции, приведшие к кардинальным изменениям условий функционирования отечественной экономики. Так, отказ ряда стран от сотрудничества в сырьевой сфере снизил экспорт газа на 30,7 %, до 170,6 млрд куб. м [137]. Однако несмотря внешнее давление, экспорт нефти в 2022 г. достиг 242,0 млн т, увеличившись на 7,6 % по сравнению с 2021 г. [138]. Данный рост обусловлен оперативной переориентацией экспортных поставок нефти в Китай, Индию и Индонезию.

Рестрикции на нефтегазовую сферу были направлены на ухудшение социально-экономического положения России вследствие возникшего дефицита федерального бюджета, увеличения темпов инфляции, падения уровня жизни населения, снижения темпов роста экономики и др. Согласно Доктрине энергетической безопасности [139] и Стратегии национальной безопасности [87] подобное давление квалифицируется как действия, которые направлены на причинение ущерба энергетическим, экономическим и национальным интересам РФ.

Необходимо добавить, что позитивных показателей по уровню добычи и экспорта сырьевых ресурсов во многом удалось добиться за счет усиления сотрудничества между Россией и странами Азиатско-Тихоокеанского региона. В частности, за счет соглашения между ПАО «Роснефть» и китайской компанией «CNPC»

[140], в рамках которого в течение десяти лет (до 31.12.2033) в Китай через Казахстан будет поставлено 100 млн т нефти. Также был заключен еще один важный договор купли-продажи между компанией «CNPC» и ПАО «Газпром», по условиям которого объем поставок газа в Китай с Дальнего Востока должен достигнуть 48 млрд куб. м. в год [141].

Снижение поступлений нефтегазовых доходов в 2023 г. обусловлено снижением цен на нефть и газ, а также усилением недобросовестного поведения со стороны недружественных стран. Например, введение потолка цен на нефтепродукты из России, согласно которому нельзя покупать светлые нефтепродукты (бензин и дизельное топливо), если их цена выше 100 долл. США за баррель, а темные нефтепродукты выше 40 долл. США. Подобные дискриминационные меры привели к значительному сокращению экспорта отечественных нефтепродуктов. Так, например, в январе 2023 г. доходы от экспорта нефти и газа упали на (-)38 % по сравнению с тем же периодом прошлого года. Кроме того, на объем нефтегазовых доходов оказало негативное влияние изменение налогового и таможенного законодательства в части продолжения реализации механизма «налогового маневра».

Анализ табл. 2.7 показывает, что на соотношение нефтегазовых и ненефтегазовых доходов оказывают существенное влияние цены на энергоносители. Ярким примером является рост цен на газ в 2022 г. По сравнению с 2021 г. цена на газ выросла в 3,2 раза, что обеспечило увеличение объемов пошлин, несмотря на падение объема экспорта газа. Однако в 2023 г. цена на газ упала на (-)45,5 %. Исполнение федерального бюджета в 2018–2023 гг. показывает, что размер пошлины для нефти снизился с 1550,0 до 283,9 млрд руб., для нефтепродуктов — с 648,7 до 126,8 млрд руб. (см. табл. 2.7).

Снижение объемов поступлений объясняется реализацией «налогового маневра», т. е. постепенного уменьшения пошлины на нефть и нефтепродукты с 30 % в 2019 г. до 0 % в 2024 г.) [142]. Смысл «налогового маневра» заключается в снижении зависимости российского бюджета от цены на нефть, так как для расчета НДПИ используется цена на нефть и курс доллара США, а пошлина напрямую исчисляется в долларах США.

Таблица 2.7

Фактическое исполнение доходов федерального бюджета в 2018–2023 гг.

В млрд руб.

Наименование	2018 г.	2019 г.	2020 г.	2021 г.	2022 г.	2023 г.
Цена «Юралс», $ за баррель	70,0	63,8	41,4	69,0	77,6	62,9
Цена на газ (Дальнее зарубежье), $ за тыс. куб. м	245,3	204,8	131,6	334,7	954,5	434,6
ДОХОДЫ	**19 454,4**	**20 188,8**	**18 719,1**	**25 286,4**	**27 824,0**	**29 124,0**
НЕФТЕГАЗОВЫЕ ДОХОДЫ	**9 017,8**	**7 924,3**	**5 235,2**	**9 056,5**	**11 586,2**	**8 822,2**
Нефть/нефтепродукты	**7 431,0**	**6 432,4**	**4 174,7**	**7 115,9**	**7 703,9**	**6 577,4**
НДД (налог на дополнительный доход)	0,0	101,1	149,0	1 008,7	1 008,7	1 292,6
НДПИ на нефть (налог на добычу полезных ископаемых)	5 232,3	5 175,5	3 198,3	6 295,7	8 391,5	7 786,5
Акциз на нефтяное сырье	0,0	-424,6	135,0	-1 287,6	-3 248,9	-2 912,4
Пошлины на нефть сырую	1 550,0	1 115,5	436,0	707,8	606,8	283,9
Пошлины на товары, выработанные из нефти	648,7	*464,9*	256,4	391,4	269,5	126,8
Газ	**1 439,9**	**1 322,6**	**921,4**	**1 703,2**	**3 502,2**	**1 785,3**
НДПИ на газ	630,6	627,0	482,2	577,8	1 872,1	1 219,3
Пошлины на газ	809,2	695,7	439,1	1 125,4	1 630,1	566,0
Газовый конденсат	**147,0**	**169,3**	**139,1**	**237,4**	**380,1**	**459,4**
НДПИ на газовый конденсат	147,0	169,3	139,1	237,4	380,1	459,4
НЕНЕФТЕГАЗОВЫЕ ДОХОДЫ	**10 436,6**	**12 264,5**	**13 483,8**	**16 229,9**	**16 237,8**	**20 301,7**

Например, пошлина на нефть в 2022 г. установлена в размере $46,7 за тонну, на светлые нефтепродукты — $14,0 за тонну, на темные нефтепродукты – $46,7 за тонну [143]. Реализуется «налоговый маневр» путем введения поправочных коэффициентов для пошлины от 0,167 в 2019 г. до 1 в 2024 г. и для НДПИ и от 0,833 в 2019 г. до 0 в 2024 г.

Особое внимание необходимо обратить в структуре поступлений доходов федерального бюджета на величину НДД, существенно увеличившуюся по сравнению с 2019–2021 гг. с 101,1 до 1008,7 млрд руб. (см. табл. 2.7). Подобный рост НДД свидетельствует о результативности перехода месторождений на этот режим налогообложения. Под режим НДД подпадают определенные арктические проекты, а также месторождения в Восточной и Западной Сибири, для которых выработанность составляет менее 5 %. Данный налог направлен на замену пошлины и частично НДПИ [144].

Важно отметить, что в 2022 г. цена на нефть превысила $43,3 за баррель, в результате чего сформированы нефтегазовые сверхдоходы в объеме 5077,3 млрд руб., из которых 1127,9 млрд руб. согласно Постановлению Правительства РФ № 699 было направлено на покупку иностранной валюты и золота [145]. Согласно Федеральному закону № 384-ФЗ указанные средства были направлены на увеличение резервного фонда [146]. Согласно данному закону при снижении цены на нефть марки «Юралс» ниже $43,3 за баррель для недопущения дефицита федерального бюджета и покрытия выпадающих нефтяных доходов Минфин России применяет «бюджетное правило», продавая валюту (доллары США, фунты, евро и др.) со счетов резервного Фонда национального благосостояния (ФНБ) Банка России. «Бюджетное правило», сутью которого является направление сверхдоходов от продажи нефти марки «Юралс» в ФНБ, если ее цена превышает $43,3 за баррель, действует в Российской Федерации с 2017 г.

Существенно возросло влияние на структуру нефтегазовых доходов акциза на нефтяное сырье, направленного на переработку (см. табл. 2.7). Величина акциза изменилась с (-)424,6 млрд руб. за 2019 г. до (-)2 912,4 млрд руб. за 2023 г. Увеличение размера «обратного акциза» связано с постепенным переходом от

пошлины на нефть при соизмеримом повышении НДПИ. Так, «обратный акциз» в виде налогового вычета выплачивается нефтеперерабатывающим заводам (НПЗ) в следующих случаях: если их материнские компании находятся под рестрикциями; если данные НПЗ перерабатывают за год более 600 тыс. т нефти; если НПЗ в течение квартала производят бензина и нефти для внутреннего рынка не менее 5 тыс. т.

Уменьшение нефтегазовых доходов обусловлено сокращением добычи, которое вызвано, прежде всего, рестрикциями. В частности, страны G7, ЕС и Австралия 5 декабря 2022 года установили эмбарго на поставки нефти в ЕС и ввели потолок цен на нефть, поставляемую в третьи страны, на уровне $60 за баррель, а 5 февраля 2023 года ввели потолок цен на нефтепродукты, поставляемые в третьи страны [147].

Наряду с геополитическим давлением для нефтяной отрасли актуальны следующие факторы, оказывающие влияние на стоимость нефти:

- ***увеличение себестоимости добычи***. Согласно годовым отчетам ПАО «Роснефть» средняя себестоимость добычи нефти марки «Юралс» составляет $10 за баррель, а со временем будет увеличиваться вследствие перехода на поздние стадии разработки месторождений;
- ***ухудшение физико-химических характеристик добываемой нефти***. Плотность нефти варьируется от 0,65–1,05 г/куб. см. Если плотность нефти ниже 0,830, то ее принято называть легкой, если 0,831–0,860 — средней, если выше 0,860 — тяжелой. Нефть марки «Юралс» является тяжелой, так как ее плотность составляет 0,860–0,871 г/куб. см. Кроме плотности, качество нефти также определяется количеством различных примесей, таких как сера, кислород, металлоорганические соединения, углеводородный газ, вода, механические примеси и др. Чем выше уровень примесей, тем дороже обходится переработка нефти;
- ***незавершенность процесса формирования механизмов налогообложения***. Состояние перехода в условиях «налогового маневра» дестабилизирует ценообразование нефтепродуктов на внутреннем рынке;

- ***снижение объемов добычи и экспорта нефти в результате соглашений ОПЕК и ОПЕК+.*** На членов ОПЕК и ОПЕК+ приходится около 40 % от всемирной добычи нефти. Консолидирование решения стран-участниц ОПЕК[1] и ОПЕК+[2] оказывает значительное влияние на стоимость нефти.

Кроме того, необходимо отметить для газовой отрасли факторы, влияющие на цену газа:

- ***увеличение затрат при добыче и транспортировке газа.*** Рост расходов обусловлен сокращением неглубоко залегающих запасов, поэтому добыча перемещается на месторождения со сложными природно-климатическими и геологическими условиями. В частности, в настоящее время ведутся работы по созданию крупных производств в Арктической зоне на полуострове Ямал и Гыданском полуострове. Рост расходов при транспортировке связан также с ухудшающимися условиями, вызванными уничтожением газовой инфраструктуры, а именно газопроводов «Северный поток» и «Северный поток-2», которые были выведены из строя 26.09.2022 году [148];
- ***отсутствие конкурентного внутреннего рынка газа***. По итогам 2022 г. в России было добыто 672,0 млрд куб. м., из которых 170,6 млрд куб. м. (25,3 % от общего объема) было экспортировано. Однако стоит отметить, что с запуском газопровода «Сила Сибири» реализуется программа газификации ряда субъектов России, расположенных на Дальнем Востоке.

---

[1] ОПЕК — Организация стран-экспортёров нефти (*англ.* The Organization of the Petroleum Exporting Countries — OPEC) — международная межправительственная организация, созданная нефтеэкспортирующими странами в целях контроля квот добычи на нефть. Основана в сентябре 1960 г. По состоянию на октябрь 2024 г. в состав организации входят 12 стран: Алжир, Экваториальная Гвинея, Габон, Иран, Ирак, Кувейт, Ливия, Нигерия, Республика Конго, Саудовская Аравия, ОАЭ и Венесуэла.

[2] ОПЕК+ — расширенный формат ОПЕК, образованный на фоне недовольства многих стран текущей стоимостью нефти в ноябре 2016 г. с целью создания новых возможностей регулирования рынка. На январь 2024 г. в ОПЕК+ входят 11 стран: Азербайджан, Бахрейн, Бруней, Бразилия, Казахстан, Малайзия, Мексика, Оман, Россия, Судан, Южный Судан.

2.5. Особенности риск-менеджмента в системе государственного и муниципального управления за рубежом

Великобритания

В развитии риск-менеджмента в государственном секторе Великобритании одну из важных ролей играет Казначейство. Например, в 1997 г. Казначейством было опубликовано руководство «Зеленая книга: Оценивание и оценка в центральном правительстве», где впервые была закреплена обязанность государственных органов учитывать риски во время анализа государственных проектов, программ и политики [149].

В следующем издании, которое вышло в свет в 2003 г., было отмечено, что риск-ориентированное управление является важным фактором, обеспечивающим успешное достижение запланированных государственных целей за счет рационального использования ресурсов и минимизации материальных потерь [149].

В издании, опубликованном в 2022 году, диапазон использования риск-менеджмента был расширен [150]. В частности, помимо анализа государственных проектов, программ и политики, Казначейством Великобритании был продекларирован учет рисков в процессе рассмотрения предложений, касающихся государственных расходов и налогообложения, законодательных актов, а также решений, связанных с государственными закупками.

Важно отметить, что «Зеленая книга» не описывает методологию управления рисками, поэтому для решения данной проблемы Казначейством Великобритании в 2001 г. было опубликовано отдельное руководство «Управление рисками – стратегический обзор», также известное как «Оранжевая книга» [151]. «Оранжевая книга» закрепила основные процессы управления и методы оценки рисков.

В следующем издании «Оранжевой книги», вышедшем вышло в 2004 г., были уточнены некоторые позиции управления рисками. Например, для визуализации рисков была рекомендована матрица рисков «3х3», если информация неточна или ее

недостаточно, либо матрица рисков «5х5» и более, если информация позволяет осуществлять более точную оценку вероятности наступления рисков и возможного влияния в случаях их материализации.

