ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 72254— 2025

Менеджмент риска

РУКОВОДЯЩИЕ УКАЗАНИЯ ПО ПРИМЕНЕНИЮ ГОСТ Р ИСО 31000—2019 В СИСТЕМАХ МЕНЕДЖМЕНТА

Издание официальное

Москва
Российский институт стандартизации
2025

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 010 «Менеджмент риска»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 1 сентября 2025 г. № 977-ст

4 Настоящий стандарт является модифицированным по отношению к международному документу IWA 31:2020 «Менеджмент риска. Руководящие указания по применению ИСО 31000 в системах менеджмента» (IWA 31:2020 «Risk management — Guidelines on using ISO 31000 in management systems», MOD), путем внесения изменений, которые выделены в тексте полужирным курсивом, а также исключения приложения С и добавления элемента «Библиография».

Внесение указанных технических отклонений направлено на учет потребностей национальной стандартизации.

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе, приведены в дополнительном приложении ДА.

Сопоставление структуры настоящего стандарта со структурой указанного международного документа приведено в дополнительном приложении ДБ

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.rst.gov.ru)

Содержание

Введение

Число организаций всех типов и размеров, использующих системы менеджмента, основанные на стандартах ИСО и МЭК (Management System Standard, MSS), устойчиво растет. Разрабатываются новые стандарты ИСО и МЭК на системы менеджмента, рассматривающие конкретные аспекты деятельности, продукцию или услуги организации. Часть 1 директивы ИСО/МЭК определяет структуру высокого уровня (High Level Structure, HLS) для стандартов на системы менеджмента. Эта общая структура регламентирует согласованный основной текст, общие термины и основные определения для всех стандартов на системы менеджмента ИСО и МЭК. Организация может внедрить в свою систему управления требования или рекомендации различных стандартов на системы менеджмента. Унифицированная структура стандартов MSS может упростить для пользователей построение не фрагментарной, а интегрированной системы менеджмента (Integrated Management System, IMS). Во всех стандартах MSS используется концепция, основанная на менеджменте риска, риск-ориентированном подходе или риск-ориентированном мышлении (в зависимости от терминологии, используемой в рассматриваемой системе менеджмента), которая лежит в основе любой системы менеджмента. Главным преимуществом этого является комплексное применение взаимосвязанных систем. Применение ***ГОСТ Р ИСО 31000*** может способствовать развитию или совершенствованию интегрированной системы менеджмента, в нем содержатся рекомендации по определению рисков, на которые необходимо обратить внимание, чтобы обеспечить уверенность в том, что система менеджмента может достигать намеченных результатов, усиливать желаемые эффекты, предотвращать или уменьшать нежелательные эффекты и обеспечивать постоянное улучшение.

ГОСТ Р ИСО 31000 — это передовая практика в области менеджмента риска, которая является общепринятой, универсальной и применимой к менеджменту любых видов рисков. Интеграция менеджмента риска в системе(ах) менеджмента с применением ***ГОСТ Р ИСО 31000*** приносит организации множество преимуществ, независимо от того, касаются ли они только негативных последствий или предусматривают положительные эффекты. Целью менеджмента риска в соответствии с ***ГОСТ Р ИСО 31000*** является создание и защита ценностей организации. Применение ***ГОСТ Р ИСО 31000*** помогает повысить эффективность решений владельцев рисков или владельцев процессов, а также повышает качество управления процессами и всеми другими видами деятельности организации, включая стратегическую и оперативную, что, в свою очередь, способствует достижению лучших результатов, что, в свою очередь, способствует повышению качества выпускаемой продукции, снижению издержек из-за ошибок, а также позволяет управлять ответственностью.

