

КАЗАНСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА,
РОБОТОТЕХНИКИ И СИСТЕМНОЙ ИНЖЕНЕРИИ

КАФЕДРА ТЕХНОЛОГИЧЕСКОГО ПРЕДПРИНИМАТЕЛЬСТВА

А. Р. ЗАКИРОВА, Б. А. ЗАППАРОВ, Р. Л. ФЕЙФЕР

УПРАВЛЕНИЕ РИСКАМИ ПРОЕКТОВ

Учебное пособие



Казань
2025

УДК 658.56
ББК 65.2/4

*Рекомендовано к изданию
Учебно-методической комиссией ИИРСИ КФУ
(протокол № 2 от 28 апреля 2025 г.)*

Рецензенты:

кандидат технических наук, начальник коммерческого отдела **И.Р. Калимуллин**
кандидат технических наук, доцент **Э.М. Хуснутдинова**

Закирова А.Р.

318 Управление рисками проектов: учебное пособие/А. Р. Закирова, Б. А. Заппаров, Р. Л. Фейфер – Казань: КФУ, 2025. – 96 с.

Рассмотрены основы управления рисками проектов с учетом требований профстандарта 08.018 «Специалист по управлению рисками», утвержденному приказом Министерства труда и социальной защиты РФ от 30 августа 2018 года N 564н. Учебное пособие может быть полезным для обучающихся по инженерным, технологическим и экономическим направлениям вузов; слушателей школ бизнеса и системы повышения квалификации и переподготовки кадров; преподавателям вузов, работникам исследовательских и консалтинговых фирм, предпринимательских структур, руководителям и специалистам предприятий.

УДК 658.56
ББК 65.2/4

СОДЕРЖАНИЕ

	ВВЕДЕНИЕ	4
Тема 1	Основные термины и определения по управлению рисками	13
Тема 2	Принципы менеджмента риска проекта	23
Тема 3	Интеграция процессов менеджмента риска с процессами менеджмента проекта	28
Тема 4	Контекст функционирования организации и процесса управления рисками	32
Тема 5	Структура менеджмента риска	36
Тема 6	Процесс менеджмента риска	40
Тема 7	Уровни принятия решений менеджмента рисков	45
Тема 8	Законодательство Российской Федерации и отраслевые стандарты по управлению рисками	48
Тема 9	Базовые положения международных стандартов по риск-менеджменту и смежным вопросам	52
Тема 10	Требования к обеспечению сохранения коммерческой тайны	57
Тема 11	Информационная политика организации	68
Тема 12	Нормы корпоративного управления и корпоративной культуры	72
Тема 13	Нормы профессиональной этики	78
	ЗАКЛЮЧЕНИЕ	83
	ГЛОССАРИЙ	84
	СПИСОК ЛИТЕРАТУРЫ	93

ВВЕДЕНИЕ

Конкуренция на рынке постоянно растет. Для привлечения и удержания клиентов компаниям нужно подстраиваться под растущие требования аудитории, оперативно выполнять задачи и решать проблемы. Одним из способов эффективной организации работы внутри компании является проектный менеджмент.

Проект – это комплекс мероприятий, ограниченных по времени, с общей целью по созданию нового продукта или услуги, достижению определенных результатов. Управление проектами позволяет организовать работу таким образом, чтобы выполнить все требования к проекту. Для достижения успехов, менеджеру понадобятся технические знания по проекту, качества управленца, умение решать проблемы и организовывать работу в коллективе.

Разработано множество документов управления проектами, например, международные стандарты; одним из самых известных из них является PMBOK (A Guide to the Project Management Body of Knowledge). Это руководство по управлению проектами, где приведена терминология и базовые принципы. Его применяют в более чем в 160 странах мира. Первый РМВоК вышел в 1996 году. С того времени его регулярно обновляют и дополняют, поскольку появляется новый управленческий опыт, новые проблемы и их решения. Актуальное издание на январь 2024 года – седьмая версия РМВОК (2021).

Согласно данному руководству, проект – это «временное предприятие, направленное на создание уникального продукта, услуги или результата» [1]. Именно уникальность создает почву для многочисленных рисков при реализации на любом из этапов жизненного цикла проекта: инициировании, планировании, исполнении, мониторинге и контроле, закрытии. Поэтому необходимо постоянно оценивать подверженность риску как в виде возможностей, так и в виде угроз, для максимизации положительных и минимизации отрицательных воздействий на ход проекта и его конечные результаты.

Угрозы могут представлять такие проблемы, как задержки сроков, превышение стоимости, технические отказы, снижение показателей исполнения или потеря репутации. Возможности могут вести к таким выгодам, как сокращение сроков и стоимости, улучшение показателей исполнения, повышение доли на рынке или укрепление репутации.

Управление риском – это меры, направленные на изменение риска. Управление риском охватывает процессы, политику, устройства, методы и другие средства, используемые для модификации риска. Управление не всегда может привести к ожидаемым результатам изменения риска. Поэтому командам проектов также рекомендуется осуществлять мониторинг совокупного риска проекта.

Совокупный риск проекта – это эффект от неопределенности на проект в целом. Совокупный риск возникает из любых источников неопределенности, включая индивидуальные риски, и представляет собой влияние последствий вариаций результатов проекта, как положительных, так и отрицательных, на заинтересованные стороны. Для более полного понимания совокупного риска может осуществляться объединение нескольких видов в один риск. Управление совокупным риском проекта стремится удерживать подверженность проекта риску в приемлемом диапазоне.

Организации и команды проектов, применяющие единообразную оценку рисков, планирование и проактивную реализацию рисков, часто обнаруживают снижение стоимости трудозатрат по сравнению с ситуацией реагирования на проблемы после возникновения риска.

Кроме того, в процессе анализа могут быть выявлены позитивные риски – это риски, влекущие за собой возможность улучшить продукт, сократить сроки работ, снизить их стоимость, повысить качество.

Таким образом, риск-менеджмент приобретает все большее значение и признание в бизнесе, а соответственно, роль специалистов проектного и риск-менеджмента в стратегическом управлении неуклонно растет, потому что трудно найти универсальные решения – они будут зависеть от размера и специфики проекта и компетенций сотрудников.

Учебное пособие подготовлено с учетом требований профстандарта 08.018 «Специалист по управлению рисками», утвержденному приказом Министерства труда и социальной защиты РФ от 30 августа 2018 года N 564н [2].

Согласно данному стандарту основной целью профессиональной деятельности является: формирование стратегической интегрированной системы управления рисками, поддержание уровня рисков, обеспечивающего непрерывную экономически безопасную деятельность и устойчивое развитие организации, социально-экономических систем и процессов на различных уровнях управления.

Для уровня квалификации 6 (Высшее образование – бакалавриат и дополнительное профессиональное образование – программы повышения квалификации или Высшее образование (непрофильное) – бакалавриат и дополнительное профессиональное образование – программы профессиональной переподготовки в области управления рисками или в функциональных областях деятельности организации и программы повышения квалификации) определена одна обобщенная трудовая функция:

В – Разработка отдельных функциональных направлений управления рисками, для нее устанавливаются трудовые функции:

- выработка мероприятий по воздействию на риск в разрезе отдельных видов и их экономическая оценка;

- документирование процесса управления рисками и корректировка реестров рисков в рамках отдельных бизнес-процессов и функциональных направлений;

- оказание методической помощи и поддержка процесса управления рисками для ответственных за риск сотрудников организации - владельцев риска;

- разработка методической и нормативной базы системы управления рисками и принципов управления рисками в рамках отдельных бизнес-процессов и функциональных направлений.

Для уровня квалификации 7 (Высшее образование – магистратура или специалитет и дополнительное профессиональное образование – программы повышения квалификации или Высшее образование (не-профессиональное) – магистратура или специалитет и дополнительное профессиональное образование – программы профессиональной переподготовки в области управления рисками или в функциональных областях деятельности организации и программы повышения квалификации) определены две обобщенные трудовые функции:

- С – построение интегрированной системы управления рисками;
- D – методическое обеспечение, поддержание и координация процесса управления рисками.

Для обобщенной трудовой функции С устанавливаются следующие трудовые функции:

- планирование, координаирование и нормативное обеспечение интегрированной комплексной деятельности подразделений по управлению рисками в соответствии со стратегическими целями организации;
- поддержание эффективных коммуникаций в сфере управления рисками и мотивация сотрудников подразделений;
- контроль эффективности работы сотрудников и подразделений в сфере управления рисками;
- разработка интегрированной системы управления рисками;
- внедрение интегрированной системы управления рисками;
- эксплуатация интегрированной системы управления рисками;
- поддержание устойчивого функционирования интегрированной системы управления рисками;
- разработка совместных предложений по результатам мониторинга эффективности управления рисками со всеми участниками процесса управления рисками и консультирование сотрудников по вопросам повышения эффективности управления рисками.

Для обобщенной трудовой функции Д устанавливаются следующие трудовые функции:

- формирование методологических основ интегральной системы управления рисками, формирование основных принципов разработки локальных нормативных актов по управлению рисками на уровне крупных организаций и подразделений;
- разработка стандартов организации, методических и нормативных документов в сфере обеспечения функционирования и координации процесса управления рисками;
- консультирование по вопросам управления рисками в организации;
- взаимодействие с заинтересованными сторонами по вопросам управления рисками и публичное представление организации в средствах массовой информации в вопросах риск-менеджмента, обеспечение открытой информации о системе управления рисками
- поддержание и совершенствование культуры управления рисками в организации.

Профессиональный стандарт представляет собой многофункциональный документ, описывающий цель и содержание профессиональной деятельности через обобщенные трудовые функции и действия, место в системе уровней квалификации, образование и обучение работника, знания, умения и опыт его практической работы. Профессиональные стандарты позволяют: сотрудникам оценивать свой профессиональный уровень и повышать квалификацию, планировать дальнейший профессиональный и карьерный рост; руководству организации проводить оценку соискателей при найме и действующих сотрудников, разрабатывать программы переподготовки, аттестации, планирования кадрового резерва; образовательным учреждениям разрабатывать образовательные стандарты, учебные программы и курсы дисциплин, учитывающие требования работодателя к выпускникам. Далее представлены требования к знаниям для двух квалификационных уровней в области управления рисками.

В результате освоения дисциплины для уровня квалификации 6 обучающийся должен знать:

Базовые положения международных стандартов по риск-менеджменту и смежным вопросам
Виды, методы, формы и инструменты внутреннего контроля
Возможности инструментов риск-менеджмента для анализа рисков организаций
Законодательство Российской Федерации и отраслевые стандарты по управлению рисками
Инструменты анализа существующих методов контроля рисков и управления рисками и их достаточности; инструменты анализа последствий рисков
Информационная политика организации
Классификация рисков организации
Критерии, применяемые при выработке мероприятий по воздействию на риски в разрезе отдельных видов
Локальные нормативные акты по управлению рисками в организации (политики, процедуры, регламенты, методики оценки рисков)
Локальные нормативные акты по управлению рисками в организации и системы управления рисками
Методология проведения социологического исследования
Методы воздействия на риск
Методы воздействия на риски в разрезе отдельных их видов
Методы и инструменты, применяемые для предупреждения рисков несоответствия законодательству Российской Федерации и регуляторным требованиям
Методы, техники, технологии управления различными видами риска
Нормы корпоративного управления и корпоративной культуры
Нормы профессиональной этики
Нормы этики организации
План мероприятий по управлению рисками
Принципы и правила выбора метода, техники оценки риска (достаточность ресурсов, характер и степень неопределенности, сложность метода, техники)
Принципы построения реестра рисков, карты рисков
Реестр рисков, карта рисков, планы мероприятий и контрольные процедуры по рискам
Требования к обеспечению сохранения коммерческой тайны

В результате освоения дисциплины для уровня квалификации 7 обучающийся должен знать:

Базовые концепции теории корпоративных финансов
Внешний и внутренний контекст процесса управления рисками
Внутренний и внешний контекст функционирования организации
Должностные инструкции работников подразделения
Законодательство Российской Федерации и отраслевые стандарты по управлению рисками
Информационная политика организации
Ключевые показатели эффективности деятельности организации
Компоненты системы управления рисками и их взаимосвязь
Локальные нормативные акты организации по управлению рисками
Локальные нормативные акты организации, определяющие политику взаимодействия со средствами массовой информации и связей с общественностью
Локальные нормативные акты по управлению рисками в организации
Локальные нормативные акты, определяющие нормы профессиональной этики, нормы корпоративного управления и корпоративной культуры
Международные и национальные стандарты обеспечения социальной ответственности и регулирования вопросов устойчивого развития
Международные и национальные стандарты по управлению рисками
Международные и национальные стандарты по управлению рисками в части, касающейся создания культуры управления рисками
Методика выбора варианта или метода воздействия на риск; методы подготовки и внедрения планов воздействия на риск
Методики и лучшие практики определения ключевых индикаторов риска
Методики, лучшие практики, оценки и исследования предельно допустимого уровня риска
Методы и процедуры контроля деятельности работников и подразделения
Методы и процедуры совершенствования системы управления рисками
Методы и современные технологии подбора и управления работниками в организации
Методы и технологии обмена профессиональным опытом внутри подразделения
Методы идентификации, оценки и управления рисками и возможности их применения
Методы мониторинга и оценки качества риск-менеджмента на основе системы индикаторов и их динамики
Методы оценки и управления рисками и возможности их применения в организации

Методы, методологии оценки культуры управления рисками в разных организациях, лучшие практики оценки культуры управления рисками
Методы, технологии, инструменты совершенствования контроля деятельности работников и подразделения
Национальные и международные стандарты, лучшие практики интегрированного управления рисками
Национальные и международные стандарты, лучшие практики по обеспечению социальной ответственности и регулированию вопросов устойчивого развития
Национальные и международные стандарты, лучшие практики по построению систем управления рисками
Нормы корпоративного управления и корпоративной культуры
Нормы профессиональной этики
Нормы этики организации
План работ подразделения и планы работ работников подразделения
Полномочия и обязательства менеджмента по реализации плана управления рисками
Положения законодательства Российской Федерации, национальных и международных стандартов, руководств и лучших практик по управлению рисками, управлению непрерывностью бизнеса и в чрезвычайных ситуациях
Понятия, методы и инструменты количественного и качественного анализа рисков
Принципы внедрения процесса управления рисками
Принципы внедрения системы управления рисками
Принципы делового общения, принципы и методы организации деловых коммуникаций
Принципы и концепции теории корпоративной социальной ответственности
Принципы и методы обеспечения устойчивого развития организации и социальной ответственности
Принципы и методы создания мотивационных схем и кадрового резерва
Принципы и методы управления проектами
Принципы построения карты рисков, ее назначение и методы анализа
Принципы теории управления изменениями
Принципы управления в чрезвычайных и кризисных ситуациях, а также управления непрерывностью бизнеса
Принципы целеполагания, организационного планирования и прогнозирования
Принципы, методы и технологии обучения

Принципы, методы, технологии и инструменты оценки знаний, умений и личностных качеств работников
Принципы, методы, технологии и инструменты оценки потребностей в развитии и обучении работников
Процесс управления в чрезвычайных и кризисных ситуациях, а также управления непрерывностью бизнеса
Результаты современных исследований по проблемам управления рисками в Российской Федерации и мире
Современные инструменты управления человеческими ресурсами
Современные информационные системы и технологии управления рисками и возможности их применения в организации
Современные информационные системы и технологии управления рисками и возможности их применения
Современные информационные технологии и программные продукты для управления рисками
Современные методы и методики проведения исследований
Современные методы и приемы психологии управления
Современные принципы построения организационной культуры
Способы оценки эффективности процесса управления рисками
Стратегии, методы управления рисками и варианты их применения
Стратегические и оперативные цели и задачи системы управления рисками в организации
Стратегия организации по управлению рисками
Сущность и методы управления проектами
Сущность и элементы процесса стратегического и оперативного планирования
Сущность и принципы теории и концепции взаимодействия людей в подразделении, вопросы управления человеческим капиталом, мотивации, групповой динамики, командообразования, коммуникаций и управления конфликтами
Теория управления изменениями
Требования к обеспечению сохранения коммерческой тайны
Элементы методологии управления рисками
Элементы системы управления рисками и их взаимосвязь
Этапы разработки систем управления рисками

ТЕМА 1

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ ПО УПРАВЛЕНИЮ РИСКАМИ

В соответствии с Федеральным законом Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» риск – это вероятность причинения вреда жизни или здоровью граждан, имуществу физических или юридических лиц, государственному или муниципальному имуществу, окружающей среде, жизни или здоровью животных и растений с учетом тяжести этого вреда [3].

Риск является следствием влияния неопределенности на достижение поставленных целей. Неопределенность – это состояние полного или частичного отсутствия информации, необходимой для понимания события, его последствий и их вероятностей. Следствием влияния неопределенности на цели может быть отклонение от ожидаемого результата или события (позитивное и/или негативное).

Цели могут различаться по содержанию (в области экономики, здоровья, экологии, ...) и назначению (стратегические, общеорганизационные, относящиеся к разработке проекта, конкретной продукции и процессу, ...).

Риск можно охарактеризовать путем описания возможного события и его последствий или их сочетания, а также в виде последствий возможного события (включая изменения обстоятельств) и соответствующей вероятности.

Вероятность – мера возможности появления события, выражаемая действительным числом из интервала от 0 до 1. где 0 соответствует невозможному, а 1 – достоверному событию.