Кроме того, в оборот было введено понятие «*толерантность к риску*» (уровень риска, который компания готова принять для достижения конкретных целей), означающее установление границ: между опасными рисками, для которых может быть применен «принцип нулевой толерантности», и рисками, которыми можно пренебречь. Использование матриц рисков стало значительным прорывом в оценивании рисков, так как позволило определить наиболее опасные риски для каждого государственного органа и проектов, которые были ими инициированы.

Помимо Казначейства, риск-ориентированный подход активно применяется в деятельности Кабинета министров Великобритании. Так, в 1999 г. Кабинетом министров был опубликован документ «Белая книга модернизации правительства» (далее «Белая книга») [152]. В данном документе закреплялись меры реформирования публичного управления за счет внедрения информационных технологий, результатом использования которых государственные услуги должны были стать доступными «24 часа в сутки», «7 дней в неделю» и «в любом месте».

Например, в гл. 1 сказано, что для государственных служащих складывается ситуация, когда вознаграждение за успех является очень скромным, а наказание за неудачу слишком суровым. В «Белой книге» отмечается, что подобное положение дел сложилось во многом из-за того, что система государственного управления не склонна к риску. По этой причине государственные органы и государственные служащие не спешат внедрять информационные и другие новые технологии в свою деятельность.

В 2002 г. Кабинетом министров Великобритании было опубликовано руководство «Риск: усовершенствование способности правительства справляться с рисками и неопределенностью», закрепляющее основные положения риск-менеджмента [153]. В частности, в документе было сказано, что Кабинет министров несет ответственность за элиминирование следующих рисков:

- прямые атаки и акты агрессии, такие как химические и биологические атаки, кибератаки на критические информационные системы и акты агрессии схожие с событиями, которые произошли 11 сентября 2001 года в США;
- угрозы жизни и здоровью населения из-за вспышек кори, краснухи и др., а также других событий, таящих угрозы для населения (аварии на железнодорожном транспорте, наводнения и др.);
- негативные последствия от изменения климата;
- допущение ошибок государственными органами и государственными служащими;
- использование информационных и новых технологий, в том числе и в государственном секторе;
- репутационные риски.

Согласно руководству по управлению рисками для элиминирования выше представленных рисков Кабинет министров должен выполнять следующие функции:

- ***регулирующую функцию***, назначение которой состоит в обязательном создании легальных механизмов регуляции для элиминирования технологических и общественных угроз, неизбежно возникающих в результате промышленной и коммерческой деятельности, обусловливающих, в свою очередь, множество угроз для жизни и здоровья общества и граждан;
- ***надзорную функцию***, суть которой заключается в непрерывном осуществлении государственными органами и государственными служащими надзора за негативным воздействием окружающей среды, вызванным нехваткой природных ресурсов, изменениями климата, пандемиями, наводнениями и др., с целью оперативного применения чрезвычайных мер;
- ***управляющую функцию***, заключающуюся в проведении государственным сектором непрерывной работы по обеспечению общественного порядка и законности, составляющих залог стабильности общества.

В соответствии с указанным руководством риск-менеджмент представляет собой непрерывный процесс, в котором присутствуют следующие элементы:

- ***коммуникации и обучение***. Чтобы процесс управления рисками осуществлялся непрерывно требуется беспрепятственный обмен информацией о рисках между всеми государственными органами. Причем для повышения результативности и эффективности управления рисками государственным органам необходимо выявлять лучшие практики и через обучение передавать государственным служащим передовой опыт;
- ***идентификация рисков***. Определение рисков является творческой деятельностью и требует большой вовлеченности работников. В связи с этим для повышения качества выявления рисков рекомендуется использовать различные методы (метод Делфи, мозговой штурм и др.). В 2001 г. Отделом стратегии Кабинета министров было проведено крупное исследование, в котором принимали участие около 1800 госслужащих. По итогам исследования было установлено, что значительный вклад в процесс идентификации рисков внесен Министерством обороны, выявляющем риски посредством планирования сценариев;
- ***оценка рисков***. Для оценки рисков используются как количественные, так и качественные методы. Количественные методы оценки вероятности наступления рисков и возможного влияния в случаях их материализации, как правило, используются для рисков, которые относятся к финансовому сектору. Остальные риски оцениваются с помощью экспертов, где результатом их работы является матрица рисков (рис. 2.12 [153]);
- ***элиминирование рисков***. На основе данных, полученных по итогам оценки рисков, разрабатываются планы элиминирования наиболее опасных рисков, выходящих за границу толерантности;

анализ рисков и подготовка отчетности. Данный элемент основан на оценке результативности и эффективности мер элиминирования рисков. Если предпринятые меры не достигли запланированных целей, то процесс управления рисками повторяется снова, пока все опасные риски, вышедшие за границу толерантности, не будут перемещены в безопасные зоны.

Отдельно стоит отметить работу Министерства финансов Великобритании в области управления рисками, в частности, опубликование в 2004 г. документа «Руководство по риск-менеджменту

для министерств и государственных служб» [154]. Данный документ примечателен тем, что в нем продекларированы следующие цели:

- внедрение риск-менеджмента;
- установление ролей и ответственности между государственными служащими;
- разработка методического обеспечения.

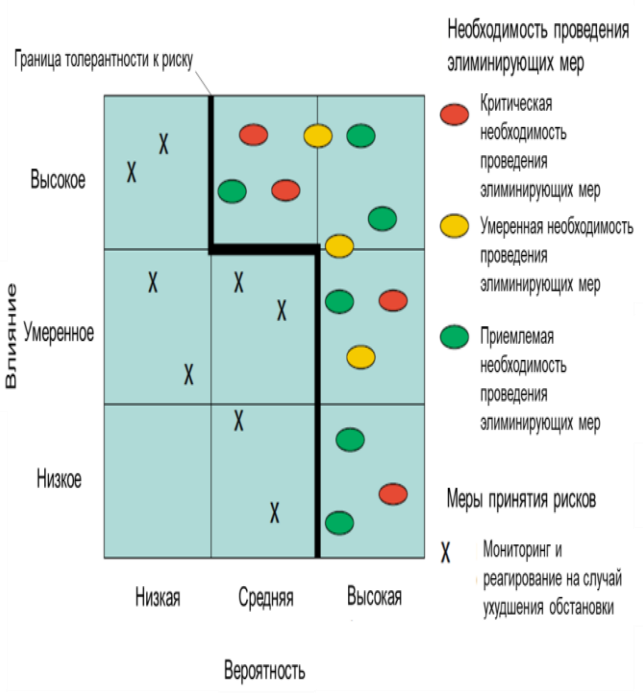

Рис. 2.12. Пример матрицы рисков согласно руководству «Риск: усовершенствование способности правительства справляться с рисками и неопределенностью»

Для достижения названных целей в Министерстве финансов были созданы специальные структурные единицы — ***комитеты по управлению рисками*** (*risk committees*), в функции которых

входили надзор за внедрением риск-менеджмента, оценка и пересмотр стандартов и методологии риск-менеджмента, а также повышение квалификации государственных служащих.

Канада

Внедрение риск-менеджмента в систему государственного управления Канады началось в 1999 г., когда международная аудит-консалтинговая компания KPMG[1] провела масштабные исследования в 18 международных организациях (12 частных и 6 государственных), результаты которых были опубликованы в отчете «Лучшие практики в риск-менеджменте: частный и государственный секторы на международном уровне» (Best Practices in Risk Management: Private and Public Sectors Internationally) по заказу Совета казначейства Канады [150].

Выявленные лучшие практики управления рисками легли в основу методологии управления рисками в государственном секторе, подготовленную Советом казначейства Канады и опубликованную в 2001 г. Методология получила название «Интегрированная система управления рисками» (Integrated Risk Management Framework — IRMF).

С целью распространения разработанной методологии правительство Канады создало специальный Совет по внедрению IRMF, который взял на себя функции по органичному внедрению принципов риск-менеджмента в системе государственного управления. В 2003 г. Совет по внедрению опубликовал документ «Структура управленческой ответственности» (Management Accountability Framework — MAF), в котором была закреплена новая структура управленческой отчетности [150], предусматривающая обязатель-ное описание наиболее опасных рисков и способов их элиминиро-вания.

В 2004 г., Совет по внедрению IRMF опубликовал «Руководство по интегрированному управлению рисками» (Integrated Risk

[1] KPMG — аббревиатура, обозначающая название крупной международной аудит-консалтинговой компании, образованная из первых букв фамилий основателей: Пита Клинфельда (Klynveld), Уильяма Барклая Пита (Peat), Джеймса Марвика (Marwick) и Райнхарда Герделера (Goerdeler).

Management Implementation Guide), в котором подробно представлено описание механизма идентификации и систематизации рисков, их анализ, а также стратегии элиминирования наиболее опасных рисков [150].

Следует отметить, что созданный Советом по внедрению IRMF механизм риск-менеджмента получил большое распространение в системе государственного управления. Например, в 2008 г. правительством Канады было принято решение о создании Центра передового опыта в области управления рисками, а в 2009 г. Комитет по аудиту департаментов и агентств (DAAC) принял решение об обновлении политики внутреннего аудита с учетом международного стандарта управления рисками ISO 31000.

С 27.08.2010 г. в Канаде вступил в силу нормативно-правовой акт «Структура управления рисками» (Framework for the Management of Risk)», который по своей сути является методологическим обеспечением по использованию риск-менеджмента на всех уровнях государственного управления [150]. Данный акт включает следующие документы:

1) «Руководство по интегрированному управлению рисками» (Guide to Integrated Risk Management);

2) «Руководство по корпоративным профилям рисков» (Guide to Corporate Risk Profiles);

3) «Руководство по заявлениям о рисках» (Guide to Risk Statements);

4) «Руководство по таксономии рисков» (Guide to Risk Taxonomies);

5) «Модель возможностей управления рисками» (Risk Management Capability Model).

В частности, согласно «Guide to Corporate Risk Profiles» наиболее опасные риски должны оцениваться с помощью матрицы рисков, представленной на рис. 2.13 [150].

Для ранжирования предлагается использовать шкалы 0÷3 либо 0÷5 в зависимости от требований государственного органа и доступности входящих данных. Для визуализации рисков рекомендуется использовать матрицы рисков «3x3» либо «5x5».

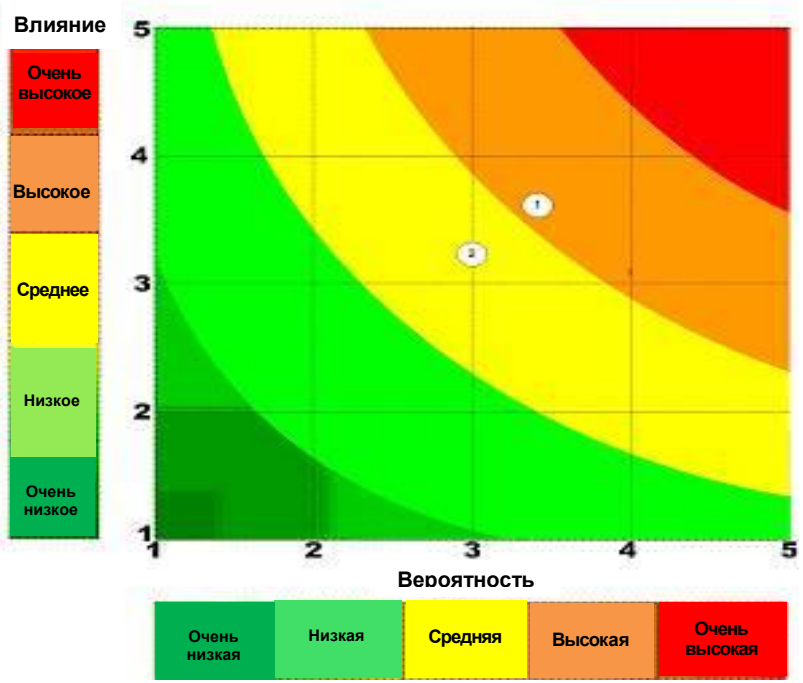

Рис. 2.13. Пример матрицы рисков согласно «Guide to Corporate Risk Profiles»

США

В 2004 г. COSO[1] публикует первую версию стандарта управления рисками «Enterprise Risk Management – Integrated Framework», закрепляющий универсальные принципы управления рисками, которые могли быть использованы как в частных организациях, так и в органах государственной власти [17].

[1] COSO (The Committee of Sponsoring Organizations of the Treadway Commission — Комитет организаций-спонсоров Комиссии Тредвея) — добровольная частная организация в США, целью которой является выработка соответствующих рекомендаций для корпоративного руководства по важнейшим аспектам организационного управления, деловой этики, финансовой отчетности, внутреннего контроля, управления рисками компаний и противодействия мошенничеству.

На основании COSO ERM в 2005 г. Главным бюджетно-контрольным управлением США был опубликован документ, который закрепил систему управления рисками в государственном секторе США. Документ получил название «Структура управления рисками GAO[1] (GAO Risk Management Framework) [155]. Особенностью предложенной системы управления рисками стала фокусировка не на точности оценки рисков, а на реализации полного цикла управления рисками, начиная от стратегического планирования и заканчивания его внедрением и мониторингом. Подобный подход позволяет вводить новую информацию в любой момент времени, что делает систему управления рисками устойчивой за счет оперативной адаптации к условиям среды (рис. 2.14 [155]).

Рис.2.14. Управление рисками согласно «GAO Risk Management Framework»

[1] GAO — Счётная палата США (Government Accountability Office). Это независимое и беспартийное агентство, работающее на Конгресс. GAO осуществляет аудиторскую, оценочную и аналитическую работу.

Система управления рисками согласно «GAO Risk Management Framework» включает следующие фазы:

- ***стратегические цели, задачи и ограничения***. Для данной фазы, кроме определения стратегических целей и задач, необходимых для их достижения, характерно исследование внешней и внутренней сред с целью выявления существующих ограничений и барьеров;
- ***оценку рисков***. Оценивание рисков предполагает идентификацию и анализ рисков, а также определение вероятностей наступлений и возможных влияний в случаях их материализации;
- ***выбор альтернатив***, направленный на определение наиболее результативных и эффективных мер воздействия на риски;
- ***принятие решений*** о выделении ресурсов, которые необходимы для элиминирования рисков;
- ***внедрение и мониторинг***. Проведение элиминирующих мер, а также реализация мониторинга на случай, если предпринятые меры воздействия не достигли запланированных целей.