Интеграция менеджмента риска в соответствии с принципами ***ГОСТ Р ИСО 31000*** создает и защищает ценность организаций, способствуя достижению целей и делая организацию более устойчивой к неблагоприятным воздействиям. Измерение рисков позволяет надлежащим образом их оценивать и создает основу для повышения результативности системы управления организацией, достижения улучшенных результатов и предотвращения негативных последствий. Интеграция менеджмента риска в систему управления может создавать сложности, которые можно уменьшить, следуя рекомендациям, изложенным в настоящем стандарте.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Менеджмент риска

РУКОВОДЯЩИЕ УКАЗАНИЯ ПО ПРИМЕНЕНИЮ ГОСТ Р ИСО 31000—2019 В СИСТЕМАХ МЕНЕДЖМЕНТА

Risk management. Guidelines on using GOST R ISO 31000—2019 in management systems

Дата введения — 2026—03—01

1 Область применения

Настоящий стандарт содержит руководящие указания по интеграции и применению ***ГОСТ Р ИСО 31000*** в организациях, которые внедрили один или несколько стандартов на системы менеджмента ИСО и МЭК (MSS) или которые решили реализовать проект по внедрению одного или нескольких стандартов MSS, включающих ***ГОСТ Р ИСО 31000***. В настоящем стандарте приведены разъяснения о том, как положения ***ГОСТ Р ИСО 31000*** соотносятся со структурой высокого уровня (HLS) для MSS.

Настоящий стандарт не содержит рекомендаций по внедрению системы менеджмента в целом. В нем не определены требования к MSS. Настоящий стандарт не содержит краткого изложения ***ГОСТ Р ИСО 31000***, но обеспечивает основу для его понимания. Применение настоящего стандарта не устраняет необходимости использования других стандартов, направленных на конкретные аспекты риска.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

ГОСТ Р ИСО 14001 Системы экологического менеджмента. Требования и руководство по применению

ГОСТ Р ИСО 31000—2019 Менеджмент риска. Принципы и руководство

ГОСТ Р ИСО 45001 Системы менеджмента безопасности труда и охраны здоровья. Требования и руководство по применению

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины и определения по ***ГОСТ Р ИСО 31000***.

4 Использование термина «риск» в *ГОСТ Р ИСО 31000* и в других стандартах

Применение терминологии следует рассматривать в контексте ***ГОСТ Р ИСО 31000—2019*** (пункт 3.1), который определяет «риск» для целей менеджмента организации как «следствие влияния неопределенности на достижение поставленных целей». В некоторых стандартах при определении риска не упоминаются цели, но в тексте говорится, что риск необходимо учитывать, чтобы обеспечить уверенность в том, что система менеджмента сможет достичь запланированных результатов. Цель может быть выражена как поставленная задача или результат.

Структура и процесс менеджмента риска в соответствии с ***ГОСТ Р ИСО 31000*** интегрированы и соразмерны внешней и внутренней среде организации, связанным с ее целями. Они включают в себя точки зрения заинтересованных сторон.

В некоторых областях (таких как безопасность, охрана труда, область медицинских изделий) используется другая терминология, отражающая общее понимание термина «риск», которое сужает концепцию риска, определенную в ***ГОСТ Р ИСО 31000***, поскольку оно фокусируется на потенциальном негативном воздействии отклонений от ожидаемого. Данный подход можно считать включенным в более широкое определение риска, установленное в *ГОСТ Р ИСО 31000—2019* (пункт 3.1).

5 Руководящие указания к *ГОСТ Р ИСО 31000* для пользователей стандартов на системы менеджмента (MSS)

В ГОСТ Р ИСО 31000 представлены руководящие указания для всех типов организаций, независимо от их типа и размера, и предназначенные для пользователей, которые создают и защищают ценность организаций посредством менеджмента риска, принятия решений, постановки целей и стратегии, достижения поставленных задач и повышения производительности.

Восемь принципов менеджмента риска служат основой для создания и защиты ценностей организации. Они содержат рекомендации по характеристикам эффективного и действенного менеджмента риска, информируют о его ценности и объясняют его предназначение и цели. ***ГОСТ Р ИСО 31000*** обеспечивает единый подход к менеджменту любых видов риска, с которым сталкивается организация на протяжении всей своей деятельности.

Цель системы менеджмента риска заключается в том, чтобы помочь организации интегрировать менеджмент риска в значимых видах деятельности и функциях. Результативность менеджмента риска будет зависеть от его интеграции в систему управления организацией, включая процесс принятия решений.