События характеризуются возможностью и частотой появления. В качестве характеристики возможности появления события, которая может быть определенной или неопределенной, измеримой или неизмеримой, объективной или субъективной, иметь качественную или количественную оценку и может быть выражена математически как вероятность или частота за установленный период времени применяют термин «правдоподобность».

Правдоподобность появления события – это характеристика возможности и частоты появления события. Частота – это количество событий или их последствий за определенный период времени. Частота может быть применима к прошлым событиям или возможным будущим событиям, тогда частоту можно рассматривать как меру правдоподобности вероятности события.

Инструментом классификации и представления риска путем ранжирования последствий и правдоподобности/вероятности является матрица риска. Уровень риска оценивается как мера риска или комбинации нескольких видов риска, характеризуемая последствиями и их правдоподобностью/вероятностью.

Полностью исключить все риски невозможно, поэтому необходимо умело управлять ими. Для организации и реализации мер по управлению рисками, а также мониторинга их текущего статуса назначается так называемый владелец риска – лицо или организация, имеющие ответственность и полномочия по менеджменту риска.

Под процессом менеджмента риска понимают действия, которые обеспечивают реализацию принципов и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге, анализе и постоянном улучшении менеджмента риска организации. Принципы отражают политику, цели, полномочия и обязательства в области менеджмента риска. Организационные меры включают планы, взаимоотношения, подотчетность, ресурсы, процессы и действия.

Эти действия представляют следующие взаимосвязанные элементы, которые составляют структуру менеджмента риска:

- обмен информацией и консультации,
- установление целей и области применения,
- идентификация рисков,
- исследование,
- оценка,
- обработка,
- мониторинг и анализ риска.

Обмен информацией и консультации – это непрерывные итеративные процессы, выполняемые организацией для обеспечения, распространения или получения информации и участия в диалоге с причастными сторонами по вопросам, относящимся к менеджменту риска.

Информация может относиться к существованию, природе, форме, правдоподобности, уровню, оценке, приемлемости, обработке или другим аспектам риска и менеджменту риска.

Консультации как двухсторонний процесс обмена информацией между организацией и ее причастными сторонами по проблеме проводят до принятия решения или определения действий по этой проблеме.

Консультация – это:

- процесс, который способствует принятию решения на основе убеждения, а не под давлением
- процесс, который предшествует процессу принятия решения, но не объединяется с ним.

Причастной стороной считается любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска. Лицо, принимающее решение, также является причастной стороной.

Причастная сторона может иметь собственное представление о риске – восприятие риска, отражающее его потребности, проблемы, знание, доверие и ценности. Поэтому необходимо установить критерии риска – совокупность факторов, по сопоставлению с которыми оценивают значимость риска.

Критерии риска основаны на установленных целях организации, внешней и внутренней области применения организации. Критерии риска формулируются на основе требований стандартов, политики, законодательных и иных требований.

Относительно установления целей и области применения у каждой организации имеются отличительные особенности.

Отличительные особенности включают:

миссию: смысл существования организации
видение: то, какой организация стремится стать
ценности: принципы и/или модели мышления, призванные играть роль в формировании культуры организации и определения того, что важно для организации для поддержки ее миссии и видения
культуру: убеждения, история, этика, соблюдаемые правила поведения и точки зрения, взаимосвязанные с отличительными особенностями организации

Особенно важно, чтобы культура организации была согласована с ее миссией, видением и ценностями. Высшему руководству следует учитывать среду организации при определении ее миссии, видения и ценностей. Это включает в себя понимание существующей культуры и оценку необходимости изменения культуры. Стратегическое направление организации и ее политику следует согласовать с данными отличительными элементами.

Высшему руководству следует пересматривать миссию, видение, ценности и культуру организации через запланированные промежутки времени и при изменении среды организации. При таком пересмотре следует учитывать внешние и внутренние факторы, которые могут влиять на способность организации достигать устойчивого успеха. При внесении изменений в какие-либо из идентифицированных элементов эти изменения следует довести до сведения сотрудников в рамках организации и заинтересованных сторон, если применимо.

Целью менеджмента риска является создание и защита ценностей организации. Менеджмент риска повышает производительность, поощряет инновации и поддерживает достижение целей.

Для установления области применения необходимо определить внешние и внутренние факторы, которые следует учитывать при управлении риском.

Внешняя область применения – это внешние условия, в которых организация работает и достигает своих целей. Внешняя область применения может включать в себя:

- внешнюю среду, связанную с культурной, социальной, политической, законодательной, регулирующей, экономической, природной или конкурентной сферой на международном, национальном, региональном или местном уровне;
- ключевые критерии и тенденции, которые могут воздействовать на достижение установленных целей организации;
- взаимоотношения с внешними причастными сторонами, восприятие ими риска и значимость для организации этих сторон.

Внутренняя область применения – это внутренние условия, в которых организация работает и достигает своих целей. Внутренняя область применения может включать в себя:

- управление, организационную структуру, обязанности и подотчетность;
- политику, цели и задачи, а также стратегию их достижения;
- возможности организации с точки зрения ресурсов и знаний (например, капитал. время, люди, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (формальные и неформальные);
- взаимоотношения с внутренними причастными сторонами, восприятие ими риска и значимость для организации этих причастных сторон;
- культуру организации;
- стандарты, руководящие принципы и модели работы, принятые в организации;
- форму и объем договорных отношений.

Идентификация рисков – это процесс определения, составления перечня и описания элементов риска, которая может включать в себя теоретический анализ, анализ хронологических данных, экспертных оценок и потребностей причастных сторон.

На их основе составляется описание элементов риска в виде структурированного заключения о риске, обычно содержащее описание четырех элементов: источников риска, событий, их причин и возможных последствий.

Источник риска – это объект или деятельность, которые самостоятельно или в комбинации с другими обладают возможностью вызывать повышение риска. Источник риска может быть материальным или нематериальным. Внутренние свойства или слабые места объекта, вызывающие его чувствительность к источнику риска, что может привести к реализации события и его последствий отражает уязвимость объекта.

Событие – это возникновение или изменение специфического набора условий. Событие может быть единичным или многократным, и может иметь несколько причин. Событие может быть определенным или неопределенным. Событие может быть названо терминами «инцидент», «опасное событие» или «несчастный случай». Событие без последствий может также быть названо терминами «угроза возникновения опасного события», «угроза инцидента», «угроза поражения» или «угроза возникновения аварийной ситуации».

Опасность – это источник потенциального вреда, поэтому может быть источником риска.

Причина – это явление, процессы, состояния, вызвавшие возникновение изменений объекта. Понимание причин потенциальных событий и рисков может быть использовано для разработки стратегий предотвращения неблагоприятных последствий или повышения положительных результатов. Часто существует иерархия причин с несколькими уровнями до того, как будет найдена основная причина. Обычно причины анализируются до тех пор, пока действия не будут определены и обоснованы [13].

Последствие – это результат воздействия события на объект. Результатом воздействия события может быть одно или несколько последствий. Первоначальные последствия могут вызвать эскалацию дальнейших последствий по принципу «домино».

Последствия могут быть определенными или неопределенными, могут быть ранжированы от позитивных до негативных. Последствия могут быть выражены качественно или количественно.

Процесс, охватывающий идентификацию рисков, анализ рисков и сравнение рисков называется оценкой риска.

Анализ риска – это процесс изучения природы и характера риска и определения уровня риска. Как правило, анализ риска включает в себя установление причинно-следственных связей опасного события с его источниками и последствиями, включает в себя количественную оценку риска. Анализ риска обеспечивает базу для проведения сравнительной оценки риска и принятия решения об обработке риска.

Сравнительная оценка риска – это процесс сравнения результатов анализа риска с критериями риска для определения приемлемости риска. Отношение организации к оценке риска и, таким образом, к наличию риска, сохранению риска, решениям о его принятии, изменении и устраниении риска выражается в выявлении предпочтительного, допустимого, неприемлемого и принимаемому риску.

Предпочтительный риск – это тип риска и его уровень, к которому организация стремится или готова поддерживать.

Допустимый риск – это риск, который организация и причастные стороны готовы сохранять после обработки риска для достижения своих целей. Допустимость риска связана с законодательными и обязательными требованиями.

Неприятие риска – это отношение к риску, выражаемое в неприемлемости наличия риска.

Принятие риска – обоснованное решение о принятии риска. Решение о принятии риска может быть принято без обработки риска или в процессе обработки риска. Необходимо проводить мониторинг и пересмотр принятого риска.

Обработка риска – это процесс модификации риска, при этом могут возникнуть новые риски и измениться существующие риски.

Обработка риска может включать в себя:

- исключение риска путем принятия решения не начинать или не продолжать деятельность, в процессе или в результате которой может возникнуть опасное событие; решение может быть принято на основе результатов сравнительной оценки риска;

- принятие или повышение риска для обеспечения более широких возможностей:

- устранение источников риска;

- изменение правдоподобности вероятности опасного события;

- изменение последствий опасного события;

- разделение риска с другой стороной или сторонами (путем включения в контракты или финансирования обработки риска) – это форма обработки риска, включающая согласованное распределение риска между несколькими сторонами. Законодательные или обязательные требования могут ограничить, запретить или обязать проведение разделения риска. Разделение риска может представлять собой страхование или иметь форму договора (контракта). Степень, до которой риск зависит от точности и однозначности условий договоров по разделению риска. Перенос риска является формой разделения риска. Финансирование обработки риска – это форма обработки риска, предусматривающая долевое финансирование для сохранения или изменения возникающих финансовых последствий.

- обоснованное решение о сохранении риска. Сохранение риска – это принятие потерь или выгод от достигнутого уровня риска. Сохраняемый уровень риска зависит от критериев риска. Сохранение риска предполагает принятие остаточного риска.

Остаточный риск – это риск, оставшийся после обработки риска, может представлять собой неопределенный риск. Остаточный риск иногда называют сохраняемым риском.

Профиль риска – это набор сведений о всех видах риска, который может содержать информацию о риске для организации в целом, ее частей и другую информацию.

Мониторинг – это систематические проверки, надзор, обследования и определение состояния, проводимые для идентификации изменений требуемого или ожидаемого уровня функционирования. Мониторингу могут быть подвергнуты структура и процесс менеджмента риска, риск и управление риском.

Пересмотр – деятельность, предпринимаемая для анализа пригодности, адекватности, результативности рассматриваемого объекта по отношению к достижению установленных целей. Может быть проведен анализ структуры менеджмента риска, процесса менеджмента риска, риска и управления риском.

Отчетность о риске – это форма обмена информацией о риске, предусматривающая информирование соответствующих внутренних и внешних причастных сторон путем предоставления информации о текущем состоянии риска и менеджменте риска.

Реестр риска – форма записи информации об идентифицированном риске. Термин «журнал риска» иногда используют вместо термина «реестр риска».

Аудит менеджмента риска – систематический, независимый, документированный процесс получения свидетельств и оценки их объективности для установления степени адекватности и эффективности структуры менеджмента риска или ее части.

Риск может возникнуть в любой сфере деятельности, будь то бизнес, производство, наука или другое направление. Он может негативно сказаться на качестве выполнения работ, соблюдении сроков и бюджета проекта, а также на репутации компании. Способность организации к адаптации в сложной и изменчивой окружающей среде характеризует устойчивость организации.

Степень подверженности организации и/или причастных сторон воздействию события называют экспозицией. Определяя экспозицию менеджмент рисков позволяет определить потенциальные риски, предсказать вероятность их появления и вероятные последствия. Благодаря этому разрабатывают стратегии по минимизации негативного влияния.

В результате компании, инвесторы, государственные органы и другие заинтересованные стороны имеют возможность максимально снизить риск потерь и опасных последствий, увеличить эффективность и поддерживать высокий уровень конкурентоспособности [4].

Все действия должны выполняться в соответствии с политикой, процедурами и методами менеджмента организации. Таким образом, менеджмент риска – это скоординированные действия по руководству и управлению организацией в области риска. Структура менеджмента риска должна быть интегрирована в общую стратегию, политику и практическую деятельность организации.

Стратегия – это образ организационных действий и управляющих подходов, используемых для достижения организационных задач и целей организации в исходной ситуации с помощью имеющихся ресурсов и с учетом возможных действий конкурентов. Стратегия организации – набор документально оформленных правил для принятия решений, которыми организация руководствуется в своей деятельности [5].

Одним из таких документов является политика в области менеджмента риска – заявление высшего руководства об общих намерениях, руководящих принципах и направлениях деятельности организации в области менеджмента риска.

На основе политики составляется план менеджмента риска – краткое, схематичное описание деятельности и мероприятий в пределах структуры менеджмента риска, устанавливающих подход, элементы менеджмента и ресурсы, применяемые для менеджмента риска.

План менеджмента риска может быть применен к конкретной продукции, процессу и проекту, к части или всей организации. Элементы менеджмента риска обычно включают в себя процедуры, методы, распределение ответственности, последовательность действий и сроки их исполнения [6].

ТЕМА 2

ПРИНЦИПЫ МЕНЕДЖМЕНТА РИСКА ПРОЕКТА

Для того чтобы менеджмент риска проекта был эффективным, организация должна на всех уровнях выполнять принципы:

Менеджмент риска должен

- создать и защитить ценности организации;
- являться неотъемлемой частью всех процессов организации, связанных с проектом;
- являться частью процесса принятия решений, так что все решения должны учитывать риск;
- учитывать неопределенность имеющейся информации;
- быть систематическим, структурированным и своевременным;
- основываться на наилучшей доступной информации;
- быть адаптируемым;
- учитывать человеческие и культурные факторы;
- обеспечивать прозрачность процессов;
- учитывать интересы заинтересованных сторон;
- быть динамичным, итеративным и реагирующим на изменения;
- способствовать постоянному улучшению деятельности [7].

Следует различать ценность с точки зрения потребителей, которая для них отождествляется, не со стоимостью или ценой, а с пользой, выгодой, удовлетворенностью потребностью, получаемыми потребителем. Ценность с точки зрения потребителей может быть ниже или выше цены, оплаченной им стоимости приобретенного предмета.

Ценность может быть выражена через полезность, и ценности организационные, установленные и сформулированные для организации, ее собственников, менеджеров и работников

Клиентоориентированность (в том числе гибкость, адаптивность) является необходимым условием существования и устойчивого успеха организации. Организация должна своевременно выявлять изменения потребностей с целью повышения удовлетворенности потребителей, создания ценности, за которую готов платить потребитель.

Основными организационными ценностями являются:

- безопасность, которую рассматривают с точки зрения персонала, продукции, процессов организации; жизнь и здоровье работников компании, потребителей воспринимается как приоритетная ценность;

- сокращение потерь, которое следует рассматривать как необходимое условие конкурентоспособности. Выявление потерь и их устранение возможны в том случае, если в эту деятельность вовлечен весь персонал. Руководству организации следует формулировать установку, согласно которой потери являются опасными для ведения бизнеса, поэтому их сокращение воспринимается работниками как насущная необходимость для стабильного существования организации;

- время – это основной невоспроизводимый ресурс организации. Избыточное время, затрачиваемое на выполнение работ, оборачивается потерями, уменьшая способность организации реагировать на изменение требований и предпочтений потребителей.

- уважение к человеку. Человеческий ресурс рассматривается как основной источник создания ценности для потребителя. Никакая технология не может обеспечить успех у потребителя – это делают люди, используя технологии, которые вносят существенный вклад как в обеспечение соответствия процессов, так и в их улучшение. Организация затрачивает огромные средства на подготовку квалифицированных работников. В организации должна быть атмосфера, в которой работники получают признание своей компетенции, достижений и успехов.

Ценностями также могут быть идеалы, нормы, запреты и табу, четко сформулированные сообразно духу и уставу организации.

Ценности в виде норм должны формулироваться в положениях этических, нравственных и иных кодексов, которые устанавливают желательные стандарты поведения работников (например, публичное признание достижений работника является примером нормы, реализующей ценность "уважение к человеку").

Запреты – это установление ограничений, не допускающих нежелательного поведения работников (например, "не принимай, не делай, не передавай "брак").

Табу – это ограничения, нарушение которых несовместимо с работой в организации (например, сознательное нарушение запретов, воровство, сокрытие и/или осознанное искажение информации).

Одни и те же положения и формулировки могут отражать как ценности, так и принципы, принятые в организации. Основное различие ценностей и принципов - в их направленности.

Ценности – то, что необходимо разделять и использовать для целей самоуправления и самоорганизации как основа самоорганизации работников. Принципы – то, что определяет подходы к построению систем менеджмента или организационных структур управления.

Например, ориентация на потребителя является и ценностью, и одновременно организационно-управленческим принципом. Как ценность, ориентация на потребителя означает, что любой работник должен смотреть на результаты своей деятельности глазами потребителя. Как принцип, ориентация на потребителя означает, что следует выстроить цепочку процессов, реализующую требования потребителей через формирование и выполнение технических требований к входам и выходам всех процессов организации [8].

Менеджмент риска не является обособленной деятельностью, не связанной с основной деятельностью и процессами в организации. Менеджмент риска включает часть обязательств руководства и является неотъемлемой частью всех процессов организации, включая стратегическое планирование, инвестиционное планирование и все процессы управления проектами и изменениями.

Менеджмент риска помогает ответственным лицам принимать обоснованные решения на каждой стадии жизненного цикла проекта, определять приоритетность действий и проводить различия между альтернативными направлениями действий. Это означает, что все решения должны учитывать риск.

Всем менеджерам следует учитывать неопределенность исходной информации, ее особенности и способы использования, особенно в критических процессах.

Систематический, регулярный и структурированный подход к менеджменту риска способствует последовательности, сопоставимости и достоверности проектных решений, управления процессами и прибыли проекта. Надежную хорошо обоснованную структуру менеджмента риска следует применять с начала проекта.