В 2007 г. в свет вышел документ «Федеральный обзор основных компетенций в области управления рисками» (Federal Risk Management Core Competency Survey), определивший требования профессиональных компетенций к государственным служащим, владение которыми необходимо для успешного внедрения и использования риск-менеджмента в системе государственного управления [150].

Существенное влияние на развитие риск-менеджмента в государственном управлении США оказали террористические акты 11 сентября 2001 г. Так, в 2002 г. правительство США, пересмотрев стратегию национальной безопасности, создало Министерство национальной безопасности США, которое взяло на себя функцию по координации деятельности всех ведомств.

В апреле 2011 г. Министерство национальной безопасности США опубликовало доктрину управления рисками национальной безопасности «Основы управления рисками» (Risk Management Fundamentals) [156], в которой отмечалось, что управление рисками не сможет предотвратить возникновение различных неблагоприятных событий, однако сможет сконцентрировать усилия госу-

дарства и общества на событиях, способных нанести значительный ущерб, и смягчить либо вовсе предотвратить их.

Согласно доктрине риски национальной безопасности разделяются на две большие группы:

1) внутренние риски, влияющие на результативность и эффективность организаций и государственных органов США;

2) внешние риски, к которым относятся изменения геополитической картины, стихийные бедствия, терроризм, вредоносная деятельность в киберпространстве, пандемии, техногенные аварии и др.

Согласно Руководству по управлению рисками при Министерстве обороны США (The Department of Defense (DoD) United States of America. Risk Management Guide for DOD Acquisition) визуализация рисков осуществляется с помощью матрицы 5x5 [59].

Контрольные вопросы для раздела 2

1. Как можно элиминировать риск отказа Заказчика от приемки выполненной работы (оказанной услуги, поставленного товара)?

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 связи с этим 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. Эффективный и результативный риск-менеджмент в системе государственного и муниципального управления 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.

Литература

1. О противодействии противникам Америки посредством санкций: федеральный закон США, принятый 24.07.2017 г. [Электронный ресурс]: Центр Международного права на Чистых прудах. Санкционные законы. США. URL: https://clck.ru/3LoMiR (дата обращения: 02.05.2025).

2. ГОСТ Р ИСО 31000-2019. Менеджмент риска. Принципы и руководство. М.: Стандартинформ, 2020. 14 с. [Электронный ресурс]: электронная версия. URL: https://pqm-online.com/assets/files/lib/std/gost-r-iso-31000-2019.pdf (дата обращения: 02.05.2025).

3. ГОСТ Р 58771-2019. Менеджмент риска. Технологии оценки риска. М.: Стандартинформ, 2020. 86 с. [Электронный ресурс]: электронная версия. URL: https://clck.ru/3NriZZ (дата обращения: 02.05.2025).

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

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

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

7. Курихин С.В. Теория внешней торговли в работе Адама Смита «Исследование о природе и причинах богатства народов» // Вектор экономики, 2019. № 5 (35). 12 с. [Электронный ресурс]: электронный научный журнал. URL: http://www.vectoreconomy.ru/images/publications/2019/5/economictheory/Kurihin.pdf (дата обращения: 02.05.2025).

8. Милль Дж. С. Основы политической экономии: пер. с англ. Т. 2. М.: Прогресс, 1980. 482 с.

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

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

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

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

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

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

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

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

17. Enterprise Risk Management. Integrating with Strategy and Performance. Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2017. 6 p.

18. Harvard Business Review [Электронный ресурс]: Официальный сайт. URL: https://hbr.org/ (дата обращения: 02.05.2025).

19. Финансовая отчетность Apple Inc. по форме 10-K за 2021 год [Электронный ресурс]: электронная версия. URL: https://clck.ru/rgwSv (дата обращения: 02.05.2025).

20. О бухгалтерском учете: Федеральный закон от 06.12.2011 № 402-ФЗ [Электронный ресурс]: электронная версия. URL: https://clck.ru/ 32sZGU (дата обращения: 02.05.2025).

21. О Кодексе корпоративного управления: Письмо Банка России от 10.04.2014 № 06-52/2463 [Электронный ресурс]: электронная версия. URL: https://clck.ru/34bht6 (дата обращения: 02.05.2025).

22. Николаенко В.С. Риск, риск-менеджмент и неопределенность: уточнение понятий // Государственное управление. Электронный вестник, 2020. № 81. С.91–119.

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

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

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

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

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

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

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

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

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

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

33. Королев В.Ю., Бенинг В.Е., Шоргин С.Я. Математические основы теории риска: учеб. пособие для студентов вузов. Изд. 2-е доп. и перераб. М.: Физматлит, 2011. 620 с.

34. Гражданский кодекс Российской Федерации. Комментарии к последним изменениям. М.: АБАК, 2019. 752 с.

35. Даль В.И. Толковый словарь живого великорусского языка. В 4-х т. М.: Цитадель, 1998. 11465 с.

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

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

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

39. США вернули Colonial Pipeline большую часть от уплаченного хакерам выкупа // Лента новостей: Атаки хакеров, сюжет от 08.06.2021 [Электронный ресурс]: РБК. URL: https://clck.ru/VMkiJ (дата обращения: 02.05.2025).

40. Американская страховая компания заплатила хакерам $40 млн. Это крупнейший выкуп из известных // Новости от 21.05.2021 [Электронный ресурс]: журнал для предпринимателей ИНК. URL: https:// clck.ru/ V2hpQ (дата обращения: 02.05.2025).

41. Бельгия заявила о масштабной кибератаке со «шпионскими» целями // Лента новостей: Политика, 26.05.21 [Электронный ресурс]: РБК. URL: https://clck.ru/V5sbS (дата обращения: 02.05.2025).

42. Все заводы JBS по производству говядины в США были вынуждены закрыться из-за кибератаки // Новости от 01.06.2021

[Электронный ресурс]: Bloomberg. URL: https://clck.ru/VFrq5 (дата обращения: 02.05.2025).

43. Злобин А. McDonald's сообщил об утечке данных из-за хакерской атаки // Бизнес. 11.06.2021 [Электронный ресурс]: Forbes. URL: https://clck.ru/VU2P6 (дата обращения: 02.05.2025).

44. В одном из регионов ФРГ впервые ввели режим ЧС из-за кибератаки // Лента новостей: Политика. 10.07.2021 [Электронный ресурс]: РБК. URL: https://clck.ru/W4qKF (дата обращения: 02.05.2025).

45. «Алроса» не сможет заплатить по евробондам $7,75 млн из-за санкций // Новости: Бизнес. 24.06.2022 [Электронный ресурс]: Ведомости. URL: https://clck.ru/rdwnT (дата обращения: 02.05.2025).

46. Вигерс К., Битти Д. Разработка требований к программному обеспечению. 3-е изд., доп. СПб.: Изд-во «БХВ», 2022. 736 с.

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

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

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

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

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

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

53. Майоров В.И. К вопросу о методах идентификации рисков, возникающих в сфере государственного управления // Вестник Нижегородского ун-та им. Н.И. Лобачевсвского. 2018. № 5. С. 135–142 [Электронный ресурс]: КиберЛенинка. URL: https://clck.ru/3Lpek2 (дата обращения: 02.05.2025).

54. ГОСТ Р 51901.21-2012. Менеджмент риска. Реестр риска. Общие положения. М.: Стандартинформ, 2020. 16 с. [Электронный ресурс]: электронная версия. URL: https://clck.ru/3Lpf9V (дата обращения: 02.05.2025).

55. Lewis S., Smith K. Lessons Learned from Real World Application of the Bowtie Method // 6th Global Congress on Process Safety, 2010. P. 1–20.

56. Wijayanti D., Sukwika T., Ramli S. Analysis Inside Fatality Akibat Covid-19 Menggunakan Metode 5 Why, SCAT, BowTie, dan ISM // JurnalMigasian, 2022. No 6(1). P. 84–92.

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

58. ГОСТ Р 56715.3-2015. Проектный менеджмент. Системы проектного менеджмента. Ч. 3. Методы. М.: Стандартинформ, 2020. 8 с. [Электронный ресурс]: Интернет и право. Актуальное законодательство. URL: https://internet-law.ru/gosts/gost/61129/ (дата обращения: 02.05.2025).

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

60. Кодекс Российской Федерации об административных правонарушениях (КоАП РФ): Федеральный закон от 30.12.2001 № 195-ФЗ (ред. от 03.02.2025) (с изм. и доп., вступ. в силу с 01.03.2025). М.: Проспект, 2019. 688 с. Доступ из справ.-прав. системы «КонсультантПлюс».

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

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

63. The CHAOS Manifesto. The Standish Group, 2014. 16 p.

64. 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; под ред. Шаминой Л.К. М.: Финансовый университет при Правительстве Российской Федерации, 2016. С. 12–16.

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

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

67. Решение Арбитражного суда Ямало-Ненецкого автономного округа по делу № А81-9472/2019 от 02.01.2020 г. [Электронный ресурс]: электронная версия. URL: https://clck.ru/kScgp (дата обращения: 02.05.2025).

68. Решение Арбитражного суда Томской области от 16.05.2017 по делу № А67-1623/2017 [Электронный ресурс]: электронная версия. URL: https://clck.ru/jec2f (дата обращения: 02.05.2025).

69. Решение Арбитражного суда города Москвы по делу № А40-248300/21-5-1672 от 09.02.2022 [Электронный ресурс]: электронная версия. URL: https://clck.ru/kRTqS (дата обращения: 02.05.2025).

70. Решение Арбитражного суда города Москвы по делу № А40-32033/19-47-287 от 02.10.2020 [Электронный ресурс]: электронная версия. URL: https://clck.ru/kTCuY (дата обращения: 02.05.2025).

71. Решение Арбитражного суда города Москвы по делу № А40-81328/2011 от 07.04.2014 [Электронный ресурс]: электронная версия. URL: https://clck.ru/nTfSN (дата обращения: 02.05.2025).

72. Решение Арбитражного суда Самарской области по делу № А55-9384/2018 от 26.09.2018 [Электронный ресурс]: электронная версия. URL: https://clck.ru/jeqZv (дата обращения: 02.05.2025).

73. Комментарий к Уголовному кодексу Российской Федерации. 8-е изд., перераб. и доп. М.: Проспект, 2019. 800 с.

74. Решение Приморского районного суда города Санкт-Петербурга по делу № 2-38/2019 (2-4158/2018;) ~ М-608/2018 от 11.06.2019 [Электронный ресурс]: электронная версия. URL: https://clck.ru/SiN5M (дата обращения: 02.05.2025 г.).

75. Решение Арбитражного суда города Москвы по делу № А40-202764/18-110-1552 от 01.02.2019 [Электронный ресурс]: электронная версия. URL: https://clck.ru/jfczi (дата обращения: 02.05.2025 г.).

76. Решение Арбитражного суда Свердловской области по делу № А60-27815/2012 от 01.10.2012. [Электронный ресурс]: электронная версия. URL: https://clck.ru/jfedG (дата обращения: 02.05.2025 г.).

77. Решение Арбитражного суда города Москвы по делу № А40-117808/10-12-740 от 30.11.2010 [Электронный ресурс]: электронная версия. URL: https://clck.ru/SiNiS (дата обращения: 02.05.2025 г.).

78. О коммерческой тайне [Электронный ресурс]: Федеральный закон от 29.07.2004 № 98-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

79. Об организации страхового дела в Российской Федерации [Электронный ресурс]: Федеральный закон № 4015-1 от 27.11.1992. Доступ из справ.-правовой системы «КонсультатнПлюс.

80. Швеция отказалась передать России итоги расследования взрывов Nord Stream // Новости: Подрыв «Северных потоков». 10.10. 2022 [Электронный ресурс]: РБК. URL: https://clck.ru/ 355Tk4 (дата обращения: 02.05.2025.

81. Путин назвал спецслужбы Украины исполнителями теракта на Крымском мосту // Новости: Взрыв на Крымском мосту. 09.10.2022 [Электронный ресурс]: РБК. URL: https://clck.ru/ 355xG6 (дата обращения: 02.05.2025).

82. ЕС ввел потолок цен на российскую нефть: что будет с акциями и рублем // Новости: Что это значит. 05.12.2022 [Электронный ресурс]: РБК: URL: https://clck.ru/355Tcc (дата обращения: 02.05.2025).

83. Bloomberg узнал об обсуждении почти полного запрета на экспорт в Россию // Новости: Война санкций. 20.04.2023 [Электронный ресурс]: РБК- URL: https://clck.ru/355xTc (дата обращения: 02.05.2025).

84. Британия запретит импорт российских алмазов и никеля Россию // Новости: Война санкций. 19.05.2023 [Электронный ресурс]: РБК. URL: https://clck.ru/355xPM (дата обращения: 02.05.2025).

85. Акции золотодобытчиков упали после их включения в SDN-лист США // Новости. 19.05.2023 [Электронный ресурс]: РБК. URL: https:// clck.ru/355xKc (дата обращения: 02.05.2025).

86. Эксперты оценили случаи изъятия автомобилей россиян в Германии // Новости: Война санкций. 02.07.2023 [Электронный ресурс]: РБК. URL: https://clck.ru/355Thd (дата обращения: 02.05.2025).

87. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 [Электронный ресурс]: электронная версия. URL: https://clck.ru/3Lq6FP (дата обращения: 02.05.2025).

88. О стратегическом планировании в Российской Федерации [Электронный ресурс]: Федеральный закон от 28.06.2014 № 172-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

89. О безопасности [Электронный ресурс]: Федеральный закон от 28.12.2010 № 390-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

90. О Стратегии экономической безопасности Российской Федерации на период до 2030 года [Электронный ресурс]: Указ Президента РФ от 13.05.2017 № 208. Доступ из справ.-правовой системы «КонсультантПлюс».

91. Военная доктрина Российской Федерации [Электронный ресурс]: утверждена Президентом РФ 25.12.2014 № Пр-2976. Доступ из справ.-правовой системы «КонсультантПлюс».

92. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). [Электронный ресурс]. Доступ из справ.-прав. системы «КонсультантПлюс».