Процесс менеджмента риска, изложенный в ***ГОСТ Р ИСО 31000***, должен быть интегрирован пропорционально внешней и внутренней среде организации, связанной с ее целями. Его следует интегрировать таким образом, чтобы он стал неотъемлемой частью системы управления и был адаптирован к структуре, деятельности и процессам организации.

Применяя руководящие указания, касающиеся принципов и структуры, организация может выбрать индивидуальную настройку применения процессов менеджмента риска в своей системе управления с учетом любого типа риска, с которыми она сталкивается на протяжении всей своей деятельности. Добавление этапов процесса менеджмента риска может улучшить систему управления. В этом контексте необходимо помнить, что, хотя процесс менеджмента риска часто представляется как последовательный, но на практике он является итеративным.

Менеджмент риска следует применять каждый раз, когда имеется какая-либо информация или оценка, которые инициируют или дополняют процесс или деятельность, или когда происходят изменения в среде организации.

В этой информации или оценке может быть некоторая неопределенность, которая может повлиять на достижение целей. В ***ГОСТ Р ИСО 31000—2019*** (пункт 3.1) эффект объясняется как отклонение от ожидаемого, которое может быть положительным, отрицательным или и тем, и другим. Следовательно,

организация должна пересматривать процедуру идентификации риска каждый раз, когда появляется новая информация или оценки, имеющие отношение к ее процессам и деятельности.

На рисунке 1 показано наложение руководящих указаний ***ГОСТ Р ИСО 31000*** на структуру общих положений HLS для MSS. В верхней строке приведены ссылки на разделы HLS, а в левом столбце представлены разделы структуры ***ГОСТ Р ИСО 31000***. Например, если посмотреть на ячейку пересечения ***ГОСТ Р ИСО 31000—2019*** (подраздел 5.2), посвященную лидерству, и раздела HLS о лидерстве, серый цвет указывает на то, что должен существовать процесс, относящийся к менеджменту риска. Таким образом, эту таблицу целесообразно использовать в качестве ориентира. Более подробная информация о связях между разделами приведена в таблице А.1.

ИСО MSS HLS разделы →	Среда организации	Лидерство	Планирование	Средства поддержки	Деятельность на стадиях жизненного цикла продукции и услуг	Результаты деятельности	Улучшение
ГОСТ Р ИСО 31000—2019 руководство и структура	*ГОСТ Р ИСО 31000—2019* (подраздел 5.1): «Структура менеджмента риска предназначена для обеспечения возможности интеграции процесса менеджмента риска в основные направления деятельности и функции»						
4 Принципы							
5.1 Общие положения							
5.2 Лидерство и приверженность							
5.3 Адаптация							
5.4 Проектирование и разработка							
5.5 Внедрение							
5.6 Оценка эффективности							
5.7 Улучшение							
6.1 Общие положения							
6.2 Обмен информацией и консультирование							
6.3 Область применения, среда и критерии							
6.4 Оценка риска							
6.5 Обработка риска							
6.6 Мониторинг и пересмотр							
6.7 Документирование и отчетность							

Рисунок 1 — Взаимосвязь между ***ГОСТ Р ИСО 31000*** и разделами HLS для MSS

6 Интегрированные системы менеджмента и применение *ГОСТ Р ИСО 31000*

Менеджмент риска может быть реализован с помощью процессного подхода к системе управления. Структуру ***ГОСТ Р ИСО 31000*** следует объединить с системой менеджмента путем применения анализа неиспользованных резервов для включения компонентов структуры *ГОСТ Р ИСО 31000*. Интеграция менеджмента риска в процессном подходе позволяет избежать дублирования и противоречий.

Для достижения эффективной и действенной интеграции и внедрения структуры ***ГОСТ Р ИСО 31000*** и его процессов в другие MSS организация должна принять принципы, изложенные в ***ГОСТ Р ИСО 31000***. В *[1]* содержатся подробные инструкции по интеграции MSS.

Приложение А содержит рекомендации для организации с описанием подходов к интеграции менеджмента риска в свои MSS. Приложение В представляет собой анализ примеров по включению ***ГОСТ Р ИСО 31000*** в междисциплинарную систему менеджмента.