Входные данные для менеджмента риска проекта должны быть основаны на таких источниках информации, как инженерно-технический анализ, анализ месторасположения и оборудования, результаты испытаний и отчеты о выполнении работ, дополненные хронологическими данными, предыдущим опытом, обратной связью с заинтересованными сторонами, прогнозами и экспертными оценками. Однако лица, принимающие решения, должны учитывать все ограничения данных или используемых моделей или возможности расхождений мнений экспертов.

Действия менеджмента риска должны соответствовать типу, внешним и внутренним условиям проекта, участвующим в нем организациям, а также уровню неопределенности и сложности проекта. Сложность менеджмента риска зависит от конкретной ситуации.

Менеджмент риска должен учитывать возможности, восприятие и намерения людей и организаций, которые могут способствовать или затруднять достижение целей проекта.

Соответствующее и своевременное вовлечение заинтересованных сторон и лиц, принимающих решения на всех уровнях организации, гарантирует, что менеджмент риска остается приемлемым и соответствует требованиям. Эта вовлеченность обеспечивает представленность заинтересованных сторон и учет их мнения при определении критериев риска.

По мере продвижения и разработки проекта и реализации внешних или внутренних событий, вносят изменения в область применения знания о проекте, проводят мониторинг и анализ риска, выявляют новые риски, виды риска изменяют, другие исключают из рассмотрения.

Действия по менеджменту риска помогают ответственным за принятие решений непрерывно осознавать изменения и реагировать на них. Организация должна разрабатывать и применять стратегии повышения зрелости менеджмента риска проекта одновременно с другими аспектами процессов организации на основе принципов менеджмента риска (рисунок 1)



Рисунок 1 Принципы менеджмента риска

Таким образом, целью менеджмента риска является создание и защита ценностей организации. Менеджмент риска повышает производительность, поощряет инновации и поддерживает достижение целей. Соблюдение принципов позволит организации управлять влиянием неопределенности в отношении достижения целей организации. Принципы устанавливают характеристики эффективного и результативного менеджмента риска, отражают его ценности и объясняют его назначение и цель. Эти принципы являются основой менеджмента риска и должны учитываться при создании структуры и процесса менеджмента риска организации [9].

ТЕМА 3

ИНТЕГРАЦИЯ ПРОЦЕССОВ МЕНЕДЖМЕНТА РИСКА С ПРОЦЕССАМИ МЕНЕДЖМЕНТА ПРОЕКТА

Процессы менеджмента риска должны быть интегрированы с процессами менеджмента проекта путем включения во все методы и процессы менеджмента проекта. Кроме того, процессы менеджмента риска должны быть встроены в более общие организационные процессы, включая разработку политики, стратегическое и бизнес-планирование, анализ и внесение изменений.

Структура управления проектом должна обеспечивать основы и мероприятия, реализующие менеджмент риска на всех стадиях жизненного цикла проекта, всех уровнях организации и для всех вовлеченных организаций. Структура обеспечивает то, что информацию о риске проекта, полученную в соответствии с процессом менеджмента риска, должным образом регистрируют и используют как основу для принятия решений распределения ответственности на всех соответствующих уровнях организации и проекта.

Если методы и процессы менеджмента, существующие в организации, включают элементы менеджмента риска, или если в организации уже существует процесс менеджмента риска проекта для отдельных видов проекта риска или конкретных ситуаций, то их необходимо критически проанализировать на соответствие требованиям ГОСТ Р МЭК 62198-2015 «Национальный стандарт Российской Федерации. Проектный менеджмент. Руководство по применению менеджмента риска при проектировании» для определения их адекватности и результативности.

Стандарт прописывает полномочия и обязательства участников проекта. Обеспечение постоянной результативности менеджмента риска требует четко сформулированных и последовательно выполняемых обязательств по реализации плана управления всеми организациями, участвующими в проекте, включая владельцев и ключевых подрядчиков, а также подробного стратегического планирования на всех уровнях для выполнения этих обязательств.

Руководству организаций владельцев проекта, подрядчикам и основным субподрядчикам или поставщикам следует:

определять и поддерживать общую политику менеджмента риска, относящегося к проекту
гарантировать согласованность культуры организаций-участников и политики менеджмента риска в максимально возможной степени
согласовывать цели менеджмента риска проекта с целями и стратегиями организаций-участников, особенно для владельцев проекта
определять показатели результативности функционирования менеджмента риска проекта и согласовать их с показателями результативности выполнения проекта и организаций-участников
обеспечивать соответствие правовым и обязательным требованиям
установить ответственность и полномочия на соответствующих уровнях организации и в организации в целом
обеспечивать распределение необходимых ресурсов для менеджмента риска проекта
обеспечивать наличие системы поставки ресурсов в нужное место в нужное время
обеспечивать обмен информацией заинтересованными сторонами о выгодах менеджмента риска
обеспечивать постоянное соответствие структуры менеджмента риска при разработке проекта на всех стадиях жизненного цикла

Организации, участвующие в выполнении проекта, должны обеспечивать распределение ответственности, полномочий и наличия соответствующей компетентности в области менеджмента риска на всех стадиях выполнения проекта, включая внедрение и поддержку процесса менеджмента риска и обеспечение адекватности, результативности и эффективности управления.

Этому может способствовать:

идентификация организаций и владельцев отдельных видов риска, ответственных и уполномоченных в области менеджмента риска проекта
определение лиц, ответственных за разработку, внедрение и поддержание структуры менеджмента риска
установление других видов ответственности работников на всех уровнях организации за процесс менеджмента риска
установление критериев функционирования работы внешней и внутренней отчетности и их распространение на риски всех проектов

Задачи менеджмента риска включают:

определение обязанностей в области менеджмента риска по выполнению проекта
создание механизмов обмена информацией внутри проекта и координирование информации о менеджменте риска
определение области применения процесса менеджмента риска
управление действиями по оценке риска и разработка соответствующих отчетов
рекомендация, инициализация, распределение ответственности по мониторингу выполнения деятельности по обработке риска
поиск руководством решений задач менеджмента риска
обмен информацией обо всех проблемах в области менеджмента риска надлежащим и своевременным образом на протяжении всего периода выполнения проекта
обеспечение планами действий в нештатных ситуациях
идентификация и регистрация проблем в области менеджмента риска
мониторинг процесса менеджмента риска и осуществление корректирующих действий при необходимости
создание системы документации для обеспечения прослеживаемости

В большинстве случаев руководитель проекта имеет определенные полномочия и обязательства, включающие и ответственность в области менеджмента риска проекта. Но в зависимости от размера и сложности проекта, задачи менеджмента риска могут быть делегированы другим специалистам.

Полномочия в области менеджмента риска проекта и их связь с другими функциями должны быть определены и документированы. Подотчетность, выходящая за границы организации, должна быть установлена в контрактной документации.

Организации, участвующие в выполнении проекта, должны выделять трудовые ресурсы, необходимые для функционирования менеджмента риска проекта.

Следует определить:

персонал, его навыки, опыт и компетентность
ресурсы, необходимые на каждом этапе процесса менеджмента риска
процессы, методы и поддерживающие системы, используемые в менеджменте риска проекта
документированные процессы и процедуры менеджмента проекта
системы управления информацией и знаниями
программы обучения
определенное в договоре распределение риска между организациями - участниками проекта

Организации, участвующие в проекте, должны установить методы обмена информацией и отчетности о выполнении проекта. Эти методы должны обеспечивать доступность информации, полученной в результате применения менеджмента риска проекта, на соответствующих уровнях и в нужное время для всех участвующих организаций, в том числе на всех стадиях разработки проекта.

В большинстве случаев отчетность по менеджменту риска должна быть объединена с регулярными отчетами в области менеджмента проекта, с использование процессов консультирования с внутренними заинтересованными сторонами [6].

ТЕМА 4

КОНТЕКСТ ФУНКЦИОНИРОВАНИЯ ОРГАНИЗАЦИИИ И ПРОЦЕССА УПРАВЛЕНИЯ РИСКАМИ

Современное общество характеризуется как «общество риска», в котором систематически возникают новые риски, затрудняющие процессы развития и жизнедеятельности индивидов. Социальная среда современного общества характеризуется как рискогенная, то есть способствующая воспроизведству и распространению рисков в обществе. Количество рисков в обществе увеличивается, индивиды находятся в постоянном ожидании.

Существуют два крупных направления при изучении риска:

Реалистический подход – развивался в психологии, экономике и статистике, так что риск определяется в научных и технических терминах, а изучается посредством вычислений вероятности наступления рисковых событий, а также подсчетов последствий от уже произошедших

Социокультурный подход – развивался в философии, культурной антропологии и социологии; включает три основных направления: культурно-символическое; теория «общества риска»; критический подход

Основной причиной возникновения «общества риска» считается глобальное изменение производственных отношений, начавшееся во второй половине XX в. Именно поэтому под риском понимается вероятность физической угрозы, вызываемая в первую очередь технологическими процессами. Хотя производство рисков осуществляется не только на предприятиях, но и во всех сферах жизнедеятельности общества: экономической, политической, социальной, что становится особенностью рисков модернизации.

Риски начинают угрожать не только жизни отдельного индивида, но и всему обществу в целом. Переход от риска к безопасности возможен только с увеличением количества информации о ситуации для возможности принятия единственного свободного от риска решения.

Но этот переход затруднен тем, что риски модернизации практически невозможно определить на уровне простого восприятия, поскольку часто они отображаются только в формулах. В связи с невидимостью рисков особую роль в современном обществе занимает наука, поскольку лишь она способна обнаружить новые формы риска, поэтому особый статус и определенную власть получают специалисты, ответственные за определение рисков.

При этом не только действие, но и отказ от принятия решений может привести к возникновению рисков. Действие вызывает риски, так как посредством модернизации усложнились технические средства и системы жизнедеятельности человека, что сделало общество более уязвимым. В обществе риска увеличивается количество внутренних рисков, связанных с ошибками человека. Бездействие же возникает потому, что, не устранив последствия одного риска, общество получает новый, иногда гораздо более существенный и сложный [10].

До начала разработки и внедрения структуры менеджмента риска важно проанализировать внешние и внутренние области применения проекта, которые могут существенно повлиять на структуру.

Анализ внешней области применения проекта может включать:

социальные и культурные особенности
правовые, финансовые, технологические, экономические требования
природные и рыночные условия
требования, установленные на международном, национальном, региональном и местном уровнях
основные движущие силы и направления, воздействующие на цели организации или выполнение проекта
взаимосвязи с внешними заинтересованными сторонами, их ценностями и восприятием

Анализ внутренней области применения проекта включает:

цель и задачи проекта и способы их согласования с целями и задачами владельца проекта и пользователями активов, продукции или услуг, созданных проектом
управление, организационную структуру, функции и обязанности для выполнения проекта
политику, цели и стратегии, необходимые для достижения целей
возможности организаций, связанных с проектом, включая доступность и возможности их ресурсов и знаний (например, капитал, время, персонал, процессы, системы и технологии)
информационные системы, потоки информации и процессы принятия решений (как формальные, так и неформальные), и особенно информационные системы, используемые для поддержки менеджмента проекта, его контроля и разработки отчетов
взаимосвязи с внутренними заинтересованными сторонами, их ценностями и восприятием
стандарты, руководства и модели, принятые организацией для выполнения проекта
форму и содержание контрактных отношений между партнерами

Указанные аспекты анализа внешней и внутренней областей применения проекта при необходимости могут быть дополнены. На основе результатов анализа контекста организации формулируется политика в области менеджмента риска проекта, которая должна устанавливать цели и обязательства организации в области менеджмента риска для всех значимых организаций, связанных с проектом.

Политика менеджмента риска для конкретного проекта может быть частью более широкого набора политик организации. Не зависимо от аспекта политики они должны быть применяемыми. Это означает то, что политики должны быть согласованы с условиями среды организации и стратегическими целями.

Политика, как правило, включает:

обоснование потребности организации в менеджменте риска
взаимосвязь целей и политики организации с политикой менеджмента риска проекта
обязательства и ответственность в отношении менеджмента риска проекта для всех вовлеченных организаций
способы разрешения конфликтов интересов
обязательства по обеспечению доступности необходимых ресурсов для подотчетных и ответственных за менеджмент риска
способы определения значений параметров, которыми будут изменяться и отчитываться об эффективности функционирования менеджмента риска проекта и его связь с выполнением проекта в целом, а также соответствующей отчетности
обязательство регулярного пересмотра и улучшения политики и структуры менеджмента риска проекта, а также в случае реализации событий или изменений в процессе разработки проекта

Политики применяется в ходе переговоров с потребителями, используется для мотивации коллектива организации на качественную работу, для поддержки ориентации на потребителя во всей организации, взаимодействия с причастными сторонами. Политика в области менеджмента риска должна быть своевременно донесена до заинтересованных сторон [7].

Значимость этого подтверждает Федерация европейских ассоциаций риск менеджеров отмечая, что «любая организация сталкивается с необходимостью предоставления информации о действующей программе управления рисками внешним контрагентам. В настоящее время все большее внимание со стороны внешних контрагентов уделяется политике организации в некоммерческих вопросах, например, взаимодействие с обществом, местным органами управления, занятостью населения, здоровье и охрана окружающей среды» [11].

ТЕМА 5

СТРУКТУРА МЕНЕДЖМЕНТА РИСКА

Структура менеджмента риска предназначена для обеспечения возможности интеграции процесса менеджмента риска в основные направления деятельности и функции (на рисунке 2 представлены компоненты структуры). Эффективность менеджмента риска будет зависеть от степени интеграции в управление организацией, включая процедуры принятия решений. Это требует поддержки со стороны причастных сторон, особенно высшего руководства организации. Организация должна оценить существующую практику и процессы менеджмента риска, выявить существующие недостатки и устраниить их в рамках структуры. Компоненты структуры и их совместная работа должны быть адаптированы к потребностям организации.



Рисунок 2 Компоненты структуры менеджмента риска

Адаптация менеджмента риска основана на понимании организационной структуры и среды, которые различаются в зависимости от цели, задачи, сложности организации.

Адаптация менеджмента риска в организации является динамичным и итеративным процессом, учитывающий потребности и культуру организации. Менеджмент риска должен быть частью, а не отдельным элементом целей организации, ее системы управления, лидерства и приверженности, стратегии, задач и операций.

Руководители высшего звена и надзорные органы, если это применимо, должны обеспечить интеграцию менеджмента риска во все направления деятельности организации, при этом должны демонстрироваться лидерство и приверженность:

адаптации и внедрению всех компонентов структуры
выпуску заявления или политики, которая устанавливает подход, план или порядок действий в отношении менеджмента риска
обеспечению выделения необходимых ресурсов менеджмента риска
установлению полномочий, ответственности и подотчетности на соответствующих уровнях организации

Это позволит организации:

обеспечить соответствие менеджмента риска целям, стратегии и культуре организации
осознавать и придерживаться всех обязательств, включая добровольные обязательства организации
установить уровень и тип риска, который может или не может быть использован для разработки критериев риска, а также гарантий того, что данные критерии будут доведены до организации и ее причастных сторон
демонстрировать ценность менеджмента риска внутри организации и причастным сторонам
поддерживать систематический мониторинг рисков
обеспечить соответствие структуры менеджмента риска среде организации

Надзорные органы ожидают и требуют от организации:

обеспечить анализ рисков при определении целей организации
понимать риски, с которыми сталкивается организация
обеспечить эффективное внедрение и функционирование системы менеджмента риска
убедиться в соответствии такого рода рисков целям организации
обеспечить обмен информацией о рисках и управлении ими

Проектирование и разработка включают:

понимание организации и ее среды
демонстрация приверженности менеджменту риска
определение организационных ролей, полномочий, обязанностей и ответственности
распределение ресурсов
установление механизмов обмена информацией и консультирования

Внедрение включает:

разработку плана, определяющего необходимое время и ресурсы
определение того, где, когда, кем и как различные типы решений принимаются в рамках организации
изменения, при необходимости, процессов принятия решений
обеспечение четкого понимания и практической реализации механизмов управления рисками в рамках организации

Оценка эффективности включает:

периодическую оценку эффективности работы структуры менеджмента риска по отношению к целям, планам реализации, показателям и ожидаемому поведению
определение по-прежнему ли менеджмент риска содействует достижению целей организации

По мере выявления соответствующих недостатков или возможностей для улучшения организации следует разрабатывать планы и задачи и поручать их ответственным за реализацию.

Улучшение включает:

непрерывный мониторинг и обновление структуры управления рисками для реагирования на внешние и внутренние изменения.

постоянное улучшение применимости, адекватности и результативности работы структуры МР, а также способов интеграции процесса МР внутри организации

После внедрения эти улучшения должны способствовать совершенствованию менеджмента риска [9].

Таким образом, функциональная структура риск-менеджмента состоит из исполнительного и координирующего уровней (рисунок 3).