93. Концепция общественной безопасности в Российской Федерации»: утв. Президентом РФ 14.11.2013 № Пр-2685 [Электронный ресурс]: электронная версия. URL: https://clck.ru/3Lq7Ck (дата обращения: 02.05.2025).

94. Об утверждении Доктрины информационной безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 05.12.2016 № 646. Доступ из справ.-правовой системы «КонсультантПлюс».

95. О Стратегии научно-технологического развития Российской Федерации [Электронный ресурс]: Указ Президента РФ от 01.12.2016 № 642. Доступ из справ.-правовой системы «КонсультантПлюс».

96. О Стратегии экологической безопасности Российской Федерации на период до 2025 года [Электронный ресурс]: Указ Президента РФ от 19.04.2017 № 176. Доступ из справ.-правовой системы «КонсультантПлюс».

97. Устав Организации Объединенных Наций. Раздел I. Понятие международного права, его сущность и роль в международных отношениях, политике и дипломатии [Электронный ресурс]: принят в г. Сан-Франциско 26.06.1945 (с изм. и доп. от 20.12.1971). Доступ из справ.-правовой системы «КонсультантПлюс».

98. Countering America’s Adversaries Through Sanctions Act [Electronic resource]: CONGRESS. GOV. URL: https://clck.ru/qjFCv (accessed: 02.05.2025).

99. Военная доктрина Союзного государства [Электронный ресурс]: Постановление Высшего Государственного Совета Союзного

государства от 4.11.2021 № 5. URL: https://clck.ru/35BSss (дата обращения: 02.05.2025).

100. МИД заявил о моделировании НАТО кибератак по энергосистеме Москвы // Новости: Политика. 28.01.2023 [Электронный ресурс]: РБК. URL: https://clck.ru/35BUYr (дата обращения: 02.05.2025).

101. Власти сообщили о хакерском взломе радиостанций в нескольких регионах Новости: Военная операция на Украине. 12.06.2023 [Электронный ресурс]: РБК. URL: https://clck.ru/ 35BUmb (дата обращения: 02.05.2025).

102. РЖД сообщили о массированной хакерской атаке на свой сайт и приложение // Новости: Бизнес. 05.07.2023 [Электронный ресурс]: РБКURL: https://clck.ru/35BUdd (дата обращения: 02.05.2025 г.).

103. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс]: Федеральный закон от 26.07.2017 № 187-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

104. Послание Президента Российской Федерации Федеральному Собранию Российской Федерации [Электронный ресурс]: Послание Президента РФ Федеральному Собранию от 04.12.2014. Доступ из справ.-правовой системы «КонсультантПлюс».

105. О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля. [Электронный ресурс]: Федеральный закон от 26.12.2008 № 294-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

106. О применении риск-ориентированного подхода при организации отдельных видов государственного контроля (надзора) и внесении изменений в некоторые акты Правительства Российской Федерации [Электронный ресурс]: Постановление Правительства РФ от 17 августа 2016 г. № 806. Доступ из справ.-правовой системы «КонсультантПлюс».

107. Реформа контрольной и надзорной деятельности: паспорт приоритетной программы [Электронный ресурс]: приложение к протоколу президиума Совета при Президенте РФ по стратегическому развитию и приоритетным проектам от 21.12.2016 № 12 (ред. от 30.05.2017). Доступ из справ.-правовой системы «КонсультантПлюс».

108. О государственном контроле (надзоре) и муниципальном контроле в Российской Федерации [Электронный ресурс]: Федеральный закон от 31.07.2020 № 248-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

109. Риск-ориентированный подход: приоритет реформы госконтроля [Электронный ресурс]: Гарант.ру, 18.08.2020. URL: https://www. garant.ru/article/1406579/ (дата обращения: 02.05.2025).

110. 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» [Электронный ресурс]: электронная версия. URL: https://clck.ru/3LqAq5 (дата обращения: 02.05.2025).

111. Высокая доля расторжения контрактов в рамках закона о контрактной системе: аналитический доклад, май 2021 г. 40 с. [Электронный ресурс]: Аналитический центр при Правительстве Российской Федерации. URL: https://clck.ru/gfMiA (дата обращения: 02.05.2025).

112. Об утверждении классификатора программ для электронных вычислительных машин и баз данных [Электронный ресурс]: Приказ Минкомсвязи России от 22.09.2020 № 486 (в ред. от 04.12.23). Доступ из справ.-правовой системы «КонсультантПлюс».

113. Решение Арбитражного суда города Москвы по делу № А40-263677/21-51-1834 от 27.07.2022 [Электронный ресурс]: электронная версия. URL: https://clck.ru/32Rowo (дата обращения: 02.05.2025).

114. Решение Арбитражного суда Алтайского края по делу № А03-5595/2021 от 04.08.2022 [Электронный ресурс]: электронная версия. URL: https://clck.ru/32RsSP (дата обращения: 02.05.2025).

115. Решение Арбитражного суда Санкт-Петербурга и Ленинградской области по делу № А56-107933/2019 от 31.03.2021 [Электронный ресурс]: электронная версия. URL: https://clck.ru/ 32S4yT (дата обращения: 02.05.2025).

116. Об утверждении типовых условий контрактов на выполнение работ по созданию и (или) развитию (модернизации) государственных (муниципальных) и(или) иных информационных систем [Электронный ресурс]: Приказ Минцифры России от 17.12.2020 № 715. Доступ из справ.-правовой системы «КонсультантПлюс».

117. Решение Арбитражного суда Алтайского края по делу № А03-14616/2020 от 21.10.2021 [Электронный ресурс]: электронная версия. URL: https://clck.ru/32RtCX (дата обращения: 02.05.2025).

118. Отчет Департамента госзаказа Томской области за 2022 г. [Электронный ресурс]: Департамент государственного заказа Томской области. URL: https://dgz.tomsk.gov.ru/ (дата обращения: 02.05.2025 г.).

119. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд [Электронный ресурс]: Федеральный закон «» от 05.04.2013 № 44-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

120. Федеральный закон «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 № 223-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

121. Об оценке заявок на участие в закупке товаров, работ, услуг для обеспечения государственных и муниципальных нужд, внесении изменений в пункт 4 постановления Правительства Российской Федерации от 20 декабря 2021 г. № 2369 и признании утратившими силу некоторых актов и отдельных положений некоторых актов Правительства Российской Федерации [Электронный ресурс]: Постановление Правительства РФ от 31.12.2021 № 2604 (ред. от 23.09.2024). Доступ из справ.-правовой системы «КонсультантПлюс».

122. Оценка опыта и деловой репутации предприятий [Электронный ресурс]: Официальный сайт Технического комитета по стандартизации. URL: https://tk066.ru/ (дата обращения: 02.05.2025).

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. О перечне товаров, работ, услуг, в случае осуществления закупок которых заказчик обязан проводить аукцион в электронной форме (электронный аукцион) [Электронный ресурс]: Распоряжение

Правительства РФ от 21.03.2016 № 471-р. Доступ из справ.-правовой системы «КонсультантПлюс».

125. «О внесении изменений в Федеральный закон «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» [Электронный ресурс]: Федеральный закон от 28.04.2023 № 154-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

126. 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.

127. О взимании операторами электронных площадок, операторами специализированных электронных площадок платы при проведении электронной процедуры, закрытой электронной процедуры и установлении ее предельных размеров [Электронный ресурс]: Постановление Правительства РФ от 10.05.2018 № 564. Доступ из справ.-правовой системы «КонсультантПлюс».

128. 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.

129. Шмелева М.В. Проблемы понятийного наполнения сферы государственных закупок и пути их решения // Журнал предпринимательского и корпоративного права, 2020. № 1. С. 12–15.

130. Решение Арбитражного суда Хабаровского края по делу № А73-6308/2022 от 28.06.2022 [Электронный ресурс]: электронная версия. URL: https://clck.ru/32RZZe (дата обращения: 02.05.2025).

131. 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.

132. О государственных закупках и об отмене Директивы 2004/18/ЕС [Электронный ресурс]: Директива № 2014/24/ЕС Европейского парламента и Совета Европейского Союза. URL: https://clck.ru/32U2Mf (дата обращения: 02.05.2025).

133. Бюджетный кодекс Российской Федерации [Электронный ресурс]: Федеральный закон от 31.07.1998 № 145-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

134. Об утверждении государственной программы Российской Федерации «Развитие энергетики» [Электронный ресурс]: Постановление Правительства РФ от 15.04.2014 № 321. URL: https://clck.ru/34k88Y (дата обращения: 02.05.2025).

135. О федеральном бюджете на 2024 год и на плановый период 2025 и 2026 гг. [Электронный ресурс]: Федеральный закон от 27.11.2023 № 540-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

136. Об утверждении Энергетической стратегии Российской Федерации на период до 2035 года [Электронный ресурс]: Распоряжение Правительства РФ от 09.06.2020 № 1523-р. Доступ из справ.-правовой системы «КонсультантПлюс».

137. Новости Минэнерго [Электронный ресурс]: Информационное телеграфное агентство России «ИТАР-ТАСС». URL: https://tass.ru/eko nomika/17270415 (дата обращения: 02.05.2025).

138. Лента новостей: Экспорт российской нефти … [Электронный ресурс]: Новости РИА. URL: https://clck.ru/34jn4g (дата обращения: 02.05.2025).

139. Об утверждении Доктрины энергетической безопасности Российской Федерации [Электронный ресурс]: Указ Президента РФ от 13.05.2019 № 216. Доступ из справ.-правовой системы «КонсультантПлюс».

140. О соглашении между «Роснефть» и китайской компанией «CNPC» Роснефть подписала соглашение о поставке 100 млн т нефти в Китай [Электронный ресурс]: РБК. URL: https://clck.ru/34jnU8 (дата обращения: 02.05.2025).

141. О договоре между Газпромом и Китаем [Электронный ресурс]: РБК. URL: https://clck.ru/34jncG (дата обращения: 02.05.2025).

142. О внесении изменения в статью 35 Закона Российской Федерации «О таможенном тарифе» [Электронный ресурс]: Федеральный закон от 18.02.2020 № 24-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

143. Таможенно-тарифное регулирование [Электронный ресурс]: Министерство экономического развития Российской Федерации. URL: https://clck.ru/34joqx (дата обращения: 02.05.2025).

144. Об одобрении Кабинетом Министров законопроекта по расширению НДД [Электронный ресурс]: ИТАР-ТАСС. URL: https://tass.ru/ekonomika/1363 7745 (дата обращения: 02.05.2025).

145. О проведении расчетов и перечислении средств в связи с формированием и использованием дополнительных нефтегазовых доходов федерального бюджета, средств Фонда национального благосостояния, а также о признании утратившими силу отдельных актов Правительства РФ [Электронный ресурс]: Постановление Правительства РФ от 14.08.2013 № 699. Доступ из справ.-правовой системы «КонсультантПлюс».

146. О внесении изменений в Бюджетный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации и установлении особенностей исполнения бюджетов бюджетной системы Российской Федерации в 2022 году [Электронный ресурс]: Федеральный закон «» от 29.11.2021 № 384-ФЗ. Доступ из справ.-правовой системы «КонсультантПлюс».

147. Потолок со смешанными прорехами [Электронный ресурс]: информационное телеграфное агентство России «ИТАР-ТАСС». URL: https://clck.ru/34jxez (дата обращения: 02.05.2025).

148. В обеих нитках «Северного потока-1» упало давление [Электронный ресурс]: Информационное телеграфное агентство России «ИТАР-ТАСС». URL: https://clck.ru/34k6cv (дата обращения: 02.05.2025).

149. The Green Book: Appraisal and Evaluation in Central Government. Her Majesty's Treasury. 2003 [Electronic resource]: Cookies on GOV.UK. URL: https://clck.ru/3Lrk4Q (accessed: 02.05.2025).

150. Кулик Г.Ю. Зарубежный опыт внедрения риск-менеджмента в государственное управление // Государственное управление. Электронный вестник, 2013. № 37. С. 32-44.

151. The Orange Book: Management of Risk – Principles and Concepts. Her Majesty's Treasury, 2004. 50 p. [Electronic resource]: electronic version. URL: https://clck.ru/3Lrk77 (accessed: 02.05.2025).

152. Supporting innovation: Managing risk in Government departments / Report by the Comptroller and Auditor General, National Audit Office, 2000 [Electronic resource]: electronic version. URL: https://www.nao.org.uk/wp-content/uploads/2000/08/9900864es.pdf (accessed: 02.05.2025).

153. Risk: Improving Governments Capability to Handle Risk and Uncertainty / Summary Report of Cabinet Office. 2002 [Electronic resource]: electronic version. URL: https://clck.ru/3Lrkym (accessed: 02.05.2025).

154. Risk Management Guidance for Government Departments and Offices. Department of Finance, 2004 [Electronic resource]: electronic version. URL: https://clck.ru/3LrnPR (accessed: 02.05.2025).

155. Hardy K. Managing Risk in Government: An Introduction to Enterprise Risk Management. IBM Center for The Business of Government, 2010 [Electronic resource]: electronic version. URL: https://clck.ru/3LrpkT (accessed: 02.05.2025).

156. Risk Management Fundamentals: Homeland Security Risk Management Doctrine. U. S. Department of Homeland Security. 2011 [Electronic resource]: electronic version. URL: https://clck.ru/3LrqVZ (accessed: 02.05.2025).

Глоссарий

Аукцион — способ определения подрядчика (исполнителя, поставщика), в котором победителем признается участник закупки, предложивший наиболее низкую цену контракта.

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

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

Дефляционные риски — вероятность усиления реальной покупательной способности денег.

Диверсификация рисков — перераспределение капитала между несколькими, несвязанными между собой инвестиционными инструментами: акциями, облигациями, валютой, недвижимостью, криптовалютой и др.

Запрос котировок в электронной форме — способ определения подрядчика (исполнителя, поставщика), в котором победителем признается участник закупки, предлагающий наиболее низкую цену контракта.

Индикаторы риска — отклонения объекта контроля (надзора) от параметров, которые могут привести к материализации риска.

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.

Ковенант — обязательство совершить какое-либо действие или воздержаться от его совершения.

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

Коллаборация — сотрудничество, целью которого является достижение общей цели в рамках одной организации (проекта, группы

компаний и др.), посредством объединения знаний, опыта и ресурсов для решения сложных задач и достижения лучших результатов.