Приложение А
(справочное)

Соответствие между *ГОСТ Р ИСО 31000* и структурами высокого уровня (HLS) для стандартов на системы менеджмента (MSS)

В таблице А.1 показаны связи между основными разделами ***ГОСТ Р ИСО 31000*** и наиболее важными соответствующими разделами HLS для MSS. Пользователи ***ГОСТ Р ИСО 31000*** могут внедрять методы менеджмента риска в систему управления организации, в которой рассматриваются эти разделы HLS.

Таблица А.1 — Соответствие между ***ГОСТ Р ИСО 31000*** и HLS для MSS

Разделы HLS для MSS		Разделы ***ГОСТ Р ИСО 31000—2019***		
		4 Принципы[1)]	5 Структура	6 Процесс
4 Среда организации	4.1 Понимание организации и ее среды	0, a), c), e), f), g)	5.2, 5.4.1	6.1, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.2 Понимание потребностей и ожиданий заинтересованных сторон	0, a), c), d), e), f), g)	5.2, 5.4.1, 5.4.5	6.1, 6.2, 6.3.1, 6.3.3, 6.3.4, 6.6, 6.7
	4.3 Определение области применения системы менеджмента XXX	0, a), c), f)	5.1, 5.2, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
	4.4 Система менеджмента XXX	0, a), b), c), f)	5.1, 5.2, 5.3, 5.4.1, 5.5	6.3.1, 6.3.3, 6.3.4
5 Лидерство	5.1 Лидерство и приверженность	0, a), c), d), g)	5.1, 5.2, 5.4.2, 5.4.4	6.2, 6.6, 6.7
	5.2 Политика	0, a), c), d), g)	5.2, 5.4.2	6.2, 6.6, 6.7
	5.3 Функции, ответственность и полномочия в организации	a), c), d), g)	5.2, 5.4.3	—
6 Планирование	6.1 Действия в отношении рисков и возможности	0, a), b), e), f)	5.1, 5.4.2, 5.7.1	6.1, 6.4, 6.5
	6.2 Цели в области XXX и планирование их достижения	0, a), b)	5.4.2, 5.7.2	6.5
7 Средства поддержки	7.1 Ресурсы	0, a), f), g)	5.1, 5.4.4	6.3.4, 6.5.2
	7.2 Компетентность	0, a), f), g)	5.1	—
	7.3 Осведомленность	0, a), f), g)	5.1	—
	7.4 Обмен информацией	0, a), d), f)	5.1, 5.4.5	6.1, 6.2, 6.3.4
	7.5 Документированная информация	0, a), f)	5.1	6.1, 6.7
8 Деятельность на стадиях жизненного цикла продукции и услуг	8.1 Планирование и управление деятельностью на стадиях жизненного цикла продукции и услуг	0, a), b), f)	5.1, 5.3, 5.5, 5.7	6.1, 6.4, 6.5, 6.6, 6.7

Окончание таблицы А.1

Разделы HLS для MSS		Разделы ***ГОСТ Р ИСО 31000—2019***		
		4 Принципы[1)]	5 Структура	6 Процесс
9 Оценка результатов деятельности	9.1 Мониторинг, измерение, анализ и оценка	a)	5.6	6.1, 6.3.3, 6.3.4, 6.4.1, 6.6, 6.7
	9.2 Внутренний аудит	a)	5.6	6.1, 6.3, 6.4.1, 6.6, 6.7
	9.3 Анализ со стороны руководства	0, a), b), e), g)	5.6, 5.7	6.1, 6.3, 6.4.1, 6.6, 6.7
10 Улучшение	10.2[2)] Несоответствие и корректирующие действия	0, a), h)	5.7	6.1, 6.4, 6.5, 6.6
	10.3[2)] Постоянное улучшение	0, a), h)	5.1, 5.2, 5.7	6.1, 6.4, 6.5, 6.6

[1)] Принцип «0» относится к основному принципу «создание и защита ценности».

[2)] Нумерация подраздела приведена в соответствии со структурой ГОСТ Р ИСО 9001—2015.