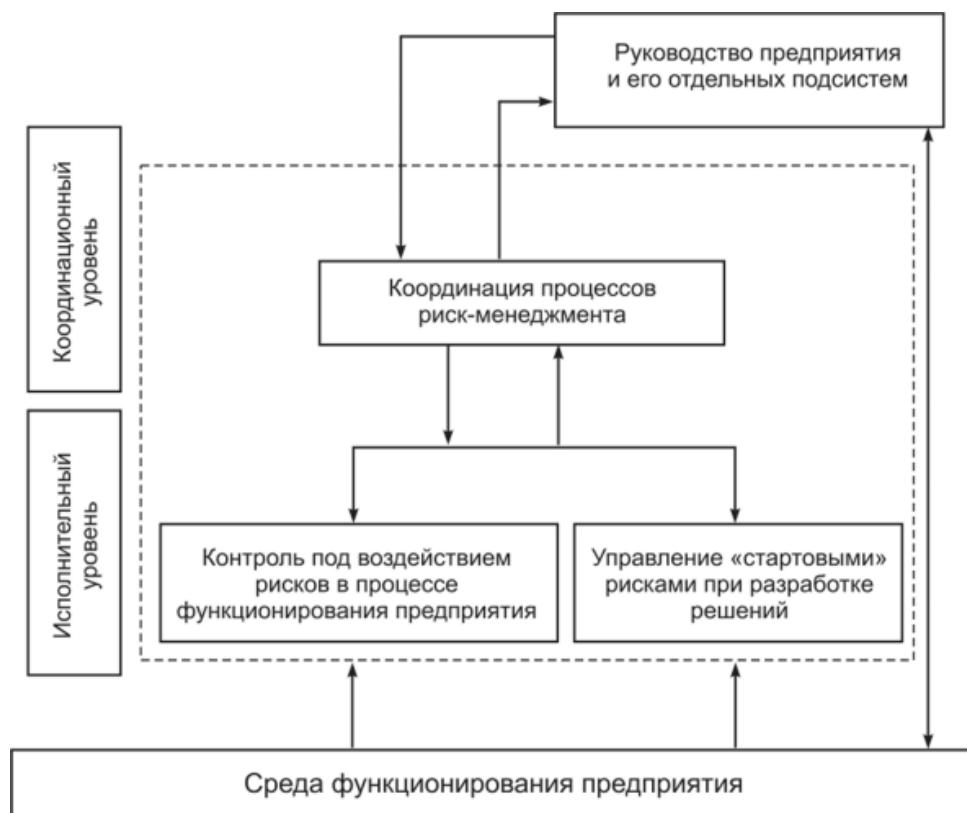


Рисунок 3 Функциональная структура риск-менеджмента

Функциональная структура риск-менеджмента предопределяет алгоритм процесса управления риском, который представляет собой определенную последовательность действий. Причем необходимо учитывать, что алгоритм управления риском должен соответствовать конкретной системе управления предприятием [12].

ТЕМА 6

ПРОЦЕСС МЕНЕДЖМЕНТА РИСКА

Процесс менеджмента риска должен быть неотъемлемой частью управления и принятия решений и интегрирован в структуру, операционную деятельность и процессы организации. Процесс менеджмента риска предполагает систематическое применение политик, процедур и действий по обмену информацией и консультированию, определению среды, а также по оценке, обработке риска, мониторингу, пересмотру, документированию рисков и подготовки отчетности.

Взаимосвязь этих этапов схематично может быть представлена по-разному, например, в ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» (рисунок 3А) акцент делается на процедуры анализа и оценки при информационной поддержке, мониторинге и документировании:

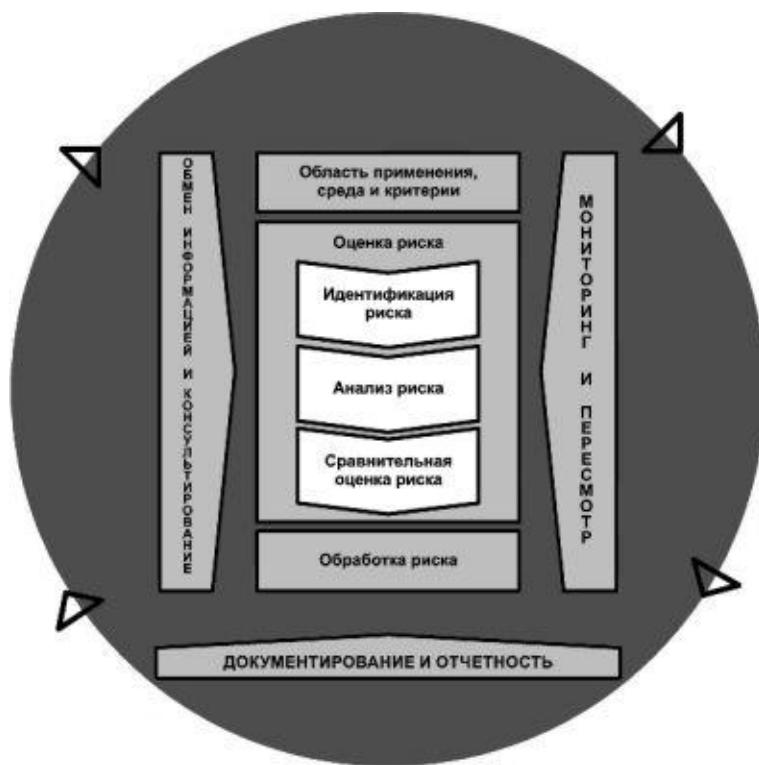


Рисунок 3А Схема процесса менеджмента риска

В ГОСТ Р 52806-2007 «Менеджмент рисков проектов. Общие положения» схема детализирована (рисунок 3Б), и поэтому позволяет более тщательно изучить процесс менеджмента риска проекта:

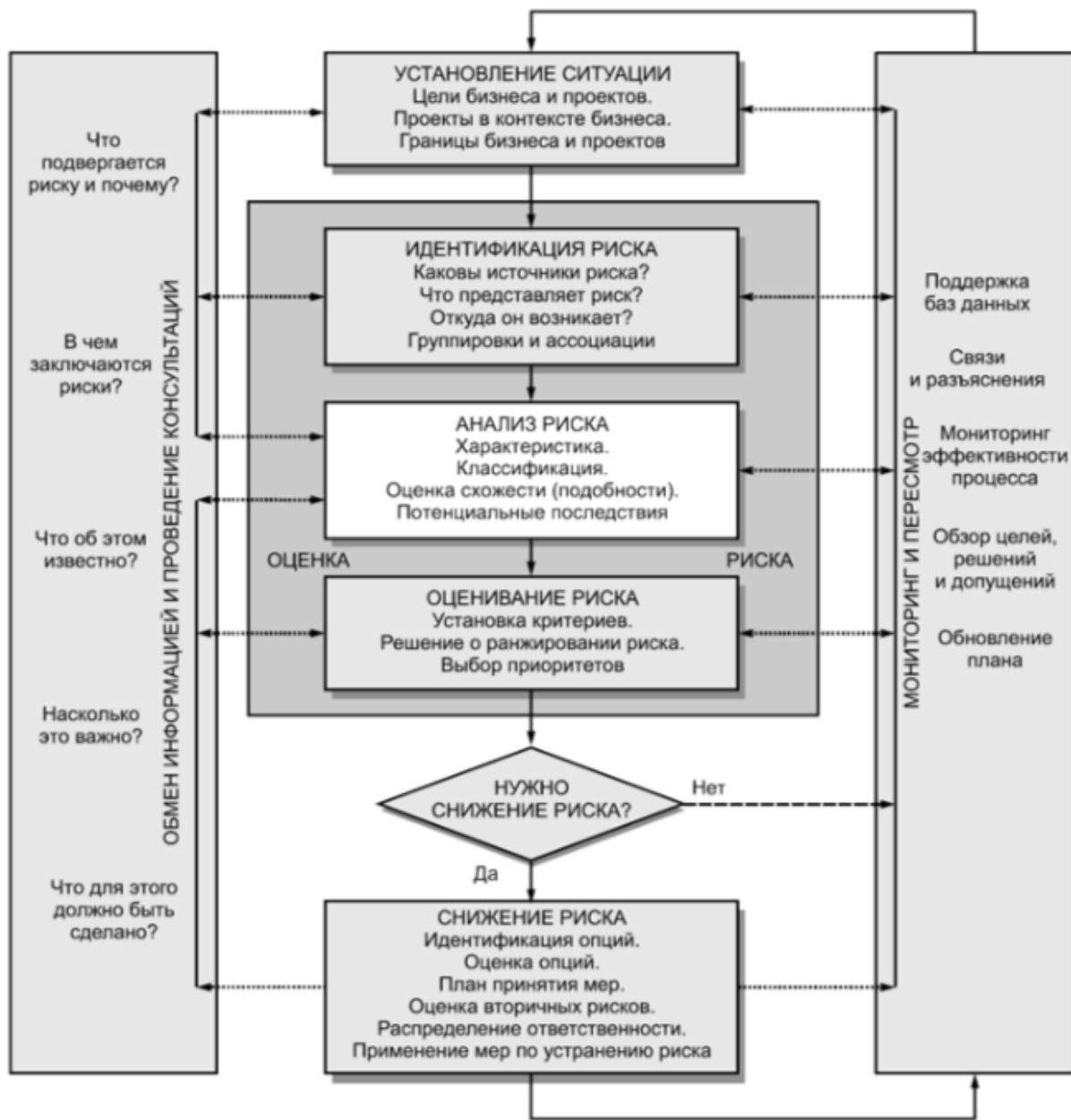


Рисунок 3Б Схема процесса менеджмента риска

Но в схеме, представленной на рисунке 3Б отсутствует важный элемент процесса – документирование, что является значимым упущением. Результаты оценки риска и применяемая методология должны быть задокументированы, также необходимо принять решение о том, какая информация, кому, в какой форме и в каком объеме должна быть сообщена.

Целью документирования является:

передача информации о рисках лицам, принимающим решения, и другим причастным сторонам. включая регулирующие органы
предоставление документальных свидетельств и обоснования принятых решений
сохранение результатов оценки для будущего использования и упоминаний
отслеживание эффективности и тенденций
доступность проверки сделанной оценки
оставить аудиторский след

Из этого следует, что любая документация или записи должны быть в форме, которая может быть понята теми, кто их прочитает, но при этом содержать необходимую техническую глубину для проверки и достаточную детализацию для применения результатов оценки в будущем. Предоставляемая информация должна быть достаточной для того, чтобы можно было проанализировать и подтвердить как сам процесс оценки, так и его результаты. Предположения, ограничения, связанные с исходными данными или методами, а также причины любых сделанных рекомендаций должны быть четко описаны.

Риск должен выражаться в понятных терминах, а единицы, в которых выполняется количественная оценка, должны быть ясными и правильными. Стороны, предоставляющие результаты, должны дать оценку их точности и полноте. Неопределенности должны быть надлежащим образом раскрыты, чтобы не создавалось впечатление, что уровень неопределенности в отчете нереально высокий [13].

Одним из элементов документационного сопровождения процесса менеджмента риска проекта является план менеджмента риска. Внедрение менеджмента риска проекта должно быть основано на выполнении процесса менеджмента риска в соответствии с планом менеджмента риска на всех уровнях организаций-участников как часть их деятельности и процессов менеджмента риска проекта.

План менеджмента риска проекта должен быть разработан на раннем этапе разработки проекта и интегрирован с планом менеджмента проекта, определена область применения процессов менеджмента риска и объем усилий, которые должны быть затрачены на выполнение различных стадий проекта.

Чтобы гарантировать результативность менеджмента риска и продолжение поддержки деятельности, организация должна:

- periodически анализировать критерии функционирования проекта на их приемлемость и соответствие критериям выполнения проекта
- periodически определять выполнение плана менеджмента риска проекта и определять отклонения от него
- periodически анализировать структуру, политику и план менеджмента риска проекта на их адекватность в соответствии с внутренней и внешней областью применения и продвижение разработки проекта
- предоставлять информацию о риске, продвижении выполнения плана менеджмента риска проекта, выполнении политики менеджмента риска проекта, являющейся частью отчетности организации
- анализировать эффективность структуры менеджмента риска проекта

Показатели функционирования менеджмента риска проекта могут быть следующими:

- показатели успешности выполнения проекта, характеризующие степень достижения цели
- показатели, характеризующие степень выполнения менеджмента риска процесса
- показатели, характеризующие результативность обработки риска

Решения по улучшению плана менеджмента риска проекта принимают на основе результатов мониторинга и анализа. Анализ опыта применения менеджмента риска проекта может дать полезную информацию для принятия решений об улучшении.

Важным нюансом в планировании считаются административные риски или риск-культура: неправильное распределение ответственности среди менеджеров компании и специалистами. Заранее определяются роли и полномочия сотрудников в системе менеджмента риска для недопущения пессимистического сценария психологического настроя сотрудников.

Недопонимания и разные интересы, связанные с полномочиями сотрудников, могут вызывать столкновения и снижение эффективности и результативности процесса управления рисками компании. Риск-культура подразумевает уровень осведомленности и вовлеченности в процесс менеджмента риска сотрудников компании [14].

Процесс менеджмента рисков состоит из двух стадий:

1) основное внимание концентрируют на определении масштаба риска, подлежащего менеджменту, и идентификации риска. Эту стадию рассматривают как стадию характеризации проблемы.

2) проводят окончательную оценку и осуществляют снижение риска. Эта стадия аналогична стадии решения проблемы. Однако в процессе решения проблемы могут возникнуть вопросы, требующие возврата к стадии характеризации проблемы.

Жесткого различия между этими стадиями проводить не следует, поскольку менеджмент рисков, как правило, является итеративным процессом, включающим в себя чередование этих стадий. Обе стадии и этапы каждой стадии должны быть соблюдены и выполнены на всех уровнях предприятия, проекта и подпроекта.

Менеджмент риска может применяться на различных уровнях принятия решений: стратегическом, операционном, программном или проектном уровнях [15].

ТЕМА 7

УРОВНИ ПРИНЯТИЯ РЕШЕНИЙ МЕНЕДЖМЕНТА РИСКОВ

Принятие решений целесообразно рассматривать в перспективном (временном) и структурном (организационном) плане. В перспективном плане принятие решений в области менеджмента рисков происходит на трех уровнях – стратегическом, тактическом и рабочем.

В структурном плане принятие решений может рассматриваться на уровнях коммерческой деятельности (бизнес – уровень), проекта и подпроекта. Эти уровни, как правило, соответствуют принятию долгосрочных, среднесрочных и краткосрочных решений.

В ГОСТ Р 52806-2007 «Менеджмент рисков проектов. Общие положения» приводятся примеры принятия решений на уровнях перспективного плана и соответствие принятия решений на уровнях перспективного и структурного плана.

На стратегическом уровне определяют цели, рассматривают вопросы анализа среды и постановки широкомасштабных принципиальных задач, которые необходимы для достижения цели. Процесс принятия решений на стратегическом уровне должен также идентифицировать средства достижения цели и любые ограничения, которые могут сдерживать успешное выполнение работы.

Проводится предварительный анализ риска по предприятию и проекту, рассматривается возможность включения изменений в общую корпоративную политику и задачи предприятия.

Учитывая, что риски, связанные с принятием стратегических решений, не всегда очевидны во время принятия решения и могут существенным образом проявиться только в будущем, стратегические решения необходимо постоянно пересматривать. На этом уровне могут быть приняты решения по изменению ранее поставленных и утверждению новых целей или включению изменений в производственную деятельность или проект для достижения поставленных целей.

Лицами, ответственными за принятие решений на стратегическом уровне могут быть руководитель высшего уровня, представитель владельца или спонсора проекта, менеджер проекта.

Тактическое принятие решений является связующим звеном между процессами принятия решений на стратегическом и рабочем уровнях. На уровне тактического принятия решений осуществляется широкое внедрение решений, принятых на стратегическом уровне.

Определяется политика планирования менеджмента рисков, а также при необходимости анализа рисков, оценки и рассмотрения проблем, связанных с рисками.

Область тактического принятия решений – уже, а временные рамки, финансовая ответственность, область установления целей и проведения политики – более ограничены. Принятие решений на тактическом уровне должно быть ориентировано на среднесрочную перспективу и выбор подхода и методов из предложенных на стратегическом уровне.

Лицами, ответственными за принятие решений на тактическом уровне могут быть руководитель среднего уровня, менеджер проекта, руководитель подпроекта.

Принятие решений на рабочем уровне имеет еще более узкий характер и осуществляется в рамках и пределах, установленных лицами, ответственными за принятие решений на тактическом уровне. Принятие решений на рабочем уровне должно быть более практическим и ориентированным на краткосрочную перспективу.

Разрабатываются бизнес-процессы, выделяются ресурсы, принимаются одни и отклоняются другие решения.

Лицами, ответственными за принятие решений на рабочем уровне могут быть менеджер проекта, группа реализации проекта, поставщики.

Для повышения эффективности при выполнении проектов для целей коммерческой деятельности в рамках предприятия при принятии решений рекомендуется рассматривать коммерческие аспекты деятельности предприятия на различных структурных уровнях.

С этой целью при принятии решений на любом уровне необходимо учитывать риски, возникающие в результате принятия несоответствующих решений на более высоких и более низких уровнях [15].

Важно, что на любом уровне планирования следует учитывать противоречивые функции риска, которые проявляются через право на риск (новаторская функция) и ответственность за риск (дестабилизирующая функция).

Право на риск формулируется как обеспеченная правовыми средствами возможность рискового поведения общего или специального субъекта и выступает признанием позитивного потенциала риска. Несмотря на то, что право на риск предусматривает правомочие бездействия (отказ от риска), основным содержанием права на риск выступает правомочие действия (право на эксперимент).

В последнее время увеличивается число правовых норм, регламентирующих общественные отношения, сопряженные с риском. Разрабатываются и реализуются концепции экологической, экономической, информационной, военной, национальной безопасности.