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), в котором победителем признается участник закупки, предложивший лучшие условия контракта.

Комплаенс-риск — вероятное событие, наступающее в связи с несоответствием нормативным актам, стандартам и кодексам поведения. Последствия материализации подобных рисков проявляются в форме юридических санкций со стороны регулирующих и надзорных органов, отраслевых ассоциаций и лиц, права и интересы которых были нарушены.

Макориски — глобальные риски, последствия от материализации которых отражаются на всех экономических агентах.

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

Микориски (предпринимательские риски) — вероятные события, наступление которых оказывает влияние на экономическую деятельность конкретных экономических агентов.

Митигация — (mitigation — «смягчение» или «смягчение последствий»). В управлении рисками митигация означает усилия, направленные не только на уменьшения тяжести последствий реализации риска, но также и на снижение вероятности реализации рискового события.

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

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

Нестрахуемый риск — риск, в отношении которого не может быть заключен договор страхования.

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

Опцион — *(optio* — выбор, желание, усмотрение) — договор, по которому потенциальный покупатель (колл-опцион) или потенциальный продавец (пут-опцион) базового актива (товара, ценной бумаги) получает ***право, но не обязательство***, совершить покупку или продажу данного актива по заранее оговорённой цене или по нефиксированной цене, но вычисляемой по заранее оговорённой формуле, в определённый договором момент в будущем или на протяжении определённого отрезка времени при условии наступления оговорённого события.

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

Риск-аппетит — возможный материальный ущерб, который субъект готов принять для достижения завершения проекта.

Риски ликвидности — вероятность неисполнения денежных обязательств в установленном объеме и 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.

Своп — вид контракта (торгово-финансовая операция обмена разнообразными активами), который заключают участники торгов, обязуясь вернут активы через определенное время и на определенных условиях. Наиболее часто своп используют для хеджирования рисков и более выгодного выхода на новые рынки.

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.

Страхуемый риск — риск, в отношении которого может быть заключен договор страхования.

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.

Толерантность к риску — возможный материальный ущерб, который субъект способен принять не обанкротившись.

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, актуальные 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 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).

Форвардный контракт — соглашение между двумя сторонами на покупку или продажу актива по определенной цене в будущем (разовая внебиржевая сделка между продавцом и покупателем). Контракт может быть привязан к конкретному товару, сумме или дате поставки и использоваться для хеджирования или страховки от негативных последствий падения цены на базовый актив. Оплата производится при его заключении, а поставка при завершении срока действия.

Фьючерсный контракт — стандартизированный контракт (повторяющееся предложение при торгах на бирже), по условиям которого продавец обязуется поставить покупателю некий товар или финансовый инструмент (базовый актив) в определенный срок и по фиксированной цене, оговоренной в момент заключения сделки.

Хеджирование рисков — перенос рисковых событий на субъектов, готовых их принять.

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

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

Элиминирование рисков (лат. *eliminare* — изгонять, устранять, ликвидировать) — изменение вероятности наступления рисков и (или) влияния в случаях их материализации.

Приложение А

РИСКИ ВНЕШНЕЙ СРЕДЫ: 2025 ГОД

ЭКОНОМИЧЕСКИЕ РИСКИ

- Риск изменения цен на нефть
- Риск изменения цен на газ
- Риск изменения цен на металл
- Риск изменения цен на уголь
- Риск изменения цен на зерно
- Риск изменения цен на уран
- Риск дефицита (профицита) федерального бюджета
- Риск изменения курса валют
- Риск внесения изменений в закон «О федеральном бюджете»
- Риск изменения налоговой политики
- Риск изменения размера государственного долга
- Риск изменения денежно-кредитной политики
- Риск эмиссии денежной массы
- Риск изменения ключевой ставки
- Риск изменения процентов кредитных и депозитных ставок
- Риск изменения темпов инфляции
- Риск изменения темпов роста экономики
- Риск изменения уровня жизни населения
- Риск изменения фондовых индексов
- Риск запрета торговли ценными бумагами определенных организаций
- Риск дефолта
- Риск экономического кризиса

Обозначения видов рисков:

— наступивший риск; — новый риск;

— оценка риска не изменилась по сравнению с прошлым годом;

— оценка риска выросла по сравнению с прошлым годом;

— оценка риска снизилась по сравнению с прошлым годом.

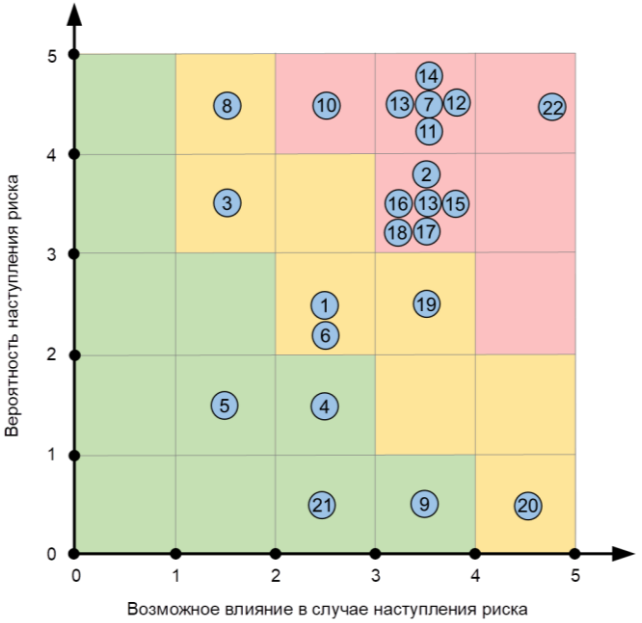

Рис. А1. Матрица экономических рисков

ОБЩЕСТВЕННЫЕ РИСКИ

23. Риск изменения уровня смертности
24. Риск изменения уровня рождаемости
25. Риск отсутствия на рынке труда квалифицированных кадров
26. Риск социальной напряженности
27. Риск изменения уровня образования
28. Риск изменения уровня медицины
29. Риск изменения уровня преступности
30. Риск изменения уровня миграции
31. Риск голода
32. Риск изменения численности населения
33. Риск изменения духовно-нравственной (культурной) сферы

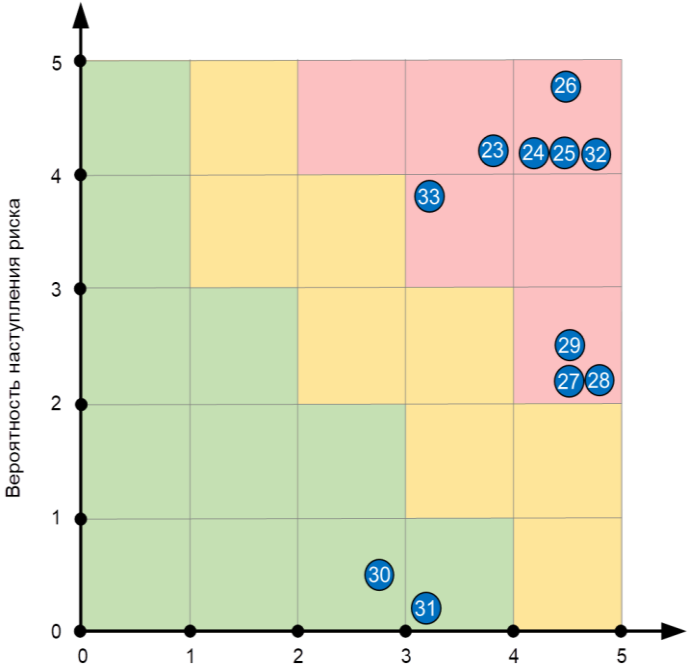

Рис. А2. Матрица общественных рисков

ПОЛИТИЧЕСКИЕ РИСКИ

34. Риск изменения геополитического положения
35. Риск расширения альянса НАТО
36. Риск военного конфликта
37. Риск введения военного положения
38. Риск террористического акта
39. Риск изменения норм действующего законодательства
40. Риск интеграции РФ с внешними субъектами
41. Риск государственного переворота
42. Риск национализации и экспроприации имущества
43. Риск редомиляции
44. Риск массовых беспорядков
45. Риск гражданской войны
46. Риск импичмента президента

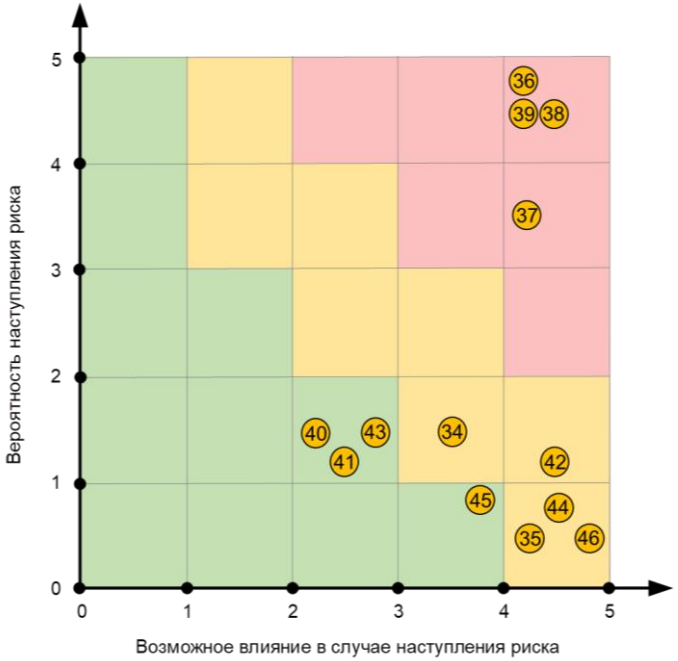

Рис. А3. Матрица политических рисков

ЭКОЛОГИЧЕСКИЕ РИСКИ

- 47. Риск нехватки природных ресурсов
- 48. Риск изменения климата
- 49. Риск загрязнения окружающей среды
- 50. Риск пандемии
- 51. Риск наводнения
- 52. Риск радиоактивного заражения
- 53. Риск тайфуна
- 54. Риск землетрясения
- 55. Риск падения космического тела
- 56. Риск извержения вулкана
- 57. Риск пожара
- 58. Риск уничтожения Земли
- 59. Риск таяния ледников

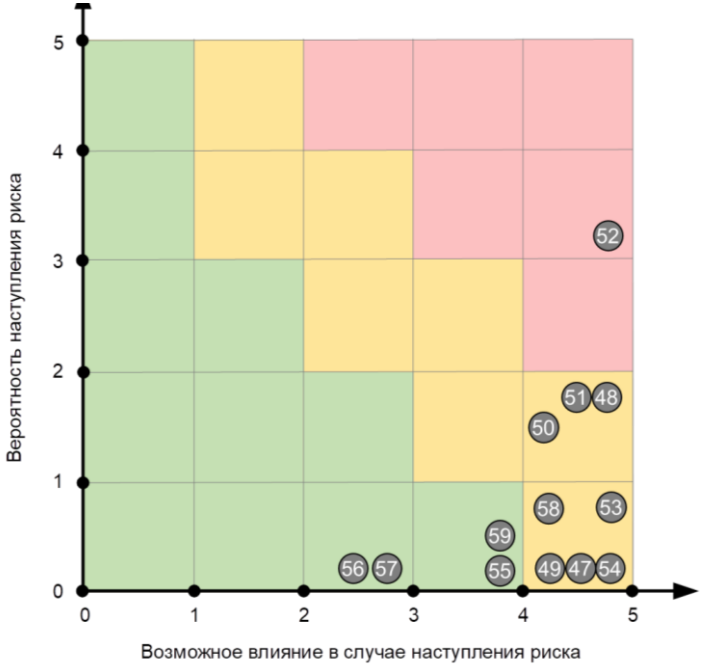

Рис. А4. Матрица экологических рисков

ТЕХНОЛОГИЧЕСКИЕ РИСКИ

- 60. Риск атаки искусственного интеллекта (ИИ)
- 61. Риск отключения Интернета
- 62. Риск кибератак на критическую информационную инфраструктуру (КИИ)
- 63. Риск атаки на критическую инфраструктуру
- 64. Риск использования новых технологий
- 65. Риск поломки оборудования
- 66. Риск нехватки электроэнергии