Примечание — Номера разделов в графах относятся к структурным элементам ***ГОСТ Р ИСО 31000*** в соответствии с наименованием соответствующей графы.

Приложение В
(справочное)

Примеры внедрения *ГОСТ Р ИСО 31000* в систему менеджмента с несколькими областями

В.1 Общие положения

Примеры внедрения иллюстрируют целостный подход к менеджменту риска в организации, охватывающий ряд аспектов и основанный на принципах ***ГОСТ Р ИСО 31000*** и HLS для MSS. Анализ примеров не дает каких-либо указаний о том, как интегрировать ***ГОСТ Р ИСО 31000*** в систему(ы) менеджмента организации. Он также не содержит требований, относящихся к каждому из упомянутых MSS.

Выделены только аспекты некоторых разделов/требований (которые считаются особенно эффективными), чтобы показать, как применение требований к процессам системы менеджмента качества (QMS) организации было пересмотрено с точки зрения менеджмента риска.

В анализе примеров применены следующие виды написания текста:

- *курсив*: представляет точку зрения организации;
- обычный текст: содержит руководящие указания.

Примечание — ***В настоящем приложении используется термин «заинтересованная сторона».*** Согласно определению термина «причастная сторона» в ***ГОСТ Р ИСО 31000—2019*** (пункт 3.3) также можно применять термин «заинтересованная сторона».

В.2 Описание и история организации

«XYZ» — это вымышленная организация, со следующими характеристиками:

а) в ее состав входит приблизительно 120 человек,

б) ее деятельность связана с разработкой, продажей, техническим консультированием и производством продукции путем смешения в порошкообразном и жидком состоянии:

1) химических средств для обработки поверхностей материалов,

2) химических средств для очистки воды,

3) смазочных материалов для механической обработки,

4) химических вспомогательных ингредиентов,

5) временных защитных пленок и клеевых систем для аэрокосмической промышленности,

в) это коммерческая корпорация;

г) компания должна учитывать нормативно-правовую среду, действующую в ***нескольких странах,*** по таким вопросам, как требования к утилизации, требования к химическим отходам, требования к транспортированию, требования безопасности и т. д.;

д) активы компании состоят из двух заводов и одного головного офиса, находящегося в другом городе.

Организация сертифицирована по ***ГОСТ Р ИСО 9001***.

После сертификации по ***ГОСТ Р ИСО 9001*** *клиенты предъявляли дополнительные требования к работе с другими стандартами на системы менеджмента (MSS) для управления аспектами окружающей среды, здоровья и безопасности, которые использовались как отдельные системы.*

К концу декабря 2017 года менеджер по качеству (QM) осознал возможность интеграции менеджмента риска в соответствии с ***ГОСТ Р ИСО 31000*** *в систему управления компанией, начиная с консолидированной QMS.*

После обсуждения с руководителем организации и получения его принципиального одобрения QM предложил руководителю организации совместно посетить семинар, на котором организации из трех разных секторов поделятся своим собственным опытом использования ***ГОСТ Р ИСО 31000, в том числе и опытом перехода с редакции 2010 года на редакцию 2019 года****. К концу семинара руководитель организации и QM осознали ценность внедрения структуры менеджмента риска для поддержки систем менеджмента в организации и приняли решение двигаться дальше.*

Подход к менеджменту риска должен быть интегрирован в существующую систему менеджмента по ***ГОСТ Р ИСО 9001****. Руководитель организации и совет директоров возложили на отдел управления качеством ответственность и наделили его полномочиями по подготовке подробного проекта, в котором должны были быть сформулированы положения и способы подхода к менеджменту риска в соответствии с* ***ГОСТ Р ИСО 31000****. Они также поручили всем владельцам процессов активно сотрудничать с отделом управления качеством как при подготовке, так и при реализации проекта.*

Эти намерения и указания затем были включены в интегрированную политику организации. Далее приведены примеры:

- риск является неотъемлемой и неизбежной составляющей нашего бизнеса, любая деятельность, которая помогает организации достигать поставленных целей, сопряжена с новыми рисками для организации;

- мы берем на себя обязательство управлять всеми рисками на опережение и эффективно;