Постепенное введение рискологической терминологии в действующее законодательство подтверждает обоснованность научной концепции позитивной ответственности. С одной стороны, риск непосредственным образом связан с предположительными негативными последствиями, что всегда предполагает их оценку со стороны рискующего субъекта перед принятием риска, с другой стороны, ответственное отношение к собственному поведению составляет содержание перспективной ответственности.

При привлечении к юридической ответственности за совершение правонарушения, сопряженного с рисковым поведением, оценка риска позволяет определить обоснованность (разумность) поведения субъекта правонарушения. Комплексность оценки определяет причинно-следственные связи между риском и возможными или состоявшимися юридическими последствиями [16].

ТЕМА 8

ЗАКОНОДАТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ И ОТРАСЛЕВЫЕ СТАНДАРТЫ ПО УПРАВЛЕНИЮ РИСКАМИ

Нормативно-правовое обеспечение риск менеджмента в предпринимательской деятельности в нашей стране представлено двумя блоками источников информации:

- нормативно-правовые документы в форме законов, правил, распоряжений, требований регулирующих органов, законодательных и исполнительных органов государственной власти относительно поведения хозяйствующего субъекта
- стандарты риск-менеджмента в виде справочников по терминологии, требований к процедурам, порядкам проведений управленческих процессов, руководствами по идентификации, оценке, анализу рисков и отчетности;

Нормативно-правовая база риск-менеджмента в РФ представлена рядом федеральных законов, различных документов Банка России, регулирующих банковские операции кредитно-финансовых учреждений, а также переводами Международных стандартов финансовой отчетности в части раскрытия информации по рискам и риск-менеджмента (табл. 1). Из содержания табл. 1 видно, что законодательное регулирование риск-менеджмента охватывает преимущественно страховую и банковскую деятельность в стране, а также импортно-экспортные операции и кредитно-финансовую деятельность отечественных компаний за рубежом. Регулирование риск-менеджмента в госучреждениях, также, как и в системе госзакупок отсутствует. Остальной объем документов, регулирующих менеджмент риска в коммерческих компаниях, представлен переводами рекомендованных международных стандартов внутреннего контроля и отчетности МСФО и управления рисками.

Таблица 1

Нормативно-правовая база риск-менеджмента в РФ

Наименование нормативно-правового документа	Содержание документов части регулирования менеджмента риска
Федеральный закон "О техническом регулировании" от 27.12.2002 N 184-ФЗ	Регулирует управление техническими и производственными рисками
Федеральный закон "О финансовой аренде (лизинге)" от 29.10.1998 N 164-ФЗ	Регулирует распределение рисков между сторонами договора лизинга, страхование предпринимательских рисков
Постановление Правительства РФ от 22 ноября 2011 г. N 964 «Об осуществлении страхования экспортных кредитов и инвестиций от предпринимательских и (или) политических рисков, а также осуществлении перестрахования»	Устанавливает правила страхования предпринимательских рисков отечественных организаций, осуществляющих деятельность за рубежом, связанную с экспортом товаров и услуг и инвестиций в иностранные активы за рубежом
Международный стандарт финансовой отчетности (IFRS) 7 "Финансовые инструменты: раскрытие информации", введенный в действие на территории РФ Приказом Минфина РФ от 25.11.2011 № 160н	Устанавливает характеристики раскрытия информации по кредитному, рыночному риску, риску ликвидности и анализу чувствительности предприятий к каждому виду рыночных рисков

В роли субъекта регулирования и стандартизации риск-менеджмента выступает Росстандарт (Федеральное агентство по техническому регулированию и метрологии) как основной официальный источник нормативной базы по управлению рисками [17].

Национальные стандарты общего плана – система стандартов Менеджмент риска, которые могут быть применены при управлении рисками проектов, представлены в таблице 2, с текстами которых можно ознакомиться на сайте Росстандарта.

Таблица 2
Перечень стандартов по менеджменту риска (МР)

Обозначение	Название
ГОСТ Р ИСО 31000-2019	МР. Принципы и руководство
ГОСТ Р 51897-2021	МР. Термины и определения
ГОСТ Р 51901.1-2002	МР. Анализ риска технологических систем
ГОСТ Р 51901.3-2007	МР. Руководство по менеджменту надежности
ГОСТ Р 51901.5-2005	МР. Руководство по применению методов анализа надежности
ГОСТ Р 51901.6-2005	МР. Программа повышения надежности
ГОСТ Р 51901.7-2017	МР. Руководство по внедрению ИСО 31000
ГОСТ Р 51901.16-2017	Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки
ГОСТ Р 51901.21-2012	МР. Реестр риска. Общие положения
ГОСТ Р 51901.22-2012	МР. Реестр риска. Правила построения
ГОСТ Р 51901.23-2012	МР. Реестр риска. Руководство по оценке риска опасных событий для включения в реестр риска
ГОСТ Р 52806-2007	МР проектов. Общие положения
ГОСТ Р 54141-2010	МР. Руководство по применению организационных мер безопасности и оценки рисков. Эталонные сценарии инцидентов
ГОСТ Р 54142-2010	МР. Руководство по применению организационных мер безопасности и оценки рисков. Методология построения универсального дерева событий
ГОСТ Р 54143-2010	МР. Руководство по применению организационных мер безопасности и оценки рисков. Промышленные инциденты
ГОСТ Р 54144-2010	МР. Руководство по применению организационных мер безопасности и оценки рисков. Идентификация инцидентов

Обозначение	Название
ГОСТ Р 54145-2010	МР. Руководство по применению организационных мер безопасности и оценки рисков. Общая методология
ГОСТ Р 55354-2012	Форматы описания и нормирования требований. Система информации о показателях и требованиях к менеджменту рисков
ГОСТ Р 56275-2014	МР. Руководство по надлежащей практике менеджмента рисков проектов
ГОСТ Р 57272.1-2016	МР применения новых технологий. Ч. 1. Общие требования
ГОСТ Р 57272.2-2016	МР применения новых технологий. Ч. 2. Применение к новым технологиям
ГОСТ Р 57272.3-2016	МР применения новых технологий. Ч. 3. Применение к новым материалам и продукции
ГОСТ Р 57272.4-2016	МР применения новых технологий. Ч. 4. Применение к новым производствам и производственным сетям
ГОСТ Р 57272.5-2016	МР применения новых технологий. Ч. 5. Анализ обязательных требований
ГОСТ Р 57272.6-2016	МР применения новых технологий. Ч. 6. Взаимосвязь риска с неопределенностью измерений
ГОСТ Р 57272.7-2016	МР применения новых технологий. Ч. 7. Примеры факторов, влияющих на возникновение риска
ГОСТ Р 58771-2019	МР. Технологии оценки риска.
ГОСТ Р 58969-2020	МР. Управление технико-производственными рисками промышленного предприятия
ГОСТ Р 58970-2020	МР. Количественная оценка влияния рисков на стоимость и сроки инвестиционных проектов
ГОСТ Р МЭК 62198-2015	Проектный менеджмент. Руководство по применению менеджмента риска при проектировании
ГОСТ Р МЭК 62502-2014	МР. Анализ дерева событий
ГОСТ Р 70350-2022	МР. Оценивание качества менеджмента риска организации
ГОСТ Р 71034-2023	МР. Риск-аппетит и ключевые индикаторы риска

ТЕМА 9

БАЗОВЫЕ ПОЛОЖЕНИЯ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ПО РИСК-МЕНЕДЖМЕНТУ И СМЕЖНЫМ ВОПРОСАМ

Кроме стандартов по менеджменту риска общего плана разработаны стандарты риск-менеджмента, например, по безопасности труда; экологическому менеджменту; надежности в технике, а также отраслевые стандарты, например, оценки риска при проектировании зданий и сооружений; медицинских изделий; космических систем; в нефтяной и газовой промышленности.

Но несмотря на возросшую популярность риск-менеджмента в стране, большинство организаций, независимо от их размера и отрасли, нуждаются в более полном понимании всех рисков, с которыми они сталкиваются в своей хозяйственной деятельности. Все хорошо научились уже управлять и страховаться от имущественных и финансовых рисков, но немногие рассматривают риски комплексно как проблему предприятия в целом. Проблема заключается в существовании множества понятий и подходов к риск-менеджменту. Известны как минимум три самостоятельных подхода, имеющие общие цели, но разные способы их достижения: организационный (ЕРМ), предпринимательский и операционный риск-менеджмент. При этом, не существует разделительной линии между риск-менеджментом как отдельной наукой и риск-менеджментом как части общего менеджмента организации.

Чтобы справиться с проблемой всевозрастающей сложности наук о рисках многие страны утверждают множество кодексов, стандартов и других официальных руководств, которые служат своего рода эталоном или «передовым опытом» того, как риск-менеджмент наилучшим образом должен быть построен в организации. Однако недостаток всех этих кодексов и стандартов заключается в отсутствии явных связей между ними, отсутствии источников использованной информации, технических требований и условий их применения и др., что запутывает логику подобных документов.

Задачи стандартизации теории и практики риск-менеджмента заключаются в предоставлении бизнесу общепринятой терминологии управления рисками, целей риск-менеджмента, формализации процесса, которому должен следовать риск-менеджмент на предприятии, и организационной структуры риск-менеджмента.

Наиболее поступательное развитие риск-менеджмента в коммерческой деятельности начиная с 2000-х годов отмечалось в Канаде, Австралии и Новой Зеландии. Стандарт AS/NZS 4360 впервые был разработан в 1995 г. и представлял собой общее руководство по управлению рисками, которое может применяться как в частных предприятиях, так и общественных и муниципальных организациях. Впоследствии он и стал основой первого Международного стандарта ISO 31000 (2009 г.), который на данный момент завоевал общемировое признание, наряду с британским стандартом BS 31100:2008 'Risk management – Code of practice'. Регулирование риск-менеджмента в деятельности госучреждений поддерживается американским стандартом GAO1, британским OCEG Red Book 2.0 (Оранжевая книга Казначейства Великобритании) и канадской политикой «Инфраструктуры риск-менеджмента» CAN/CSA2.

Помимо общепринятых «универсальных» стандартов разработаны стандарты риск-менеджмента (ERM3), ориентированные на частные «коммерческие» предприятия (преимущественно эмитентов ценных бумаг), такие как IRM/AIRMIC4 и COSO5 ERM6.

Стандарт IRM Института риск-менеджмента является одним из самых широко применяемых руководств высокого уровня для специалистов широкого профиля (не риск-менеджеров), он переведен на множество языков, включая русский. Напротив, Австралийский стандарт AS/NZS 4360, ИСО 31000 и COSO предназначены для использования преимущественно специалистами по риск-менеджменту. Все эти стандарты находятся в свободном доступе для загрузки.

Некоторые из доступных стандартов разработаны профессионалами риск-менеджмента, другие – бухгалтерами и аудиторами. Стандарты предлагается, как показано в таблице 3, подразделять на три группы исходя из используемых в них подходов.

Таблица 3

Группы международных стандартов менеджмента риска

Подходы к стандартизации риск-менеджмента предприятий		
Общие принципы и методы управления рисками	Управление рисками в системе внутреннего контроля и аудита	Развитие культуры управления рисками на предприятии
MS ISO 31000 Менеджмент риска	Инфраструктура внутреннего контроля COSO комитета спонсорских организаций (США)	Инфраструктура СоСо Канадского института дипломированных бухгалтеров
BS 31100 Менеджмент риска	Инфраструктура GAO счетной палаты (США)	
Стандарт IRM Международного института риск-менеджмента	Доклад Тернбулла «Руководство для директоров по объединенному кодексу» для листинговых компаний	
ГОСТ Р ИСО 31000 Менеджмент риска	OCEG Red Book 2.0: 2009 (Оранжевая книга Казначейства Великобритании)	

Наиболее развитые и широко применяемые стандарты: IRM, ИСО 31000, BS 31100 и COSO. Они предоставляют описание инфраструктуры менеджмента риска, но первые три больше уклон делают на процесс риск-менеджмента, в то время как COSO не предоставляет очевидного разграничения между инфраструктурой и процессом риск-менеджмента, и преимущественно рассматривает вопросы создания инфраструктуры.

Международный стандарт ИСО 31000 теоретически применим в организациях любой формы собственности (включая госучреждения), размера и отрасли, но, в отличие от национальных аналогов - стандартов внутреннего контроля - не обязывает организации ему следовать.

Стандарт, принятый в более чем 40 странах (в том числе в РФ принят ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство»), рекомендует организациям разрабатывать, применять и непрерывно совершенствовать инфраструктуру, предназначенную для встраивания процесса управления риском в общую систему руководства, стратегического и текущего планирования, управления, отчетности, норм, ценностей и культуры организации.

Стандарт ИСО 31000 предоставляет целостную картину риск-менеджмента с терминами и определениями процессов. Он рассчитан на широкий круг пользователей, включая малый бизнес различных отраслей, и устанавливает ряд принципов, которым должна следовать организация, чтобы повысить эффективность управления рисками, и требований интеграции риск-менеджмента посредством создания инфраструктуры поддержки процесса управления риском.

Среди достоинств стандарта можно выделить логичность описываемой в нем инфраструктуры, последовательность терминологии и широты принятия многими странами.

ИСО 31000 предоставляет возможность предпринимателям применить ряд концепций, соответствующих их целям в достижении коммерческого и конкурентного преимущества, в результате чего добиться его внедрения в хозяйственные процессы и финансовые отношения. В самой общей трактовке предлагается исчерпывающий набор методов, инструментов и приемов оценки риска, не акцентируя внимания на обороты организации, сектор или ее структуру.

Ряд стран (США, Канада, Великобритания) разработали и приняли, наряду с требованиями по внутреннему контролю, собственные стандарты риск-менеджмента, являющиеся частью требований лизинга на их фондовых рынках.

Разработаны и активно применяются международные и национальные стандарты и кодексы риск-менеджмента. Из недостатков многообразия подходов к стандартизации риска-менеджмента можно выделить разобщенность применяемых категорий, классификаций, терминов и определений, применяемых профессионалами в различных странах и различных отраслях их экономик.

Таким образом, можно наметить три основных направления развития нормативно-правового обеспечения риска-менеджмента в РФ:

1) необходимость разработки национального стандарта риска-менеджмента отраслевой направленности, который бы учитывал (и содержал ссылки на) законодательство РФ относительно формирования структуры управления, руководства, финансовой политики, учета и отчетности, а также нормативно-правовые документы, регулирующие отдельные стороны операционной деятельности организаций при осуществлении процессов риска-менеджмента;

2) разработка национального стандарта внутреннего контроля и отчетности (наподобие зарубежных COSO или Руководства Тернбулла), имеющего необходимые ссылки и совместимость с принципами и инструкциями, установленными как в национальном, так и международном стандарте риска-менеджмента;

3) оптимизация национального стандарта к культуре менеджмента, которая сложилась в нашей стране, а не навязывание иностранной, подразумевающей те организационные процессы, которые регулируются законодательством и/или сформированы в правовом поле тех стран, которые участвовали в разработке международного стандарта.

Наличие утвержденного стандарта на предприятии не может заменить необходимых компетенций риск-менеджеров. Успешные организации принимают на работу специалистов риска-менеджмента, которые способны выбрать стандарт, подходящий ему по роду деятельности или сектору экономики, действовать своевременно, учиться на прошлых ошибках и, предвидя будущее, направлять стратегию организации с учетом требований режима коммерческой тайны [17].

ТЕМА 10

ТРЕБОВАНИЯ К ОБЕСПЕЧЕНИЮ СОХРАНЕНИЯ КОММЕРЧЕСКОЙ ТАЙНЫ

Кроме законодательного регулирования риск-менеджмента, большое внимание уделяется вопросам, связанным с установлением, изменением и прекращением режима коммерческой тайны. Разглашение сведений, составляющих коммерческую тайну, меняет ситуацию на рынке товаров, работ, услуг не в пользу потерпевшей стороны. Это может повлечь смену владельцев, банкротство.

Нормативными документами в РФ по вопросам установления и защиты информации, представляющей коммерческую конфиденциальность, считаются 98-ФЗ от 21.07.2004 «О коммерческой тайне», 402-ФЗ от 06.12.2011 «О бухгалтерском учёте». Также права владельца на личную тайную информацию закреплены частично кодексом об административных нарушениях, трудовым, гражданским, уголовным кодексами.

Согласно № 98-ФЗ коммерческая тайна – это режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неправдивых расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Информация, составляющая коммерческую тайну – это сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.

Положения № 98-ФЗ распространяются на информацию, составляющую коммерческую тайну, независимо от вида носителя, на котором она зафиксирована, но не распространяются на сведения, отнесенные в установленном порядке к государственной тайне, в отношении которой применяются положения законодательства Российской Федерации о государственной тайне.

Нарушение № 98-ФЗ влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РФ:

- работник, который в связи с исполнением трудовых обязанностей, получил доступ к информации, составляющей коммерческую тайну, обладателями которой являются работодатель и его контрагенты, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством РФ;

- органы государственной власти, иные государственные органы, органы местного самоуправления, получившие доступ к информации, составляющей коммерческую тайну, несут перед обладателем информации, составляющей коммерческую тайну, гражданско-правовую ответственность за разглашение или незаконное использование этой информации их должностными лицами, государственными или муниципальными служащими указанных органов, которым она стала известна в связи с выполнением ими должностных (служебных) обязанностей;

- невыполнение обладателем информации, составляющей коммерческую тайну, законных требований органов государственной власти, иных государственных органов, органов местного самоуправления о предоставлении им информации, составляющей коммерческую тайну, а равно воспрепятствование получению должностными лицами этих органов указанной информации влечет за собой ответственность в соответствии с законодательством РФ;

- лицо, которое использовало информацию, составляющую коммерческую тайну, и не имело достаточных оснований считать использование данной информации незаконным, в том числе получило доступ к ней в результате случайности или ошибки, не может в соответствии с настоящим Федеральным законом быть привлечено к ответственности;

- по требованию обладателя информации, составляющей коммерческую тайну, лицо, указанное выше, обязано принять меры по охране конфиденциальности информации. При отказе такого лица принять меры, обладатель информации, составляющей коммерческую тайну, вправе требовать в судебном порядке защиты своих прав;

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.

Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания.

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;

2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;

3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;

4) о состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;

5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия или недопустимость ограничения доступа, к которым установлена иными федеральными законами;

12) составляющих информацию о состоянии окружающей среды (экологическую информацию).

Обладатель информации, составляющей коммерческую тайну, имеет право:

- 1) устанавливать, изменять, отменять в письменной форме режим коммерческой тайны в соответствии с настоящим Федеральным законом и гражданско-правовым договором;
- 2) использовать информацию, составляющую коммерческую тайну, для собственных нужд в порядке, не противоречащем законодательству Российской Федерации;
- 3) разрешать или запрещать доступ к информации, составляющей коммерческую тайну, определять порядок и условия доступа к этой информации;
- 4) требовать от юридических лиц, физических лиц, получивших доступ к информации, составляющей коммерческую тайну, органов государственной власти, иных государственных органов, органов местного самоуправления, которым предоставлена информация, составляющая коммерческую тайну, соблюдения обязанностей по охране ее конфиденциальности;
- 5) требовать от лиц, получивших доступ к информации, составляющей коммерческую тайну, в результате действий, совершенных случайно или по ошибке, охраны конфиденциальности этой информации;
- 6) защищать в установленном законом порядке свои права в случае разглашения, незаконного получения или незаконного использования третьими лицами информации, составляющей коммерческую тайну, в том числе требовать возмещения убытков, причиненных в связи с нарушением его прав.

Меры по охране конфиденциальности информации, принимаемые ее обладателем, должны включать в себя:

- 1) определение перечня информации, составляющей коммерческую тайну;
- 2) ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;

3) учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;

4) регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;

5) нанесение на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включение в состав реквизитов документов, содержащих такую информацию, грифа «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства).

Меры по охране конфиденциальности информации признаются разумно достаточными, если:

1) исключается доступ к информации, составляющей коммерческую тайну, любых лиц без согласия ее обладателя;

2) обеспечивается возможность использования информации, составляющей коммерческую тайну, работниками и передачи ее контрагентам без нарушения режима коммерческой тайны.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работодатель обязан:

1) ознакомить под расписку работника, доступ которого к этой информации, обладателями которой являются работодатель и его контрагенты, необходим для исполнения данным работником своих трудовых обязанностей, с перечнем информации, составляющей коммерческую тайну;

2) ознакомить под расписку работника с установленным работодателем режимом коммерческой тайны и с мерами ответственности за его нарушение;

3) создать работнику необходимые условия для соблюдения им установленного работодателем режима коммерческой тайны.

Доступ работника к информации, составляющей коммерческую тайну, осуществляется с его согласия, если это не предусмотрено его трудовыми обязанностями.

В целях охраны конфиденциальности информации, составляющей коммерческую тайну, работник обязан:

1) выполнять установленный работодателем режим коммерческой тайны;

2) не разглашать эту информацию, обладателями которой являются работодатель и его контрагенты, и без их согласия не использовать эту информацию в личных целях в течение всего срока действия режима коммерческой тайны, в том числе после прекращения действия трудового договора;

3) возместить причиненные работодателю убытки, если работник виновен в разглашении информации, составляющей коммерческую тайну и ставшей ему известной в связи с исполнением им трудовых обязанностей;

4) передать работодателю при прекращении или расторжении трудового договора материальные носители информации, имеющиеся в пользовании работника и содержащие информацию, составляющую коммерческую тайну.

Работодатель вправе потребовать возмещения убытков, причиненных ему разглашением информации, составляющей коммерческую тайну, от лица, получившего доступ к этой информации в связи с исполнением трудовых обязанностей, но прекратившего трудовые отношения с работодателем, если эта информация разглашена в течение срока действия режима коммерческой тайны.

Работник имеет право обжаловать в судебном порядке незаконное установление режима коммерческой тайны в отношении информации, к которой он получил доступ в связи с исполнением трудовых обязанностей.

Трудовым договором с руководителем организации должны предусматриваться обязанности по обеспечению охраны конфиденциальности составляющей коммерческую тайну информации, обладателем которой являются организация и ее контрагенты, и ответственность за обеспечение охраны конфиденциальности этой информации.

Причиненные работником или прекратившим трудовые отношения с работодателем лицом убытки не возмещаются, если разглашение информации, составляющей коммерческую тайну, произошло вследствие несоблюдения работодателем мер по обеспечению режима коммерческой тайны, действий третьих лиц или непреодолимой силы.

Руководитель организации возмещает организации убытки, причиненные его виновными действиями в связи с нарушением законодательства Российской Федерации о коммерческой тайне. Размер убытков определяется в соответствии с гражданским законодательством.

Наиболее ценными и требующими неприкословенности считаются данные в ведомостях с техническими, производственными, организационными, экономическими, интеллектуальными материалами, и деятельность компании невозможна при их отсутствии.

Особый статус и важность для бизнеса коммерческой тайны заключаются в том, что без нее проблематично удержать собственные наработки, инструменты, базы клиентов для успешного ведения деятельности в условиях нечестной рыночной конкуренции.

Наибольшую важность и необходимость защиты представляют виды сведений:

- документы по типу лицензий, грантов, тендеров;
- эмпирически подтвержденные и исследованные данные о состоянии окружающей среды, качестве и составе продуктов питания, лекарственных средств, определённых товаров, которые оказывают влияние на человека при контакте;
- внутренняя финансовая документация: численность штата работников, условия оплаты труда, задолженность перед партнерами, расходы на аренду, обслуживание помещений, ремонт;
- сведения о владельцах бизнеса, их долях, доходе, дочерних проектах;

- документация о рентабельности деятельности, ежегодном обороте средств, отчислениях в налоговую службу;
- информация о случаях нарушения действующего законодательства;
- инновационные исследования, собственные технологии, патенты;
- базы контактов с деловыми партнерами, списки участников инвестиционного портфеля компании;
- документы, связанные с закупками, коммерческими предложениями, контрактами.

Примеры обнародования секретной информации:

- прямая продажа в руки потенциальных конкурентов характерна для руководящего персонала, имеющего доступ к секретной информации и намерение действовать в пользу конкурентов;
- открытый доступ к информации, если организация не заботится о сохранности цифровых и документальных материалов, пренебрегает мерами элементарной защиты так, что получить доступ к интересующим данным может любой человек (папка на столе, открытое электронное письмо, программа – становится источником утечки). Такой очевидный способ доступа к собственности компании игнорируется большинством руководителей, особенно если штат сотрудников малый, а служба безопасности отсутствует;
- отсутствие сознательности у работников при наличии особенностей характера (болтливость, общительность, любознательность и желание быть в курсе происходящего) способно привести к ситуации, когда закрытая информация станет достоянием широких масс, даже не преднамеренно работником, который поставлен в известность внутренней ситуации;
- преднамеренное хищение секретных материалов, когда имеет место продуманная и подготовленная схема мошенничества, в которой участвуют работники специально с целью продвижения по карьерной лестнице, чтобы получить права доступа к закрытым коммерческим сведениям, перепродать их или использовать в личных целях;

- немотивированный персонал, когда у сотрудников отсутствует страх за провинность, привлечение к ответственности, что создаёт дополнительные риски информационных утечек. Больше всего страдают организации, где в коллективе присутствуют исполнители, которые считают, что их труд плохо оплачиваем, отсутствуют перспективы карьерного продвижения. Своими незаконными действиями такие лица компенсируют финансовое неблагополучие и чувство удовлетворения от собственной значимости;

- одним из часто встречаемых случаев считается разглашение коммерческой тайны уволенным работником на почве личного конфликта. После расторжения трудового договора обиженный сотрудник может искать финансовой выгоды своим знаниям: незаконное разглашение коммерческой тайны конкурентам за вознаграждение, пользование правами доступа в личных целях, выполнение подлога, мошенничества, мести;

- не исключен вариант, когда в компанию специально внедряют шпиона для сбора определенных сведений с последующей продажей конкурентам.

Каждую из описанных ситуаций в управлении рисками нужно рассматривать отдельно, чтобы найти уязвимые места, посчитать полученный ущерб, принять меры по предупреждению рецидивов.

Для обеспечения защиты и должного уровня безопасности на предприятии проводится комплекс мер, который направлен на исполнение определенных стандартов, правил поведения персонала, контроль деятельности, поиск уязвимостей и улучшение защиты.

Для этого рекомендуется реализовать следующие мероприятия:

- вести в обиход гриф секретности, которым маркируются папки с документами, цифровыми носителями, оборудованием повышенной важности. Также необходимо позаботиться о размещении и хранении носителей информации, они должны находиться в строго отведенных местах: кабинетах, накопителях, архивах, сейфах;

- установить правила обращения и использования конфиденциальных данных: подписать с сотрудниками соглашение о хранении в секрете внутренней информации от третьей стороны; провести инструктаж о мерах безопасности и порядке обращения с ценными для компании информационными ресурсами; озвучить наказание за незаконное разглашение коммерческой тайны;

- создать определенный круг лиц, располагающий повышенными полномочиями и доступом, специально отобранных руководителем и службой безопасности, и прошедший проверку на пригодность. Рекомендуется разделить полномочия и права доступа между этими работниками, чтобы не было единственного человека, обладающего абсолютной властью;

- ведение регулярного мониторинга сотрудников, проведение регулярных проверок персонала на предмет поддержания трудовой дисциплины и инцидентов безопасности, которые позволяют собирать аналитику по поведению работников, их подозрительных действиях, во время пресекать попытки несанкционированного доступа;

Разглашение коммерческой тайны чревато ненужными расходами и рисками для бизнеса, часть из которых способна стать критическими. Разумнее заранее обеспечить условия, препятствующие возникновению происшествий и утечек. Защитные меры пригодятся как малым организациям, так и крупным корпорациям. Расходы на обеспечение превентивных и защитных мер в разы ниже, чем устранение последствий. Только регулярный контроль и предотвращение нежелательных рисков уберегут бизнес от атак конкурентов и внутреннего мошенничества [18].

ТЕМА 11

ИНФОРМАЦИОННАЯ ПОЛИТИКА ОРГАНИЗАЦИИ

Перечень информации, составляющей коммерческую тайну, и иной информации конфиденциального характера, порядок обращения с конфиденциальной информацией, ее предоставления и меры по защите конфиденциальной информации, а также круг лиц, осуществляющих контроль за соблюдением установленного порядка обращения с конфиденциальной информацией, устанавливаются информационной политикой организации.

В широком смысле к информационной политике можно отнести информирование всех сотрудников компании о ее текущем состоянии, поддержание корпоративной лояльности, регламентацию доступа различных сотрудников и подразделений к корпоративной информации (в том числе и представляющей коммерческую тайну), своевременное доведение приказов и распоряжений руководства. Но в том числе под информационной политикой подразумевают и внешнюю информационную работу компании – связи с общественностью, которые осуществляются в рамках строго регламентированной системы [19].

Организации, участвующие в выполнении проекта, должны разработать и применять план обмена информацией с внешними заинтересованными сторонами. Такой план должен включать:

взаимодействие с соответствующими внешними заинтересованными сторонами и обеспечение обмена информацией с ними о проекте
внешнюю отчетность о соответствии правовым, обязательным и другим требованиям
обратную связь и отчетность об обмене информацией и консультациях
обмен информацией для обеспечения доверия к организациям-участникам
обмен информацией с заинтересованными сторонами в критической ситуации или непредвиденных условиях

Информационная политика строится организациями, участвующими в проекте, которая должна обеспечивать полномочия по менеджменту риска в каждой фазе жизненного цикла проекта.

Должны быть установить методы обмена информацией и отчетности о выполнении проекта, которые должны обеспечивать:

- надлежащее представление информации о ключевых элементах структуры менеджмента риска и последующих ее модификациях
- наличие соответствующей внутренней отчетности о структуре, ее эффективности и выходах
- доступность информации, полученной в результате применения менеджмента риска проекта, на соответствующих уровнях и в нужное время для всех участвующих организаций, в том числе на всех стадиях разработки проекта
- использование процессов консультирования с внутренними заинтересованными сторонами

В большинстве случаев методами обмена информацией должен управлять владелец проекта, если не установлены обязательные требования для подрядчиков и поставщиков. Отчетность по менеджменту риска должна быть объединена с регулярными отчетами в области менеджмента проекта [7].

Целями обмена информацией и консультирования являются:

- объединение различных областей знаний для каждого этапа процесса менеджмента риска
- обеспечение учета различных взглядов при определении критериев риска и при оценке риска
- предоставление достаточной информации для облегчения управления риском и принятия решений
- создание чувства вовлеченности и причастности среди лиц, подверженных риску

Таким образом, цели обмена информацией и консультирования оказывают помочь причастным сторонам в понимании риска, предпосылок, на основании которых принимаются решения, и причин, в отношении которых требуются конкретные действия.

Обмен информацией направлен на повышение осведомленности и понимание риска, тогда как консультирование подразумевает получение обратной связи и информации для поддержки процесса принятия решений. Обмен информацией и консультирование с соответствующими внешними и внутренними причастными сторонами должны проводиться на всех этапах процесса менеджмента риска. Тесная взаимосвязь между данными процессами должна способствовать фактическому, своевременному, актуальному, точному и понятному движению информации в организации с учетом конфиденциальности и целостности информации, прав на частную жизнь отдельных лиц [9].

Внешняя информационная работа компаний стала значимой в силу того, что в конце XX века окончательно оформилась идея перехода современных обществ к новой форме их существования – информационному обществу. Изначально это понятие употреблялось для обозначения прогресса технических средств коммуникации и изменения самого процесса коммуникации (большая доступность, массовость и т.д.). С приходом информационного общества информация стала главной движущей силой, а следовательно, повысилась значимость коммуникации.

Зачастую руководители предприятий сосредоточивают свой интерес на функционировании самого предприятия и его доходах, оставляя в стороне вопрос его позиционирования. Однако за счёт грамотно выстроенной информационной политики предприятие способно получить дополнительные бонусы как в виде положительной оценки своей деятельности и положительного контекста своего функционирования, так и более существенные выгоды, влияющие на его прибыль.

Информационная политика, ориентированная на внешний аспект, существует на двух уровнях: на уровне государства и на уровне негосударственных организаций, причём последний опосредованно включен в первый так, что именно государство организует информационное пространство и правила игры в нём.

Для выстраивания эффективной информационной политики предприятия необходимо учитывать все ограничения с позиции законодательства государства. Ключевые способы выстраивания информационной политики являются технологии PR (public relations) – установление связей с обществом и GR (government relations), – установление связей с государственными организациями.

Важность PR для организации связывается с репутационными выгодами. Идеи PR деятельности схожи с эффектами от рекламы, их вниманием к аудитории и опорой на обратную связь, однако существуют некоторые существенные отличия. PR в отличие от рекламы имеет больший спектр применения. Целью рекламы является не просто создание положительного образа объекта, а именно «продажа» этого объекта, в то время как PR создаёт положительный контекст, в котором существует некий объект. Отсюда и разные способы воздействия: PR действует косвенно, может распространяться через взаимо-выгодное партнёрство, тогда как реклама, которая должна побудить к конкретному действию (к покупке), – напрямую.

Информирование предприятием граждан о вакансиях, о том, что происходит на предприятии не только создаёт положительный образ предприятия. Даже если предприятие является техническим или связано с опасными производствами, простое информирование о деятельности убирает страх у граждан.

Таким образом, информационная политика в области связей с общественностью несет в себе репутационные выгоды для предприятия по сравнению с другими конкурентами, уже имеющимися или только планирующими войти в отрасль; должна быть частью корпоративной культуры организации [20].

ТЕМА 12

НОРМЫ КОРПОРАТИВНОГО УПРАВЛЕНИЯ И КОРПОРАТИВНОЙ КУЛЬТУРЫ

Корпоративная культура выступает в качестве философии и базовых ценностей компании, находит отражение в миссии компании, формирует общее видение развития компании. Отражает индивидуальность компании и ее восприятие в общественной среде (репутацию).

Корпоративную культуру можно разделить на:

внешнюю: формальные и неформальные нормы, инструмент управления персоналом, философия компании, модель коммуникации внутри компании, система ценностей, принципов, правил и традиций
внутреннюю: модель формирования имиджа и бренда компании, модель взаимодействия с клиентами, партнерами, контрагентами, СМИ, стратегия позиционирования компании на рынке как работодателя

Корпоративная культура может стать эффективным средством управления персоналом и незаменимым маркетинговым инструментом. Развитая культура формирует имидж компании, является неотъемлемой частью процесса построения бренда

Мировые корпорации привлекают лучших специалистов, чтобы прорабатывать собственную миссию и принципы. Они используют сформулированные постулаты для воздействия на сознание и мотивацию сотрудников. На основании миссии и ценностей компании осуществляется не только набор и увольнение сотрудников, но и выбор коммерческих партнеров. Устанавливаемые корпоративные принципы позволяют сформировать уникальный климат в организации, но существую и общие принципы корпоративной культуры.