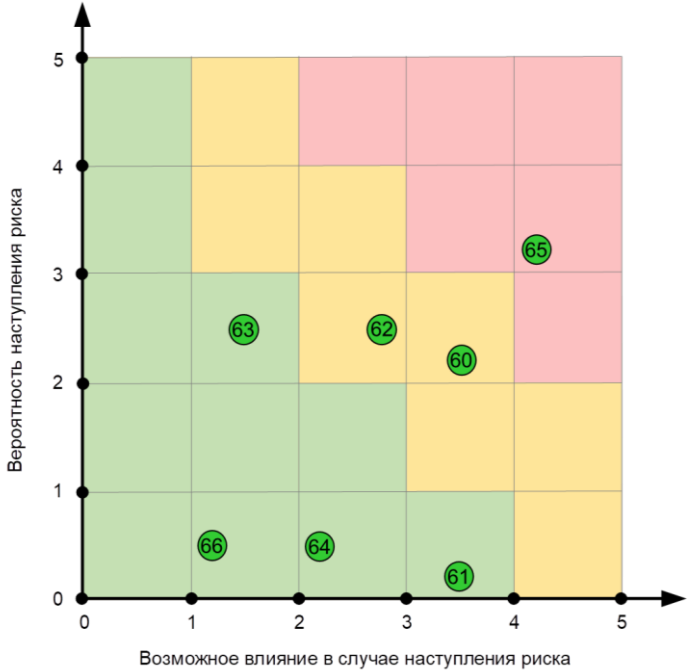

Рис. А5. Матрица технологических рисков

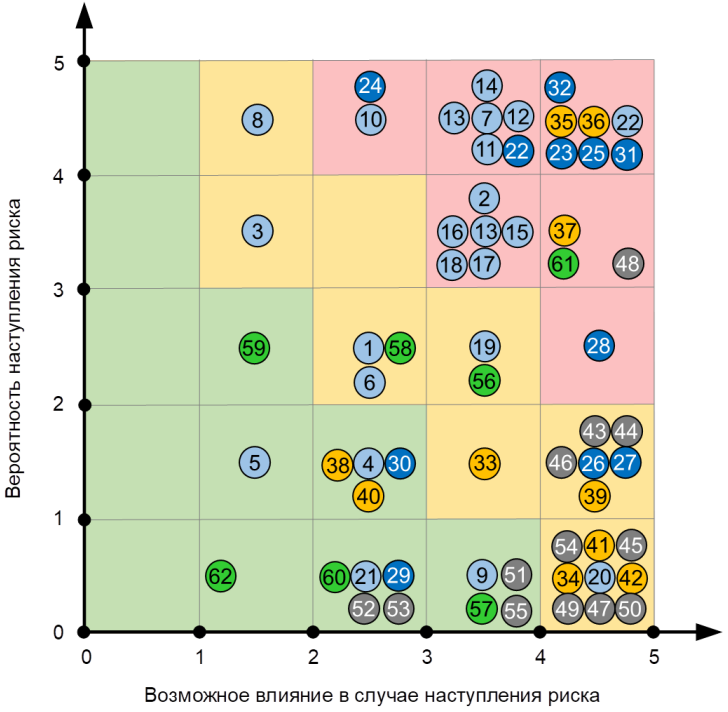

Рис. А6. Матрица рисков внешней среды

Приложение Б

РЕЕСТР УНИВЕРСАЛЬНЫХ РИСКОВ

ID риска	Название риска
1. КОММЕРЧЕСКИЕ РИСКИ (ПРЕДПРИНИМАТЕЛЬСКИЕ РИСКИ/БИЗНЕС-РИСКИ)	
1.1. Риски в отношениях с пользователем (клиентом)	
1.1.1	Риск несоответствия выполненной работы (оказанная услуга, поставленный товар) ожиданиям пользователя (клиента)
1.1.2	Риск низкой вовлеченности пользователя (клиента) в процесс выполнения работы (оказания услуги, поставки товара)
1.2. Риски отсутствия коммерческого эффекта	
1.2.1	Риск неполучения ожидаемого коммерческого эффекта от выполненной работы (оказанная услуга, поставленный товар) Дело № А56-57100/2017 https://clck.ru/3DbPat
1.3. Риски в отношениях с конкурентами	
1.3.1	Риск нежелательного влияния конкурентов на ход выполнения работы (оказание услуги, поставка товара)
1.4. Риски появления товаров-субститутов	
1.4.1	Риск появления товаров-субститутов, оказывающих влияние на ход выполнения работы (оказание услуги, поставка товара)
1.5. Риски в отношениях с партнерами (поставщиками)	
1.5.1	Риск изменения условий заключенных ранее контрактов (например, увеличение размера арендной платы) Дело № А11-1792/2015 https://clck.ru/3DbP84
1.5.2	Риск повреждения или гибели имущества во время перевозки Дело № А55-11958/2019 https://clck.ru/3DbPUA
2. КОМПЛАЕНС-РИСКИ	
2.1. Риски в отношениях с заказчиком	
2.1.1	Риск несоответствия выполненной работы (оказанная услуга, поставленный товар) ожиданиям заказчика
2.1.2	Риск отказа заказчика от приема и/или оплаты выполненной работы (оказанная услуга, поставленный товар) Дело № А67-7409/2013 https://clck.ru/jeNVy Дело № А67-3080/2011 https://clck.ru/kKntE Дело № А67-8923/2015 https://clck.ru/kS9ZS Дело № А56-125098-2018 https://clck.ru/jeSuC Дело № А33-4846/2020 https://clck.ru/kR9Ag Дело № А67-10731/09 https://clck.ru/kzt9p Дело № А67-5048/2014 https://clck.ru/m3VpN

2.1.2	Дело № А67-6469/2011 https://clck.ru/m45Y6 Дело № А67-3177/2012 https://clck.ru/m4ADb Дело № А67-2917/2014 https://clck.ru/m4KuV Дело № А67-5594/2012 https://clck.ru/m4TpX Дело № А67-754/2010 https://clck.ru/m4Yok Дело №А67-446/2010 https://clck.ru/m4swK Дело № А67-10000/2009 https://clck.ru/m546J Дело № А67-2738/2015 https://clck.ru/m59M5 Дело № А67-3286/2011 https://clck.ru/m5Qmx Дело № А40-137591/21-105-605 https://clck.ru/m5ZRV Дело №2-5454/2021 https://clck.ru/yyhdL Дело №2-4230/2019 https://clck.ru/yyqjs
2.1.3	Риск нарушения сроков оплаты за выполненную подрядчиком работу (оказанная исполнителем услуга, поставленный поставщиком товар) Дело № А67-10732/09 https://clck.ru/m2Hzn Дело № А67-8506/2018 https://clck.ru/m2UKr Дело № А40-46867/13 https://clck.ru/m2qhb
2.1.4	Риск судебного иска от заказчика
2.1.5	Риск недействительности (ничтожности) сделки Дело № А67-1623-2017 https://clck.ru/jec2f Дело № А67-3336/2019 https://clck.ru/m3MUe Дело № А67-3471/2010 https://clck.ru/m4kbL Дело № А67-4580/2016 https://clck.ru/m5nMz
2.1.6	Риск отсутствия возможности досрочно и в одностороннем порядке расторгнуть сделку
2.1.7	Риск неточной или некорректной формулировки и формализации существенных условий в тексте контракта
2.1.8	Риск неверной квалификации вида сделки Дело № А40-137591/21-105-605 https://clck.ru/m5ZRV Дело № А67-3080/2011 https://clck.ru/kKntE Дело № А67-8923/2015 https://clck.ru/kS9ZS
2.1.9	Риск допущения неточных и/или некорректных формулировок в тексте контракта
2.1.10	Риск нарушения установленного между сторонами договора порядка распределения возможной экономии по факту выполненной работы (оказанная услуга, поставленный товар)
2.1.11	Риск отсутствия связи с заказчиком
2.1.12	Риск нарушения заказчиком сроков предоставления информации, необходимой для выполнения работы (оказание услуги, поставка товара), либо риск отказа от предоставления данной информации
2.1.13	Риск изменения требований (выявление новых и/или существенное уточнение ранее согласованных) в процессе выполнения работы (оказание услуги, поставка товара) Дело № А55-9384-2018 https://clck.ru/jeqZv Дело № А40-32033/19-47-287 https://clck.ru/kTCuY

2.1.14	Риск предоставления неполной, недостоверной и/или не соответствующей требованиям национальных стандартов документации (спецификация, устав, техническое задание и/или др.)
2.1.15	Риск низкой вовлеченности заказчика в процесс выполнения работы (оказания услуги, поставки товара)
2.1.16	Риск отсутствия у заказчика корпоративной культуры, работников и опыта ведения деятельности в едином информационном пространстве с использованием информационных систем
2.1.17	Риск отсутствия у заказчика отлаженных корпоративных процедур по информационному взаимодействию и совместной работе его подразделений
2.1.18	Риск отсутствия ключевых и квалифицированных специалистов на стороне заказчика (например, отсутствие лиц, способных определить требования к информационным системам)
2.1.19	Риск недостаточного вовлечения в процесс работы над созданием и согласованием проектных документов всех заинтересованных лиц со стороны заказчика, участвующих в бизнес-процессах, автоматизируемых информационной системой
2.1.20	Риск возможной реструктуризации заказчика (изменение организационной структуры, функциональных обязанностей, бизнес-процессов, локальных актов, финансово-экономической модели и др.)
2.1.21	Риск выявления недостатков при использовании результата выполненной работы (оказанная услуга, поставленный товар) Дело № А45-15497/2020 https://clck.ru/36d7VV
2.2. Риски в отношениях с подрядчиком (исполнитель, поставщик)	
2.2.1	Риск заключения контракта с недобросовестным и ненадежным контрагентом (контрагент-однодневка)
2.2.2	Риск неисполнения подрядчиком (исполнитель, поставщик) своих обязательств, предусмотренных контрактом (невыполнение заявленных требований в срок, невыполнение заявленных требований в полном объеме и др.) Дело № А19-9305-2014 https://clck.ru/jf2No Дело № А40-248300/21-5-1672 https://clck.ru/kRTqS Дело № А67-5330/2014 https://clck.ru/kRkYJ
2.2.3	Риск сокрытия (утаивания) от заказчика и/или искажения подрядчиком (исполнитель, поставщик) информации о реальном положении дел
2.2.4	Риск отсутствия общего видения конечного результата проекта у заинтересованных сторон

2.2.5	Риск неисполнения подрядчиком (исполнитель, поставщик) в процессе выполнения работы (оказание услуги, поставка товара) заявленных в контракте обязательств Дело № А81-9472/2019 https://clck.ru/kScgp
2.2.6	Риск выявления подрядчиком (исполнитель, поставщик) скрытых, не обнаруженных на этапе планирования источников дополнительных затрат
2.2.7	Риск распространения сведений, порочащих деловую репутацию подрядчика (исполнитель, поставщик) Дело № А67-10456/2018 https://clck.ru/jfEaZ
2.2.8	Риск судебного иска от подрядчика (исполнитель, поставщик)
2.2.9	Риск *случайной гибели* материальных средств (материалы, инструменты, оборудование, иное имущество) переданных подрядчику (исполнитель, поставщик) для использования при выполнении работы
2.2.10	Риск *случайного повреждения* материальных средств, используемых при выполнении работы (материалы, инструменты, оборудование, иное имущество) переданных подрядчику (исполнитель, поставщик) для использования при выполнении работы
2.3. Риски отношений в области права на результаты интеллектуальной деятельности (РИД)	
2.3.1	Риск нарушения авторских прав Дело № А40-117808/10-12-740 https://clck.ru/jfNtn Дело № 88-10803/2020 https://clck.ru/yyJAZ Дело № 1-209/2022 https://clck.ru/36eUWo Дело № 5-1637/2021 https://clck.ru/36eUaL
2.3.2	Риск запрета правообладателем использования РИД Дело № А40-202764/18-110-1552 https://clck.ru/jfczi Дело № А60-27815/2012 https://clck.ru/jfedG Дело № А40-81328/11 https://clck.ru/jfgaN Дело № А40-162480/13 https://clck.ru/jfiJj Делу № А53-23110/22 https://clck.ru/36cr8y
2.3.3	Риск взыскания правообладателем убытков (компенсации) за нарушение прав на РИД Дело № 02-4545/2017 https://clck.ru/ohZBK Дело № А67-8506/2018 https://clck.ru/m2UKr Дело № А50-17729/2022 https://clck.ru/36ck9B Дело № А81-11865/2022 https://clck.ru/36cpoK Дело № А50-4247/2023 https://clck.ru/36cpzX Дело № А36-7440/2022 https://clck.ru/36cq88 Дело № А35-7078/2022 https://clck.ru/36d5KQ Дело № А29-10372/2022 https://clck.ru/36d5W7 Дело № А50-17729/2022 https://clck.ru/36d5id Дело № А14-13243/2022 https://clck.ru/36d7f5 Дело № А08-16/2022 https://clck.ru/36d7n5

2.3.4	Риск невозможности признания прав на РИД за правообладателем Дело № 2-1564/15 https://clck.ru/ohzje Дело № А40-90889/21-134-529 https://clck.ru/36cmjw Дело № А45-17338/2022 https://clck.ru/36cpVV
2.3.5	Риск создания нежелательного производного произведения Дело № А56-38522/2020 https://clck.ru/36d4mB
2.3.6	Риск ограничения для последующих сублицензионных контрактов
2.3.7	Риск расторжения контракта в «сублицензионной цепочке» контрактов
2.4. Риски в отношениях с субподрядчиком (субисполнитель, субпоставщик)	
2.4.1	Риск отсутствия связи с субподрядчиком (субисполнитель, субпоставщик)
2.4.2	Риск несоответствия полученного субподрядчиком (субисполнитель, субпоставщик) результата (оказанная услуга, поставленный товар) ожиданиям заинтересованных сторон
2.4.3	Риск судебного иска от субподрядчика (субисполнитель, субпоставщик)
2.5. Имущественные риски	
2.5.1	Риск гибели и/или повреждения электронного оборудования (компьютеров, серверов и др.) и другого имущества в результате пожара, затопления водой и др.
2.5.2	Риск гибели и/или повреждения электронного оборудования (компьютеры, серверы и др.) и иного имущества в результате противоправных действий третьих лиц (умышленное уничтожение или повреждение имущества, уничтожение или повреждение имущества по неосторожности, хулиганство, вандализм)
2.5.3	Риск банкротства
2.6. Криминальные риски	
2.6.1	Риск промышленного шпионажа
2.6.2	Риск утечки конфиденциальных данных
2.6.3	Риск ограбления
2.6.4	Риск незаконного получения и разглашения сведений, составляющих коммерческую тайну Дело№ 1-583/2022 https://clck.ru/3DrXiQ Дело № 1-159/2015 https://clck.ru/3DrXYw
2.6.5	Риск преднамеренного неисполнения контрактных обязательств в случаях причинения значительного ущерба (не менее 200 тыс. руб.), крупного ущерба (свыше 3 млн руб.) либо особо крупного ущерба (свыше 12 млн руб.)