- оценивание риска будет применяться ко всем аспектам нашего бизнеса руководством, органами управления и к операциям на соответствующих уровнях;

- мы пропагандируем культуру осознания риска при принятии любых решений, поэтому способствуем распространению риск-ориентированного мышления, направленного на использование возможностей и предотвращение нежелательных результатов;

- риск-ориентированное мышление относится к культуре осознания риска, которая должна быть прочно укоренена на всех уровнях нашей организации как неотъемлемая часть «знаний организации»;

- каждый сотрудник в нашей организации несет ответственность за менеджмент риска в пределах своей компетенции и в рамках возложенных на него полномочий, ответственности и подотчетности;

- потребители все чаще ожидают от организации соблюдения этических норм, и это относится ко всем аспектам наших процессов, которые прямо или косвенно способствуют созданию ценности организации;

- приверженность менеджменту риска распространяется на всех наших поставщиков;

- наши критерии риска (относящиеся как к оценке значимости риска, так и к выбору варианта обработки риска) основаны на нашем этическом кодексе и, в частности, на балансе трех постулатов устойчивого развития (окружающая среда, социальная политика, экономическая политика): затраты и выгоды должны быть оценены с точки зрения устойчивости развития организации;

- мы также будем применять систему менеджмента риска для менеджмента правовых рисков, что поможет нам выполнять все наши обязательства.

В.3 Применение системы менеджмента риска (в соответствии с *ГОСТ Р ИСО 31000*) в существующей системе менеджмента качества (QMS)

Отдел управления качеством отметил, что все положения должны быть в той или иной степени задействованы в проекте по применению системы менеджмента риска в существующей системе менеджмента качества (далее именуемой «проект»).

Первый этап проекта был основан на том, что компоненты системы менеджмента риска должны быть встроены в общую стратегическую и оперативную политику и практику организации. Это означает, что на первом этапе был проведен анализ каждого элемента QMS с целью выявления и оценки любых неиспользованных резервов в существующей практике менеджмента риска. Второй этап предполагал использование этих резервов путем интеграции компонентов системы менеджмента риска во взаимосвязанные и взаимодействующие элементы QMS (т. е. в структуру организации, роли и обязанности, планирование и процессы для достижения поставленных ею целей).

Помимо разделов ***ГОСТ Р ИСО 9001***, в которых прямо упоминается риск (связанный с возможностями и угрозами), почти во всех разделах и соответствующих требованиях имеются прямые или косвенные ссылки на риск и менеджмент риска.

Приведенные ниже соображения были приняты во внимание организацией.

*Планирование (см. **ГОСТ Р ИСО 9001—2015**, раздел 6) считалось ключевым пунктом менеджмента риска, поскольку оно является неотъемлемой частью концепции влияния неопределенности на достижение целей.*

*Понимание организации и ее среды (см. **ГОСТ Р ИСО 9001—2015**, подраздел 4.1) было основой как для создания процессов системы менеджмента, так и для структуры и процесса менеджмента риска. Определение соответствующих заинтересованных сторон, их потребностей и ожиданий стало основой для создания системы менеджмента и ее процессов, а также для определения критериев риска. Требования, касающиеся обмена информацией (см. **ГОСТ Р ИСО 9001—2015**, подраздел 7.4), были дополнены предложениями по обмену информацией и консультированию, приведенными в **ГОСТ Р ИСО 31000**.*

*Документированная информация (см. **ГОСТ Р ИСО 9001—2015**, подраздел 7.5) в соответствии с HLS требует наличия, в дополнение к документам, непосредственно указанным в стандарте, документированной информации, которая, по мнению организации, необходима для результативности QMS. В проекте было указано, что менеджмент риска должен использоваться для определения того, какие документы, помимо тех, которые требуются стандартом, необходимы и какой должна быть степень их детализации. Помимо рассмотрения размера организации, вида ее деятельности, сложности процессов, их взаимодействия и компетентности персонала, по каждому процессу можно было бы задать два вопроса:*

***а)** к каким негативным последствиям может привести отсутствие документированной информации (процедур, инструкций, записей или низкая степень их детализации)?*

***б)** какие положительные результаты можно было бы получить, введя новую процедуру, инструкцию, регистрацию или повысив уровень детализации существующих процедур, инструкций, регистрации?*

При этом учитывали, что документы, более объемные или более подробные, чем необходимо, рискуют быть полностью не приняты во внимание.