В общем смысле к корпоративным принципам относят:

постоянное развитие и совершенствование
оптимизм
взаимная поддержка
профессионализм и компетентность

Постоянное развитие и совершенствование – реализация этого принципа заключается в адекватной оценке себя, определении своих сильных и слабых сторон, желании совершенствовать как индивидуальные знания и навыки, так и коллективные.

Оптимизм – люди в компании убеждены, что несут в себе мощный позитивный заряд, что отражается на отношениях между сотрудниками, с клиентами, поставщиками и даже конкурентами.

Взаимная поддержка – способность работать в команде выступает как ценность.

Профессионализм и компетентность – каждый делает то, что он умеет лучше других, делясь своим опытом и находками.

Корпоративная культура:

способствует достижению целей организации
увеличивает вовлеченность персонала
помогает экономить, например, ценности бережливого производства
помогает больше зарабатывать, например, благодаря удовлетворенности от работы, через формирование соревновательной среды или командной работы

Известный немецкий психолог Рольф Рютtinger, поднявший на ноги не один десяток малых и средних фирм в ФРГ, предложил типологию культуры, которая опирается на два основания – степень риска принимаемых решений и обратную связь реальных последствий принятых решений. Его типология содержит следующие варианты:

- культура мелких успехов, или культура торговли, развивается в первую очередь в торговых организациях, организациях по сбыту, в розничной торговле и отчасти в политике;

- административная культура, проявляется в системе государственной службы, в образовании, крупных административных фирмах, на предприятиях в хорошо налаженных и защищенных отраслях, в политике и частично в банках и в системе страхования;

- инвестиционная культура (культура перспектив), встречается в инвестиционных банках, строительстве, отчасти в науке и армии, в тяжелой, в оборонной и в добывающей промышленности, например в нефтяных и газовых компаниях, отчасти в политике;

- спекулятивная культура (культура мгновенных побед), преимущественно встречается там, где заключаются выгодные сделки с ценными бумагами, но элементы этой культуры можно распознать и в таких областях, как политика, мода, косметика, биржа, профессиональный спорт, реклама и финансирование рискованных предприятий.

Эти варианты отличаются не только величиной риска и скоростью обратной связи, но и скоростью принятия решений, факторами мотивации, организацией документооборота, уровнем кооперирования сотрудников, лидерства.

Но независимо от варианта модели, преимущества внедрения в деятельность компании деловой корпоративной культуры очевидны:

действуют единые стандарты при выполнении работ и оказании услуг, что гарантирует их высокое качество

проще вносить изменения в регламент организации, поскольку персонал спокойно реагирует на новшества

каждый сотрудник осознает собственную значимость и востребованность в общем деле

Проблемы, с которыми сталкиваются компании при формировании корпоративной культуры:

всегда найдутся сотрудники, негативно реагирующие на пропагандируемые организацией принципы и нормы поведения. если не получается убедить их в необходимости придерживаться установленных стандартов, единственным выходом остается увольнение

зачастую возникают сложности со специалистами высокого уровня, которые ранее работали в другой компании и усвоили принятые там нормы – процесс погружения новичка в непривычную для него систему ценностей может протекать болезненно.

Качественно выстроенная корпоративная культура позволяет новым работникам быстро влиться в коллектив, быть мотивированными и нести ответственность за поставленные перед ними задачи. Полноценная вовлеченность сотрудника означает не только соблюдение установленных норм, но и принятие корпоративных ценностей, участие в их дальнейшем формировании.

Ценности корпоративной культуры нельзя задекларировать раз и навсегда – необходимо постоянно подтверждать их конкретными действиями, иначе они превратятся в пустую формальность и не будут выполнять возложенные на них функции. Игнорировать недостатки внедрения единой системы ценностей для персонала компании не получится, поэтому стоит продумать способы борьбы с негативными последствиями при формировании внутренних стандартов поведения.

Формирование корпоративной культуры организации является длительным и сложным процессом. В первую очередь, требуется определить миссию, базовые ценности и сформулировать основные правила поведения членов организации. Без документально оформленных основ корпоративной культуры, не будет дальнейшего ее развития и трансформации. На основе официально закрепленных базовых основ, должны проводиться семинары, тренинги, корпоративные мероприятия, призванные ускорить формирование традиций организаций и разработку общей символики.

Для любого коммерческого проекта главной целью является извлечение прибыли. Но на определение оптимального типа корпоративной культуры влияют и другие стоящие перед компанией задачи, а также личные убеждения и предпочтения владельца бизнеса.

Корпоративная культура сотрудников базируется на тех ценностях, которые руководство компании считает приоритетными. Для авторитарных руководителей важно реализовать свои управленческие амбиции, а для топ-менеджеров демократичного склада на первое место выходит создание атмосферы равноправия и свободного творчества. А значит, и цели в таких компаниях будут отличаться.

Руководству необходимо составить перечень всех значимых для компании ценностей, который первоначально может быть очень большим, затем выделить 3-5 самых важных для достижения стоящих перед организацией целей. После определения главных ценностей компании, необходимо продумать, как именно они будут воплощаться в жизнь. Для каждой задекларированной ценности необходимо разработать правила поведения работников компании, следуя которым они будут ежедневно доказывать свою приверженность заявленным идеалам.

Чтобы внедрение стандартов поведения и общения проходило эффективнее, необходимо отмечать работников, которые придерживаются установленных правил. Формы поощрения могут быть различными – от публичной благодарности до существенного расширения полномочий и продвижения по карьерной лестнице.

Цель таких действий руководства заключается в стимулировании всех сотрудников компании на выполнение правил для достижения стоящих перед коммерческой организацией целей. Важно, чтобы корпоративные ценности не остались только на бумаге, а были ориентиром для каждого действия сотрудников и руководства.

Для наиболее эффективного внедрения внутренних правил задействуются все доступные каналы: проведение общих собраний, рассылка по email, личные беседы, информационные стенды в офисе, статьи в корпоративной прессе и многое другое. Главное, чтобы у сотрудников сформировалось убеждение в обоснованности, рациональности и необходимости следования внедряемым стандартам поведения.

Убедиться в том, что правила поведения прижились и воспринимаются персоналом как норма, позволяют ежегодные мероприятия по оценке итогов внедрения корпоративных стандартов, например, выборочные проверки работы отдельных сотрудников и целых подразделений, выявление случаев отклонения от принятых в компании правил общения работников между собой и с клиентами, разработка мер по исправлению негативных ситуаций.

Процесс внедрения принципов корпоративной культуры можно считать завершенным, когда большинство сотрудников осознанно придерживаются установленных норм поведения, то есть делают это не из страха понести наказание, а полностью принимая и поддерживая декларируемые компанией ценности.

Одним из инструментов укрепления корпоративной культуры являются корпоративные активности – специальные мероприятия, направленные на поддержку корпоративного духа (коллективные игры, праздники, тренинги, мастер-классы, выездные мероприятия, обучение, корпоративный портал, тимбилдинги, совместный спорт и т.д.)

В процессе формирования корпоративной культуры используются элементы комплаенс-системы. Из них можно выделить:

- «Тон сверху» – это реализация ценностных установок и практическое следование, закрепленных в кодексах и регламентах, правил, проявляющееся со стороны руководителей, которые личным примером показывают, что соблюдение принятых правил необходимо;

- кодекс корпоративной этики – это свод правил, регулирующий взаимоотношения сотрудников с клиентами и коллегами по работе, а также совокупность ценностей, целей, норм, правил и инструкций;

- комплаенс политика – это документ, определяющий цели и задачи компании, ключевые процессы, в основе которого лежит контроль соответствия деятельности компании требованиям законодательства, а также ее внутренним правилам и стандартам;

- корпоративное обучение персонала (проведение тренингов, вебинаров, мастер классов, консультаций для сотрудников);

- анализ текущей деятельности (форензик – деятельность по предупреждению и выявлению фактов корпоративного хищения, коррупционных схем и иных неправомерных действий работников, осуществляемая в рамках служебных расследований с привлечением сторонних специалистов, экспертов, «работа над ошибками») [22].

ТЕМА 13

НОРМЫ ПРОФЕССИОНАЛЬНОЙ ЭТИКИ

Профессиональная (деловая) этика является неотъемлемой частью сообщества, объединенного одной профессией или сферой деятельности. По сути, это свод негласных правил, основанный на морально-этических нормах человеческой жизни. Каждая профессиональная среда формирует собственный кодекс поведения, правила которого объединены общими принципами.

Кодекс корпоративной этики – это свод правил, регулирующий взаимоотношения сотрудников с клиентами и коллегами по работе, а также совокупность ценностей, целей, норм, правил и инструкций. Содержание кодекса определяется, прежде всего, особенностями компании, ее структурой, задачами развития, установками ее руководителей. Как правило, кодексы содержат две части: идеологическую (миссия, цели, ценности) и нормативную (стандарты рабочего поведения).

Кодекс корпоративной этики устанавливает приоритеты в отношении целевых групп и пути согласования их интересов. При этом кодекс корпоративной этики может выполнять три основные функции:

- репутационную;
- управленческую;
- развития корпоративной культуры.

Репутационная функция кодекса состоит в формировании доверия к компании со стороны референтных внешних групп (описание политик, традиционно закрепляемых в международной практике по отношению к клиентам, поставщикам, подрядчикам и т.д.). Кодекс, являясь инструментом корпоративного PR, повышает инвестиционную привлекательность компании. Наличие у компании кодекса корпоративной этики становится общемировым стандартом ведения бизнеса.

Управленческая функция кодекса состоит в регламентации поведения в сложных этических ситуациях. Повышение эффективности деятельности сотрудников осуществляется путем: регламентации приоритетов во взаимодействии со значимыми внешними группами, определения порядка принятия решений в сложных этических ситуациях, указания на неприемлемые формы поведения.

Корпоративная этика, кроме того, является составной частью корпоративной культуры. Кодекс корпоративной этики – значимый фактор развития корпоративной культуры. Кодекс может транслировать ценности компании всем сотрудникам, ориентировать сотрудников на единые корпоративные цели и тем самым повышать корпоративную идентичность [22].

Задачи профессиональной этики:

- изучение, как морально-этические нормы формируются в сознании сотрудников, как это сказывается на их взаимодействии друг с другом и в целом на их профессиональной деятельности;
- выявление сути специфических профессионально-этических качеств, признаков высокого мастерства для той или иной профессии;
- формирование перечня морально-этических рекомендаций для людей, работающих в определенной сфере (как руководящему составу, так и другим членам коллектива);
- изучение, насколько люди, работающие в конкретной профессии, понимают ее общественную значимость и цели.

Функции профессиональной этики можно выделить следующие (они будут одинаковы практически для всех сфер деятельности):

- формирование единого сообщества специалистов, у которых будут не просто схожие профессиональные обязанности и цели, но и принципы морально-этического поведения;
- облегчение задачи подбора сотрудников путем формирования в каждом профессиональном сообществе критериев и не попадающий под них человек для той или иной профессии попросту не подходит;

- формирование кодекса профессионального долга и уровня ответственности. В каждой профессии правила работы и выстраивания сотрудничества свои, складываются с учетом принципов этики профессиональных отношений в конкретном направлении деятельности;

- выработка путей и способов развития сообщества профессионалов. В процессе работы в одной социальной группе собираются представители разных специальностей, что способствует внедрению и использованию всевозможных (в том числе инновационных) инструментов развития в любой сфере деятельности;

- воссоздание привлекательного образа профессии. Профессиональная этика способствует тому, что общество положительно воспринимает профессии и образы задействованных в них специалистов.

Основные компоненты профессиональной этики:

- восприятие собственной профессии, а далее – и людей, с которыми в рамках нее приходится взаимодействовать. Правильное осознание таких понятий, как чувство долга, ответственность, добродорядочность и т. д.;

- убедительная мотивация выбора профессии (патриотизм, достойная оплата, карьерный рост, престижность и т. д.);

- пути реализации себя в выбранной профессии (продолжение обучения, выработка важных профессиональных качеств и проч.);

- выполнение управленческих задач по регулированию производственных процессов (распределение обязанностей, моральная и материальная мотивация для членов коллектива и т. д.);

- анализ и оценка достижений (финансовых, морально-этических, управленческих и проч.);

- выработка новых теорий и методик относительно профессиональной этики в случаях, когда это становится необходимым (происходят изменения в обществе, рождаются новые профессии и т. д.).

По сути, профессиональная этика – это некий кодекс морально-нравственных норм, которых люди должны придерживаться, чтобы достичь наивысших результатов в выбранной профессии.

Она формируется в первую очередь на основании действующих общественных норм этики и морали. Однако в разных странах (или даже регионах, или в пределах определенных территориальных единиц) этика профессиональной деятельности для одних и тех же сфер может быть различной, что связано с отличием морально-этических норм и правил, принятых в той или иной местности.

Оказывает свое влияние не только сам социум, но и непосредственно характер деятельности того или иного специалиста в конкретном профессиональном сообществе. Профессиональная этика формируется именно под влиянием обстоятельств, условий (моральных и нравственных), в которых приходится вести деятельность.

Многое зависит от общепринятых моральных правил и еще от того, какого поведения ожидает общество от представителей тех или иных профессий. Формирование профессиональной этики происходит под воздействием как внешних, так и внутренних факторов (установившихся внутри профессионального сообщества).

Также и этика влияет на становление взаимоотношений между профессионалами, а также и с другими членами общества [22].

Поэтому необходимо воспитание этической культуры поведения. Западные компании используют в работе понятие tone at the top, что можно перевести как «тон поведения, задаваемый топ-менеджментом». Имеется в виду, что этическое поведение руководителя становится образцом для остальных членов коллектива. Менеджеры среднего и младшего звена специально обучаются бизнес-этике, и главные пять постулатов, которые при этом закладываются, — это понимание ценности человека, наличие чувства меры, ответственности, справедливости и честности.

Поведение сотрудника считается неэтичным, если он позволяет себе поступки, выходящие за рамки существующих морально-этических (и профессиональных в том числе) норм. Это всегда негативно сказывается и на других членах коллектива, и на клиентах.

Психологическая обстановка в компании ухудшается, а это влечет за собой снижение работоспособности, потерю доверительных отношений с заказчиками и партнерами, в целом страдает репутация фирмы, а значит, и прибыльность бизнеса.

Подобных нормативных положений нет в Трудовом кодексе, а между тем каждый сотрудник на рабочем месте должен понимать, как себя вести с точки зрения моральных и этических правил.

Задача руководителя — способствовать формированию нормальной психологической атмосферы в коллективе, воспитывать в подчиненных вежливость, корректность. Руководитель вправе формулировать правила внутреннего распорядка, в которых может перечислить нормы поведения на работе для своих подчиненных. Наряду с трудовой дисциплиной всем сотрудникам предписывается выполнять данные правила, что должно способствовать выработке этичной манеры поведения.

Формат правил внутреннего распорядка выбирает руководство компаний: где-то это объемные подробные «Правила внутреннего трудового распорядка», а где-то – лишь несколько строк в тексте трудового договора. Крупные компании предпочитают составлять самостоятельный кодекс этики и корпоративного поведения [23].

При формировании документации, регулирующей нормы профессиональной этики, можно использовать стандарты:

ГОСТ Р 59050—2020	Инновационный менеджмент. Этическая оценка исследований и инноваций Часть 1 Комpetенции комитета по этике
ГОСТ Р 59051-2020	Инновационный менеджмент. Этическая оценка исследований и инноваций. Часть 2. Оценка этического воздействия

ЗАКЛЮЧЕНИЕ

Управление рисками приобретает стратегический характер и глубоко интегрируется в деятельность компаний. Эволюционирует и роль специалистов в этой сфере: растет уровень профессионализма, риск-менеджеры стали чаще использовать инновационные технологии. Большая часть риск-менеджеров отмечают, что они выполняют функцию консультантов руководства по стратегии организации.

Многие риск-менеджеры используют локальные ИТ-инструменты (реестры рисков, карты рисков, панели и т.п.). Несмотря на то, что сегодня эти инструменты еще доминируют, риск-менеджеры в своей работе все больше используют новые технологии, такие как анализ данных, визуализация данных, автоматизация процессов с помощью роботов (RPA), искусственный интеллект, блокчейн. Эти технологии позволяют риск-менеджерам улучшить их навыки по идентификации, мониторингу и устраниению рисков за счет манипулирования большими объемами данных, проводить более углубленный анализ. В связи с чем они позволяют лучше выявлять взаимосвязи рисков и быть более проактивными и прогнозными [23].

Определение уровня компетенции, необходимой для достижения целей организации, должно начинаться с оценки текущей компетенции персонала. При этом необходимо учитывать требования нормативных документов, регулирующих потребности в развитии компетенции для конкретной должности. Компетенции специалиста по управлению рисками сформулированы в профессиональном стандарте 08.018, утвержденном приказом Министерства труда и социальной защиты Российской Федерации от 30 августа 2018 года № 564н. На его основе организация может проанализировать текущие уровни компетенции и потребности в компетенции не только на индивидуальном, но и на организационном, командном и групповом уровнях, чтобы определить, когда, где и какие действия следует предпринять для удовлетворения потребностей в компетенции.

ГЛОССАРИЙ

Глоссарий составлен на основе алфавитного указателя терминов ГОСТ Р 51897-2021 «Менеджмент риска. Термины и определения» [6] и терминов и определений, приведенных в ГОСТ Р 52806-2007 «Менеджмент рисков проектов. Общие положения» [15] и ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» [9].