2.7. Риски соблюдения условий государственных (муниципальных) контрактов	
2.7.1	Риск признания недействительными государственного (муниципального) контракта (доступ к исполнению контракта без конкурентной борьбы) (44-ФЗ) Дело № А73-6308/2022 https://clck.ru/32RZZe
2.7.2	Риск отказа от заключения государственного (муниципального) контракта (223-ФЗ) Дело № А67- 3336/2019 https://clck.ru/m3MUe (223-ФЗ) Дело № А67- 7005/2020 https://clck.ru/32RrGK
2.7.3	Риск отказа государственного (муниципального) заказчика от приемки и/или оплаты выполненной работы (оказанная услуга, поставленный товар) (223-ФЗ) Дело № А67- 2896/2017 https://clck.ru/324gBZ (44-ФЗ) Дело № А22–1041/2020 https://clck.ru/32S3hq (44-ФЗ) Дело № А22–1042/2020 https://clck.ru/32S3kq (44-ФЗ) Дело № А40-276728/19-120-2085 https://clck.ru/32S4Pk
2.7.4	Риск несоответствия выполненной работы (оказанная услуга, поставленный товар) требованиям государственного (муниципального) контракта (44-ФЗ) Дело № А40-263677/21-51-1834 https://clck.ru/32Rowo (44-ФЗ) Дело № А83-14689/2020 https://clck.ru/32S5dv
2.7.5	Риск отказа государственного (муниципального) заказчика в одностороннем порядке от исполнения государственного (муниципального) контракта (44-ФЗ) Дело № А03-5595/2021 https://clck.ru/32RsSP (44-ФЗ) Дело № А03-14616/2020 https://clck.ru/32RtCX (44-ФЗ) Дело № А56-107933/2019 https://clck.ru/32S4yT
3. ПРОЕКТНЫЕ РИСКИ	
3.1. Риски руководителей проекта	
3.1.1	Риск допущения ошибки руководителем проекта при оценивании стоимости проектных работ
3.1.2	Риск допущения ошибки руководителем проекта при оценивании длительности проектных работ
3.1.3	Риск неучета отпусков и государственных праздников при создании плана проекта
3.1.4	Риск допущения ошибки руководителем проекта при оценивании ресурсов, необходимых для выполнения проектных работ
3.1.5	Риск нерационального расходования ограниченных ресурсов проекта
3.1.6	Риск отсутствия знаний, навыков и опыта у руководителя проекта
3.1.7	Риск ухода руководителя из проекта

3.1.8	Риск низкой производительности труда у руководителя проекта
3.1.9	Риск отсутствия заинтересованности руководителя проекта в успешном завершении проекта
3.1.10	Риск занятости руководителя проекта в других проектах
3.1.11	Риск неправильного ранжирования задач руководителем проекта
3.1.12	Риск завышения качества руководителем проекта
3.1.13	Риск отсутствия в проекте инструментария управления проектом (например, PRINCE2, SCRUM и др.)
3.1.14	Риск отсутствия ресурсов для выполнения проектных работ
3.1.15	Риск заниженной оценки проектных работ, по факту оказавшихся более сложными, чем предполагалось изначально
3.1.16	Риск длительного согласования заинтересованными сторонами информации при выработке управленческих решений
3.1.17	Риск отсутствия резервов, необходимых для принятия материализовавшихся рисков
3.1.18	Риск потери и/или отсутствия контроля руководителем проекта
3.1.19	Риск конфликта между руководителем проекта и заинтересованными сторонами (заказчик, участник команды и др.)
3.1.20	Риск утери информации о материализовавшихся рисках, необходимой руководителю проекта в последующих проектах
3.1.21	Риск привлечения в проект руководителя проекта, имеющего профессиональное образование в области управления проектами
3.1.22	Риск привлечения в проект руководителя проекта, имеющего опыт управления проектами более 4-х лет
3.1.23	Риск самостоятельного формирования команды проекта руководителем проекта
3.1.24	Риск изменения содержания проекта
3.1.25	Риск изменения длительности проекта
3.1.26	Риск изменения стоимости проекта
3.1.27	Риск изменения качества проекта
3.1.28	Риск декомпозиции большого проекта на малые проекты (длительностью не более 4-х месяцев)
3.2. Риски участников проекта	
3.2.1	Риск простоя трудовых ресурсов
3.2.2	Риск конфликта интересов между заинтересованными сторонами
3.2.3	Риск неполного выявления ВСЕХ заинтересованных сторон
3.2.4	Риск возможного прерывания работы участником проекта вследствие временной нетрудоспособности (уход «больничный»)

3.2.5	Риск допущения ошибок участниками проекта при его реализации проекта (bugs)
3.2.6	Риск значительной временной задержки в получении ответов на задаваемые вопросы между участниками проекта
3.2.7	Риск возникновения эффекта Кассандры (образование переизбытка каналов коммуникации, несущих актуальную информацию)
3.2.8	Риск сокращения (менее 8 ч в день) фактического времени работы участников проекта
3.2.9	Риск отсутствия знаний, навыков и опыта у участников проекта, необходимых для реализации требований к проекту
3.2.10	Риск ухода ключевого участника проекта из проекта
3.2.11	Риск перегрузки трудовых ресурсов (сверхурочная работа и др.)
3.2.12	Риск неправильного оценивания участниками проекта трудозатрат, необходимых для выполнения проектных работ
3.2.13	Риск некорректной, ошибочной декомпозиции проектных работ участниками проекта
3.2.14	Риск занятости участников проекта в других проектах
3.2.15	Риск изменения состава участников проекта в процессе его реализации
3.2.16	Риск непонимания участниками проекта конечного результата проекта, который должен быть получен по завершении проекта
3.2.17	Риск нескоординированности действий участников проекта
3.2.18	Риск низкой производительности труда участников проекта
3.2.19	Риск отсутствия заинтересованности участников проекта в успешном завершении проекта
3.2.20	Риск создания негативной социально-психологической атмосферы в процессе выполнения проекта
3.2.21	Риск отсутствия либо недостатка внутрикорпоративных коммуникаций между участниками проекта
3.2.22	Риск использования устаревших технологий участниками проекта
3.2.23	Риск привлечения в проект высококвалифицированного работника
3.2.24	Риск определения эффективного числа участников проекта (не более 6 человек)
3.2.25	Риск коллаборации между руководителем и участниками проекта (групповая выработка решений, реализация индивидуальных идей и др.)
3.2.26	Риск привлечения в проект сторонних экспертов и советников

3.2.27	Риск утери согласованных заинтересованными сторонами изменений проекта
3.2.28	Риск невостребованности полученных результатов проекта (запрошенная функциональность программы для ЭВМ будет реализована, но никто не будет ее использовать)
3.3. Технологические риски	
3.3.1	Риск отключения электричества
3.3.2	Риск отключения интернета
3.3.3	Риск применения ранее не используемых технологий участниками проекта (языки программирования и др.)
3.3.4	Риск поломки оборудования
4. РИСКИ ВНЕШНЕЙ СРЕДЫ	
4.1. Экономические риски	
4.1.1	Риск изменения цен на нефть
4.1.2	Риск изменения цен на газ
4.1.3	Риск изменения цен на металлы
4.1.4	Риск изменения цен на уголь
4.1.5	Риск изменения цен на зерно
4.1.6	Риск изменения цен на уран
4.1.7	Риск дефицита (профицита) федерального бюджета
4.1.8	Риск изменения курса валют
4.1.9	Риск внесения изменений в Федеральный закон «О федеральном бюджете» (секвестирование бюджета)
4.1.10	Риск изменения налоговой политики
4.1.11	Риск изменения размера государственного долга
4.1.12	Риск изменения денежно-кредитной политики
4.1.13	Риск эмиссии денежной массы
4.1.14	Риск изменения ключевой ставки
4.1.15	Риск изменения процентов кредитных и депозитных ставок
4.1.16	Риск изменения темпов инфляции
4.1.17	Риск изменения темпов роста экономики
4.1.18	Риск изменения уровня жизни населения
4.1.19	Риск изменения фондовых индексов
4.1.20	Риск запрета торговли ценными бумагами определенных организаций
4.1.21	Риск дефолта
4.1.22	Риск экономического кризиса

4.2. Общественные риски	
4.2.1	Риск изменения уровня смертности
4.2.2	Риск изменения уровня рождаемости
4.2.3	Риск изменения численности населения
4.2.4	Риск отсутствия на рынке труда квалифицированных кадров
4.2.5	Риск социальной напряженности
4.2.6	Риск изменения уровня образования
4.2.7	Риск изменения уровня медицины
4.2.8	Риск изменения уровня преступности
4.2.9	Риск изменения уровня миграции
4.2.10	Риск голода
4.2.11	Риск изменения духовно-нравственной (культурной) сферы
4.3. Политические риски	
4.3.1	Риск изменения геополитического давления Дело № А55-16114/2022 https://clck.ru/3Db6DS Дело № А51-15300/2022 https://clck.ru/3Db6R5 Дело № А32-32694/2022 https://clck.ru/3Db6Yb Дело № А60-18476/2022 https://clck.ru/3Db6eA
4.3.2	Риск расширения альянса НАТО
4.3.3	Риск военного конфликта
4.3.4	Риск введения военного положения
4.3.5	Риск террористического акта
4.3.6	Риск изменения норм действующего законодательства
4.3.7	Риск нарушения норм действующего законодательства (привлечение к ответственности органами ФНС, СФР и др.) Дело № А67-4230/2017 https://clck.ru/m6N5G Дело № А67-3622/10 https://clck.ru/m3mBo
4.3.8	Риск признания контрагента недобросовестным налогоплательщиком (необоснованная налоговая выгода и наложение санкций (отказ в предоставлении налогового вычета др.)
4.3.9	Риск нарушения требований в области защиты информации Постановление № 5-300/2015 https://clck.ru/36ZdQH
4.3.10	Риск материализации обстоятельств непреодолимой силы, оказавших значительное влияние на выполнение работ
4.3.11	Риск интеграции Российской Федерации с внешними субъектами
4.3.12	Риск государственного переворота
4.3.13	Риск национализации и экспроприации имущества
4.3.14	Риск редомициляции
4.3.15	Риск гражданской войны
4.3.16	Риск массовых беспорядков
4.3.17	Риск импичмента президента

4.4. Экологические риски	
4.4.1	Риск нехватки природных ресурсов
4.4.2	Риск изменения климата
4.4.3	Риск загрязнения окружающей среды
4.4.4	Риск пандемии
4.4.5	Риск наводнения
4.4.6	Риск радиоактивного заражения
4.4.7	Риск тайфуна
4.4.8	Риск землетрясения
4.4.9	Риск падения космического тела
4.4.10	Риск извержения вулкана
4.4.11	Риск пожара
4.4.12	Риск уничтожения Земли
4.4.13	Риск таяния ледников
4.5. Технологические риски	
4.5.1	Риск атаки на критическую инфраструктуру
4.5.2	Риск использования новой технологии
4.5.3	Риск поломки оборудования из-за отсутствия импортных комплектующих
4.5.4	Риск нехватки электроэнергии
4.5.5	Риск атаки искусственного интеллекта (ИИ)
4.5.6	Риск отключения глобальной компьютерной сети Интернет
4.5.7	Риск неправомерного доступа к компьютерной информации (уничтожение, блокирование, модификация либо копирование) Дело № 1-257/2023 https://clck.ru/36UcMi Дело № 1-457/2022 https://clck.ru/36Ucs4 Дело № 1-41/2017 https://clck.ru/36VChA Дело № 1-190/2016 https://clck.ru/36VDoX
4.5.8	Риск создания, использования и распространения вредоносных компьютерных программ (уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств защиты компьютерной информации) Дело № 1-355/2023 https://clck.ru/36UeHN Дело № 1-226/2023 https://clck.ru/36UeQA Дело № 1-981/2022 https://clck.ru/36UebR
4.5.9	Риск нарушения правил эксплуатации средств хранения и обработки компьютерной информации (уничтожение, блокирование, модификация либо копирование, причинившее крупный ущерб, т. е. ущерб, сумма которого превышает 1 млн руб.) Дело № 1-22/2021 https://clck.ru/36Uezy

4.5.10	Риск неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (КИИ РФ) (уничтожение, блокирование, модификация, копирование информации или нейтрализация средств защиты) Дело № 1-171/2023 https://clck.ru/36UdEr
4.5.11	Риск хищения имущества путем ввода, удаления, блокирования, модификации компьютерной информации т. е. риск мошенничества в сфере компьютерной информации Дело № 1-422/2016 https://clck.ru/36YYyT Дело № 1-12/2017 (1-123/2016;) https://clck.ru/36YaTs Дело № 1-30/2018 https://clck.ru/36YbWy
4.5.12	Риск нарушения правил защиты информации (использование несертифицированных ИС и БД, а также несертифицированных средств защиты информации) Постановление № 5-300/2015 https://clck.ru/36ZdQH
4.5.13	Риск дезинформации

Приложение В

ПРИМЕРЫ КОВЕНАНТОВ В ДОГОВОРЕ ПОДРЯДА

Название риска	Ковенанты и меры элиминирования универсальных рисков
1. Риск несоответствия выполненной работы (оказанная услуга, поставленный товар) ожиданиям заказчика	Согласно PMBOK Guide® сторона заказчика ожидает, что проектные работы будут выполнены в полном объеме, к определенной дате, в согласованный бюджет и на требуемом уровне качества [14; 15; 16]. Логично предположить, что получения релевантной программы для ЭВМ, которую ожидает заказчик, объем, дата окончания, цена, а также качество должны быть точно сформулированы и корректно формализованы в тексте договора. Кроме того, следует отметить, что согласно действующему 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 создания программы для ЭВМ. В силу ст. 708 ГК РФ цена в тексте договора может быть твердой (*Fixed Price*) либо приблизительной (*Time & Materials*)
2. Риск отказа заказчика от приемки выполненной работы (оказанная услуга, поставленный товар)	Для элиминирования комплаенс-риска рекомендуется в тексте договора зафиксировать процедуру сдачи-приемки программы для ЭВМ
3. Риск отказа заказчика от оплаты выполненной работы (оказанная услуга, поставленный товар)	Согласно ст. 702 ГК РФ заказчик обязуется принять результат выполненных работ и оплатить его. Следовательно, основанием для оплаты выполненных работ является факт приемки работ без претензий и замечаний

Название риска	Ковенанты и меры элиминирования универсальных рисков
4. Риск нарушения сроков оплаты за выполненную подрядчиком (исполнитель, поставщик) работу (оказанная услуга, поставленный товар)	Для уменьшения негативного влияния комплаенс-риска в тексте договора рекомендуется зафиксировать порядок применения мер санкционирования в случае нарушения порядка и сроков оплаты
5. Риск судебного иска от заказчика и(или) подрядчика (исполнитель, поставщик)	Полностью нивелировать комплаенс-риск с помощью ковенантов не представляется возможным. Однако можно уменьшить негативное влияние в случае материализации данного риска. Для этого необходимо добросовестно исполнить предусмотренные договором обязательства, а также обеспечить *правовую чистоту* проектных документов, т. е. полное соответствие проектных документов требованиям действующего законодательства
6. Риск признания сделки, заключенной между сторонами, недействительной	Согласно гл. 37 ГК РФ существенными условиями договора подряда являются предмет договора, дата начала и дата окончания работ. Следовательно, для нивелирования данного риска необходимо, чтобы в тексте договора существенные условия были точно сформулированы и корректно формализованы
7. Риск невозможности расторжения сделки досрочно и в одностороннем порядке	Анализ судебных решений показал, что сторона сделки, как правило, не может досрочно и в одностороннем порядке расторгнуть договор, не причинив существенных материальных последний, поэтому для элиминирования данного риска рекомендуется проектные работы дифференцировать на этапы с указанием даты начала и окончания каждого этапа
8. Риск неточной формулировки и/или некорректной формализации предмета контракта	Уменьшение вероятности наступления риска возможно при повышении уровня зрелости в части управления коммуникациями и управления договорами в ИТ-проекте

Название риска	Ковенанты и меры элиминирования универсальных рисков
9. Риск неверной квалификации вида сделки	Для уменьшения вероятности материализации риска рекомендуется обеспечить соответствие между текстом договора и требованиями действующего законодательства
10. Риск допущения некорректных и неточных формулировок в тексте контракта	Нивелировать комплаенс-риск можно при повышении уровня зрелости в части управления коммуникациями проекта, так как выработка корректных и точных формулировок возможна при согласованных действиях заинтересованных сторон
11. Риск отсутствия порядка учета и распределения возможной экономии по факту выполненной работы (оказанная услуга, поставленный товар) между договаривающимися сторонами	В соответствии со ст. 710 ГК РФ в случаях, когда фактические расходы подрядчика оказались меньше зафиксированных в тексте договора, подрядчик сохраняет право на оплату работ по цене, предусмотренной договором
12. Риск отсутствия связи с заказчиком	Для нивелирования риска рекомендуется в текст договора включить следующий ковенант: «Длительный простой трудовых ресурсов подрядчика, превышающий 5 рабочих дней, оплачивается заказчиком по тарифу простоя трудовых ресурсов подрядчика. Тариф простоя трудовых ресурсов подрядчика равен 1 000,00 руб. за 1 человеко-час»
13. Риск нарушения заказчиком сроков предоставления информации, необходимой для выполнения работы (оказание услуги, поставка товара), либо отсутствие данной информации по вине заказчика	Для нивелирования риска рекомендуется в текст договора включить следующий ковенант: «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»

Название риска	Ковенанты и меры элиминирования универсальных рисков
14. Риск изменения требований в процессе выполнения работы (оказание услуги, поставка товара), т. е. выявление новых и/или существенное уточнение ранее согласованных требований	Элиминирование риска зависит от вида используемой подрядчиком (исполнитель, поставщик) концепции для создания программ для ЭВМ – Waterfall [Balaji, 2012] или Agile [Lee et al, 2013]. Если применяется Waterfall, то любые изменения требований к функциональности программы для ЭВМ могут привести к отклонению от запланированных целей проекта, в связи с чем рекомендуется в тексте договора фиксировать «жесткие» ковенанты; если — Agile, то изменение требований не оказывает сильного негативного влияния на процесс достижения проектных целей, поэтому в текст договора рекомендуется включение более «мягких» ковенантов
15. Риск несоответствия технического задания требованиям национальных стандартов либо предоставления неполной и/или недостоверной информации в ТЗ	Уменьшить вероятность материализации комплаенс-риска можно, если проектные работы выполняют специалисты, обладающие необходимыми профессиональными компетенциями. Например, специалист, разрабатывающий спецификацию, должен соответствовать требованиями профессионального стандарта код 06.022 «Системный аналитик»
16. Риск низкой вовлеченности заказчика в процесс выполнения работ (оказание услуги, поставка товара)	Согласно ст. 715 ГК РФ заказчик вправе в любое время проверять ход и качество выполняемой работы
17. Риск отсутствия у заказчика корпоративной культуры, квалифицированных специалистов и опыта ведения деятельности в едином информационном пространстве с использованием ИС	Для элиминирования риска рекомендуется в текст договора включить ковенант, закрепляющий ответственность за управление данным риском за заказчиком

Название риска	Ковенанты и меры элиминирования универсальных рисков
18. Риск отсутствия у заказчика отлаженных корпоративных процедур по информационному взаимодействию и совместной работе его подразделений	Для элиминирования риска рекомендуется в текст договора включить ковенант, закрепляющий ответственность за управление данным риском за заказчиком
19. Риск отсутствия ключевых и квалифицированных специалистов на стороне заказчика (специалистов, способных определить требования к ИС, и др.)	Для элиминирования риска в тексте договора рекомендуется в текст договора включить следующий ковенант: «Ответственность за действия ответственных и иных лиц заказчика, в том числе привлеченных заказчиком третьих лиц, несет заказчик»
20. Риск пренебрежения условием о необходимости включения в процесс создания и согласования проектных документов ВСЕХ заинтересованных лиц со стороны заказчика, участвующих в автоматизируемых бизнес-процессах	Для элиминирования риска требуется достижение определенного уровня зрелости в части управления коммуникациями в ИТ-проекте. В частности, должен быть создан механизм контроля за процессами создания, сбора, распространения, хранения, получения и использования информации
21. Риск возможной реструктуризации организации заказчика (изменение организационной структуры, функциональных обязанностей, бизнес-процессов, локальных актов, финансово-экономической модели и др.)	Для элиминирования риска рекомендуется в текст договора включить ковенант, закрепляющий ответственность за управление данным риском за заказчиком.

Название риска	Ковенанты и меры элиминирования универсальных рисков
22. Риск неисполнения в срок подрядчиком (исполнитель, поставщик) обязательств, предусмотренных договором (заявленные требования, установленный объем работ и др.)	Для элиминирования риска в части невыполнения подрядчиком (исполнитель, поставщик) заявленных требований в срок или работ в полном объеме в тексте договора рекомендуется зафиксировать порядок санкционирования. В части, касающейся качества работ, необходимо опираться на ст. 723 ГК РФ
23. Риск сокрытия и/или искажения подрядчиком (исполнитель, поставщик) информации о реальном положении дел по договорным обязательствам перед заказчиком	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 либо создают невозможность ее завершения в срок
24. Риск отсутствия у заинтересованных сторон общего видения конечного результата	Для элиминирования риска требуется достичь определенного уровня зрелости в части управления коммуникациями в ИТ-проекте. В частности, должен быть создан механизм контроля за процессами создания, сбора, распространения, хранения, получения и использования информации
25. Риск невозможности исполнения подрядчиком (исполнитель, поставщик) в процессе выполнения работ (оказание услуг, поставка товаров) заявленных в договоре обязательств собственными силами	Согласно ст. 706 ГК РФ в случаях, когда по условиям сделки оговорено личное исполнение работ подрядчиком, то подрядчик не вправе привлекать к исполнению своих обязательств других лиц (субподрядчиков)
26. Риск выявления подрядчиком (исполнитель, поставщик) скрытых, не обнаруженных на этапе планирования источников дополнительных затрат	В силу ст. 709 ГК РФ цена работы может быть твердой или приблизительной. Следовательно, для уменьшения вероятности материализации риска рекомендуется использование условий, при которых цена будет рассчитываться на основании фактически израсходованных ресурсов подрядчика (T&M).

Название риска	Ковенанты и меры элиминирования универсальных рисков
27. Риск распространения сведений, порочащих деловую репутацию подрядчика (исполнитель, поставщик)	Согласно ст. 152 ГК РФ деловая репутация признается нематериальным благом, защита которого гарантирована действующим законодательством, поэтому за распространение информации, порочащей честь и достоинство, законодателем установлена гражданско-правовая, административная и уголовная ответственность. Ст. 5.61 КоАП РФ предусматривает ответственность за оскорбление (унижение чести и достоинства, выраженное в неприличной форме) в виде наложения административного штрафа. В ст. 128.1 УК РФ предусмотрен штраф за клевету (распространение заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию) в размере до 500 тыс. руб.
28. Риск нарушения исключительных прав на результаты интеллектуальной деятельности	Для увеличения лояльности заказчика и элиминирования риска в тексте договора рекомендуется формализовать следующий ковенант: «Подрядчик гарантирует заказчику, что на момент предоставления заказчику права использования результата выполненных работ подрядчик будет являться его единственным правообладателем. 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»
29. Риск взыскания правообладателем (автором) вознаграждения за использование его исключительных прав на РИД	Элиминирование риска возможно при повышении уровня зрелости в части управления договорами в ИТ-проекте

Название риска	Ковенанты и меры элиминирования универсальных рисков
30. Риск запрещения правообладателем (автором) использования РИД	Элиминирование риска возможно при повышении уровня зрелости в части управления договорами в ИТ-проекте
31. Риск невозможности признания исключительного права на РИД за правообладателем (автором)	Элиминирование риска возможно при повышении уровня зрелости в части управления договорами в ИТ-проекте
32. Риск создания нежелательного производного произведения	В силу ст. 1 259 ГК РФ производные произведения являются отдельными произведениями. Следовательно, исключительные права на РИД будут принадлежать лицу, переработавшему (модифицировавшему) ранее созданную программу для ЭВМ. Для нивелирования риска рекомендуется включить в текст договора следующий ковенант: «Заказчик не имеет права изменять любым способом, переданную ему во владение программу для ЭВМ, например, проводить декомпилирование, реассамблирование, реижиниринг и иные другие переработки (модификации)».
33. Риск ограничения для заключения последующих сублицензионных договоров	Для элиминирования риска в тексте договора рекомендуется предусмотреть штраф за несогласованное ограничение для последующих сублицензионных договоров
34. Риск расторжения договора в «сублицензионной цепочке» договоров	Для элиминирования риска в тексте договора рекомендуется предусмотреть штраф за несогласованное ограничение для последующих сублицензионных договоров
35. Риск отсутствия связи с субподрядчиком	Согласно ст. 706 ГК РФ генеральный подрядчик несет перед заказчиком ответственность за последствия неисполнения или ненадлежащего исполнение обязательств субподрядчиком. Уменьшение вероятности материализации комплаенс-риска возможно при повышении уровня зрелости в части управления договорами в ИТ-проекте

Название риска	Ковенанты и меры элиминирования универсальных рисков
36. Риск несоответствия полученного субподрядчиком результата ожиданиям заинтересованных сторон	Элиминирование риска возможно при повышении уровня зрелости в части управления коммуникациями в ИТ-проекте
37. Риск судебного иска от субподрядчика	Полностью нивелировать риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации посредством добросовестного исполнения предусмотренных договором обязательств, а также обеспечения «правовой чистоты» проектных документов, т. е. полного соответствия проектных документов требованиям действующего законодательства
38. Риск гибели и/или повреждения электронного оборудования (компьютеры, серверы и др.) и другого имущества в результате пожара, затопления водой и др.	Уменьшение вероятности материализации риска возможно при повышении уровня зрелости в части управления договорами в ИТ-проекте, а именно заключения договора страхования (гл. 48 ГК РФ)
39. Риск гибели и (или) повреждения электронного оборудования (компьютеры, серверы 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 риска возможно при повышении уровня зрелости в части управления договорами в ИТ-проекте, а именно заключения договора страхования (гл. 48 ГК РФ).

Название риска	Ковенанты и меры элиминирования универсальных рисков
40. Риск промышленного шпионажа	Для уменьшения возможного материального ущерба от материализации комплаенс-риска рекомендуется заключать с заинтересованными сторонами проекта соглашения о неразглашении конфиденциальной информации
41. Риск утечки конфиденциальных данных	Для элиминирования риска в тексте договора рекомендуется предусмотреть следующий ковенант: «Условия договора, приложений и дополнительных соглашений к нему конфиденциальны и не подлежат разглашению в течение всего срока действия договора и в течение 3 лет после прекращения его действия. В случае неисполнения или ненадлежащего исполнения обязательств конфиденциальности недобросовестная сторона несет ответственность в соответствии с действующим законодательством и обязуется полностью возместить причиненный ущерб, включая упущенную выгоду»
42. Риск получения штрафа за нарушение действующего законодательства (привлечение к ответственности органами Федеральной налоговой службы, Пенсионным фондом Российской Федерации и др.)	Полностью нивелировать комплаенс-риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации при добросовестном исполнении предусмотренных действующим законодательством обязательств
43. Риск изменения норм действующего законодательства	Полностью нивелировать комплаенс-риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации при добросовестном исполнении предусмотренных действующим законодательством обязательств

Название риска	Ковенанты и меры элиминирования универсальных рисков
44. Риск материализации обстоятельств непреодолимой силы, оказывающих значительное влияние на ход выполнения работ (оказание услуг)	Для уменьшения возможного материального ущерба от материализации комплаенс-риска в тексте договора рекомендуется предусмотреть следующий ковенант: «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»
45. Риск нарушения норм действующего законодательства	Полностью нивелировать комплаенс-риск с помощью условий договора не представляется возможным. Однако можно уменьшить негативное влияние в случае его материализации, для чего необходимо добросовестно исполнить предусмотренные действующим законодательством обязательства

Приложение Г

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 информационных технологий	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

Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
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
13. Угроза истощения ресурсной базы топливно-сырьевых отраслей по мере исчерпания действующих месторождений	3,5	5

Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
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

Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
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
30. Угроза активизации деятельности вооруженных сил отдельных государств (групп государств) с проведением частичной или общей мобилизации	3,5	3,5

Название угрозы	Оценка вероятности материализации угрозы	Оценка возможного влияния в случае наступления угрозы
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

УЧЕБНОЕ ИЗДАНИЕ

Валентин Сергеевич Николаенко

БЕЗУПРЕЧНЫЙ РИСК-МЕНЕДЖМЕНТ В СИСТЕМЕ ГОСУДАРСТВЕННОГО И МУНИЦИПАЛЬНОГО УПРАВЛЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Учебное пособие

Подписано в печать 22.10.2025. Формат 60x84/16.
Усл. печ. л. 11,7. Тираж 100 экз. Заказ 173.
Федеральное государственное автономное
образовательное учреждение высшего образования
«Томский государственный университет
систем управления и радиоэлектроники»
634050, г. Томск, пр. Ленина, 40.
Тел. (3822) 53-30-18. E-mail: rio@main.tusur.ru