Термин	Определение
Агрегация рисков	Объединение нескольких рисков в один риск, выполняемое для получения более полного понимания совокупного риска
Анализ риска	Процесс изучения сути и содержания риска и определения уровня риска
Анализ участников	Процесс идентификации участников, их интересов и влияния
Аудит менеджмента риска	Систематический, независимый и задокументированный процесс получения объективных фактов о состоянии инфраструктуры менеджмента риска (и/или любой ее части) в целях определения ее эффективности и адекватности
Вероятность	Характеристика возможности и частоты появления события
Владелец риска	Лицо или организация, несущие ответственность и обладающие полномочиями в области менеджмента риска
Воздействие на риск	Процесс удержания и/или изменения риска
Воздействие риска	Мера последствия риска
Восприятие риска	Точка зрения на риск заинтересованной стороны
Идентификация риска	Процесс выявления, определения и описания риска
Измерение риска	Процесс, охватывающий идентификацию риска, анализ риска и оценивание риска

Термин	Определение
Инфраструктура менеджмента риска	Набор компонентов, формирующих основы и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге, пересмотре и постоянном улучшении менеджмента риска во всей организации
Исключение риска	Обоснованное решение об отказе от участия либо выходе из деятельности с целью исключения подверженности конкретному риску
Источник риска	Объект, ситуация или действие, которые самостоятельно или в комбинации могут повлечь за собой риск
Критерий риска	Условия и факторы, относительно которых оценивается существенность риска
Матрица рисков	Инструмент ранжирования и представления рисков путем определения диапазонов последствий и вероятности
Менеджмент риска	Скоординированные действия по руководству, контролю и управлению организацией с учетом риска
Мероприятие по управлению риском	Способ воздействия на риск, направленный на удержание и/или изменение риска
Мониторинг	Постоянный (непрерывный) анализ, надзор, критическая оценка, наблюдение за отклонениями от запланированного или требуемого состояния
Неприятие риска	Отношение к риску, выражаемое в неприемлемости наличия риска

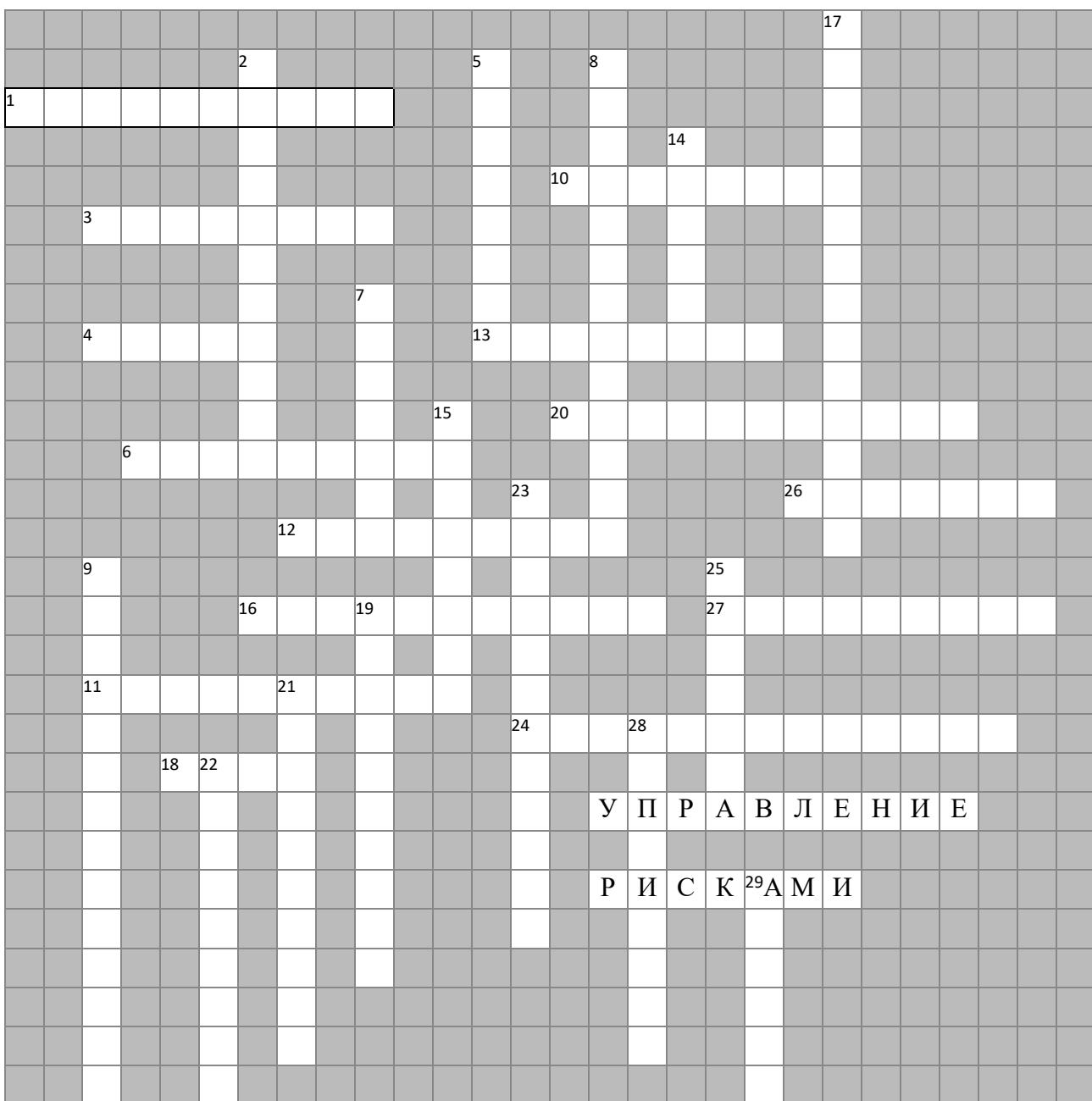
Термин	Определение
Обмен информацией и консультации	Непрерывные итеративные процессы, выполняемые организацией для предоставления, распространения или получения информации и участия в диалоге с заинтересованными сторонами по вопросам, относящимся к менеджменту риска
Опасность	Источник потенциального вреда
Описание риска	Структурированная информация о риске, обычно включающая следующие элементы: источники риска, события, причины и последствия
Определение среды	Выявление внешних и внутренних факторов, которые следует учитывать в рамках менеджмента риска, а также установление сферы применения и критериев риска для политики в области менеджмента риска
Отношение к риску	Подход организации к измерению риска и, таким образом, к увеличению, удержанию, принятию, снижению риска либо отказу от него
Отчетность о риске	Форма обмена информацией, предусматривающая информирование соответствующих внутренних и внешних заинтересованных сторон путем предоставления информации о текущем состоянии риска и менеджменте риска
Оценивание риска	Процесс сравнения результатов анализа риска с критериями риска для определения допустимости или приемлемости риска и/или его размера
Передача риска	Форма воздействия на риск, включающая согласованное перераспределение риска с прочими сторонами

Термин	Определение
Пересмотр	Деятельность, предпринимаемая для определения применимости, адекватности и эффективности объекта или действий для достижения установленных целей
План менеджмента риска	Схематичное описание деятельности и мероприятий в пределах инфраструктуры менеджмента риска, устанавливающих подход, инструменты управления и ресурсы, применяемые для менеджмента риска
Подверженность	Степень воздействия события на организацию и/или заинтересованную сторону
Политика в области менеджмента риска	Заявление организации об общих намерениях, руководящих принципах и направлениях деятельности в области менеджмента риска
Последствие	Результат влияния события на достижение целей
Правдоподобность (появления события)	Характеристика возможности и частоты появления события
Принятие риска	Обоснованное решение о принятии конкретного риска
Профиль рисков	Информация о любой совокупности рисков
Процесс менеджмента риска	Взаимосвязанные действия по обмену информацией, консультированию, определению среды, идентификации, анализу, оцениванию, воздействию, мониторингу и пересмотру риска, выполняемые в соответствии с политиками, процедурами и методами менеджмента организации
Распределение риска	Распространение риска посредством его распределения между другими участниками

Термин	Определение
Реестр рисков	Задокументированная информация об идентифицированных рисках
Риск	Влияние неопределенности на достижение поставленных целей
Риск-аппетит	Величина и тип соответствующего риска, который организация готова поддерживать или достичь
Риск вторичный	Риск, возникающий в результате рассмотрения проблем, связанных с риском
Риск остаточный	Риск, оставшийся после воздействия на него
Событие	Происшествие, проявление или изменение совокупности обстоятельств
Сохранение риска	Согласованное (обоснованное) принятие потенциальных потерь или выгод от конкретного риска
Среда внешняя	Внешние условия, в которых организация функционирует и стремится достигнуть свои цели
Среда внутренняя	Внутренние условия, в которых организация функционирует и стремится достигнуть своих поставленных целей
Сторона заинтересованная	Лицо или организация, которые могут воздействовать, или испытывать воздействие, или считать, что на них оказывает воздействие какое-либо решение или деятельность
Сторона причастная	Любой индивидуум, группа или организация, которые могут воздействовать на риск, подвергаться воздействию или ощущать себя подверженными воздействию риска
Толерантность к риску	Готовность организации и заинтересованных сторон понести риск после воздействия на него для достижения своих целей

Термин	Определение
Управление риском	Меры, направленные на изменение риска
Уровень риска	Размер риска или комбинации рисков, характеризуемый последствиями и их вероятностью
Устойчивость организации	Способность организации к адаптации в сложных и изменяющихся обстоятельствах
Уязвимость	Присущие свойства объекта, определяющие его чувствительность к источнику риска, которые могут привести к событиям, влекущим последствия
Формирование финансовых резервов по риску	Форма воздействия на риск, включающая согласованное резервирование средств в целях покрытия или изменения возникающих финансовых последствий в случае, если они произойдут
Частота	Количество событий или их последствий за определенный период времени

На основе глоссария составлен кроссворд для самопроверки:



По горизонтали:

- | |
|--|
| 1. Присущие свойства объекта, определяющие его чувствительность к источнику риска, которые могут привести к событиям, влекущим последствия |
| 3. Лицо или организация, несущие ответственность и обладающие полномочиями в области менеджмента риска |
| 4. Систематический, независимый и задокументированный процесс получения объективных фактов о состоянии инфраструктуры менеджмента риска (и/или любой ее части) в целях определения ее эффективности и адекватности |
| 6. Деятельность, предпринимаемая для определения применимости, адекватности и эффективности объекта или действий для достижения установленных целей |
| 10. Форма воздействия на риск, включающая согласованное перераспределение риска с прочими сторонами |
| 11. Точка зрения на риск заинтересованной стороны |
| 12. Источник потенциального вреда |
| 13. Условия и факторы, относительно которых оценивается существенность риска |
| 16. Характеристика возможности и частоты появления события |
| 18. Влияние неопределенности на достижение поставленных целей |
| 20. Результат влияния события на достижение целей |
| 24. Процесс выявления, определения и описания риска |
| 26. Информация о любой совокупности рисков |
| 27. Объединение нескольких рисков в один риск, выполняемое для получения более полного понимания совокупного риска |

По вертикали:

2. Процесс удержания и/или изменения риска
5. Объект, ситуация или действие, которые самостоятельно или в комбинации могут повлечь за собой риск
7. Количество событий или их последствий за определенный период времени
8. Готовность организации и заинтересованных сторон понести риск после воздействия на него для достижения своих целей
9. Степень воздействия события на организацию и/или заинтересованную сторону
14. Задокументированная информация об идентифицированных рисках
15. Обоснованное решение о принятии конкретного риска
17. Набор компонентов, формирующих основы и организационные меры, применяемые при проектировании, разработке, внедрении, мониторинге, пересмотре и постоянном улучшении менеджмента риска во всей организации
19. Риск, оставшийся после воздействия на него
21. Обоснованное решение об отказе от участия либо выходе из деятельности с целью исключения подверженности конкретному риску
22. Процесс, охватывающий идентификацию риска, анализ риска и оценивание риска
23. Способность организации к адаптации в сложных и изменяющихся обстоятельствах
25. Инструмент ранжирования и представления рисков путем определения диапазонов последствий и вероятности
28. Отношение к риску, выражаемое в неприемлемости наличия риска
29. Процесс изучения сути и содержания риска и определения уровня риска

СПИСОК ЛИТЕРАТУРЫ

1. Руководство PMBOK 7 - PMI - Руководство к своду знаний по управлению проектами (Руководство PMBOK) и Стандарт управления проектом. Седьмое издание – 2021 URL: <https://studylib.net/doc/26353386/rukovodstvo-pmbok-7---pmi---rukovodstvo-k-svodu-znanij-ro...> (дата обращения: 25.03.2024)
2. Профессиональный стандарт 08.018 «Специалист по управлению рисками» URL: <https://classinform.ru/profstandarty/08.018-spetsialist-po-upravleniu-riskami.html> (дата обращения: 25.03.2024)
3. Федеральный закон Российской Федерации от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании» URL: <http://www.kremlin.ru/acts/bank/18977> (дата обращения: 25.03.2024)
4. Риск-менеджмент: задачи, инструменты, результаты URL: <https://dasreda.ru/media/for-managers/risk-menedzhment> (дата обращения: 25.03.2024)
5. ГОСТ Р 54147-2010 «Стратегический и инновационный менеджмент. Термины и определения» URL: <https://meganorm.ru/Data/511/51109.pdf> (дата обращения: 25.03.2024)
6. ГОСТ Р 51897-2021 «Менеджмент риска. Термины и определения» URL: <https://meganorm.ru/Data/760/76097.pdf> (дата обращения: 25.03.2024)
7. ГОСТ Р МЭК 62198-2015 «Проектный менеджмент. Руководство по применению менеджмента риска при проектировании URL: <https://meganorm.ru/Data2/1/4293758/4293758071.pdf> (дата обращения: 25.03.2024)
8. ГОСТ Р 56020-2014 «Бережливое производство. Основные положения и словарь URL: <https://meganorm.ru/Data/574/57442.pdf> (дата обращения: 25.03.2024)

9. ГОСТ Р ИСО 31000-2019 «Менеджмент риска. Принципы и руководство» URL:
<https://meganorm.ru/Index2/1/4293724/4293724882.htm> (дата обращения: 25.03.2024)

10. Матвеева К.А. Особенности социологического изучения рисков URL: <https://cyberleninka.ru/article/n/osobennosti-sotsiologicheskogo-izucheniya-riskov> (дата обращения: 25.03.2024)

11. Стандарты управления рисками URL:
<https://www.ferma.eu/app/uploads/2011/11/a-risk-management-standard-russian-version.pdf> (дата обращения: 25.03.2024)

12. Рыхтикова, Н. А. Анализ и управление рисками организации: учебное пособие / Н.А. Рыхтикова. — 3-е изд. — Москва: ИНФРА-М, 2021. — 248 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/textbook_597f03f1c44465.44914120. - ISBN 978-5-16-013163-4. - Текст: электронный. - URL: <https://znanium.com/catalog/product/1937180> (дата обращения: 04.04.2024). – Режим доступа: по подписке.

13. ГОСТР 58771-2019 «Менеджмент риска. Технологии оценки риска» URL:
<https://meganorm.ru/Data2/1/4293724/4293724640.pdf> (дата обращения: 25.03.2024)

14. План менеджмента риска URL:
<https://www.homework.ru/spravochnik/plan-menedzhmenta-riska/> (дата обращения: 25.03.2024)

15. ГОСТ Р 52806-2007 «Менеджмент рисков проектов. Общие положения» URL: <https://meganorm.ru/Data2/1/4293828/4293828754.htm> (дата обращения: 25.03.2024)

16. Крючков Р.А. Правовое управление рисками: понятие и сущность явления URL: <https://cyberleninka.ru/article/n/pravovoe-upravlenie-riskami-ponyatie-i-suschnost-yavleniya> (дата обращения: 25.03.2024)

17. Вохминцев В.В. Нормативно-правовое обеспечение риск-менеджмента URL: <https://cyberleninka.ru/article/n/normativno-pravovoe-obespechenie-risk-menedzhmenta> (дата обращения: 25.03.2024)
- 18 Разглашение коммерческой тайны URL: https://rt-solar.ru/products/solar_dozor/blog/2594/ (дата обращения: 25.03.2024)
19. Матковский А.И. Информационная политика компании URL: <https://www.km.ru/biznes-i-finansy/2006/08/16/biznes-obrazovanie/informatsionnaya-politika-kompanii> (дата обращения: 25.03.2024)
20. Алиаскарова Ж.А., Дорошко А.С. Информационная политика предприятия как осознанная необходимость, или зачем обществу о вас знать? URL: <http://repo.sau.ru/bitstream/Chelovek-Znak-Tehnika/informacionnaya-politika-predpriyatiya-kak-osoznannaya-neobhodimost-ili-zachem-obshchestvu-znat-o-vas-87938/1/34.%20Алиаскарова%20Ж.А.%2C%20Дорошко%20А.С.%2020206-211.pdf> (дата обращения: 25.03.2024)
21. Корпоративная культура URL: <https://compliance.su/info/articles/podrobnyy-obzor-vebinara-korporativnaya-kultura-organizatsii-formirovaniye/> (дата обращения: 25.03.2024)
22. Профессиональная этика: правила корпоративного тона URL: <https://sales-generator.ru/blog/professionalnaya-etika/#1> (дата обращения: 25.03.2024)
23. Маликова С.Г. Роль управления рисками в стратегическом управлении компаний возрастает URL: <https://www.eg-online.ru/article/391850/> (дата обращения: 25.03.2024)

Учебное издание

Закирова А.Р., Заппаров Б.А., Фейфер Р.Л.

УПРАВЛЕНИЕ РИСКАМИ ПРОЕКТА

Учебное пособие