*Были определены процессы (см. **ГОСТ Р ИСО 9001—2015**, подраздел 4.4), необходимые для системы управления, и их применения во всей организации, независимо от того, совершаются ли эти процессы внутри компании или на аутсорсинге. Для каждого процесса (внутреннего или внешнего) со значительной неопределенностью в проекте было указано, что необходимо определить:*

- виды деятельности, которые преобразуют повышение качества в результаты работы;

- результаты, которые должны быть достигнуты;

- возможное воздействие, положительное или отрицательное, на последующие процессы и на конечный продукт;

- средства управления, мониторинга, измерения, которые должны были быть такими, чтобы иметь возможность увеличить до максимального уровня положительные воздействия (использование возможностей для улучшения) и свести до минимального уровня отрицательные воздействия (избежание нежелательных событий, несоответствий).

Документированная информация, например, о процедурах, рабочие инструкции, спецификации и т. д., содержит действия по устранению рисков для того, чтобы процессы в QMS могли достигать запланированных результатов, усиливать желаемые воздействия, предотвращать или уменьшать нежелательные воздействия и добиваться улучшений.

Существует тесная взаимосвязь между менеджментом риска и принятием решений, которая четко изложена и подтверждена во многих разделах ***ГОСТ Р ИСО 31000—2019***. Таким образом, применение системы менеджмента риска позволяет, помимо прочего, реализовать один из принципов менеджмента качества: принятие решений на основе фактических данных.

*Кроме того, первая часть **раздела 7 ГОСТ Р ИСО 9001—2015** (подразделы 7.1, 7.2 и 7.3), хоть и не содержит явных ссылок на менеджмент риска, была истолкована с этой позиции, с целью предоставления ресурсов (персонала, инфраструктуры и рабочей среды), позволяющих использовать возможности и избегать нежелательных событий для достижения главной цели — удовлетворения потребностей все большего числа потребителей, а также других соответствующих заинтересованных сторон. Персонал должен обладать необходимой компетентностью и ресурсами, чтобы держать под контролем риски, связанные с его деятельностью. Весь персонал был проинформирован обо всех видах рисков, с которыми они сталкиваются, и об их вкладе в достижение целей организации.*

*Выбор ресурсов для мониторинга и измерений (**ГОСТ Р ИСО 9001—2015**, пункт 7.1.5 и подраздел 9.1), их метрологические характеристики, межповерочные интервалы и т. д. устанавливались с учетом всех связанных с ними рисков, результатов предыдущих мероприятий по мониторингу и измерениям, а также принимая во внимание не только угрозы и опасности, но и возможности, которыми следует воспользоваться. Это касается важности проведения или отсутствия определенных измерений, требуемых допусков, допустимой погрешности измерений, возможности отклонения показаний прибора в промежутке от одной калибровки до другой, а также степени детализации записей. Решения по всем аспектам были выработаны с учетом оценки рисков и анализа эффективности затрат и пользы.*

*Деятельность на стадиях жизненного цикла продукции и услуг (**ГОСТ Р ИСО 9001—2015**, раздел 8) является ключевым разделом, и менеджмент риска строго применялся при внедрении требований, описанных в **ГОСТ Р ИСО 9001**. Установление требований к продукции и услугам, взаимоотношения с потребителями, а также проектирование и разработка продукции и услуг — все это влияло на рассмотрение связанных с ними возможностей и угроз.*

Риски, связанные с цепью поставок, являются особенно важным аспектом в компаниях, в которых часто используется аутсорсинг. Менеджмент риска считался ключевым видом деятельности, связанным с контролем процессов, продукции и услуг, поставляемых сторонними поставщиками процессов, товаров и услуг. Тип и степень управления, применяемого к стороннему поставщику и к предоставляемым сторонним поставщиком процессам, продукции и услугам, должны зависеть от их влияния на последующие производство и предоставление услуг.

Для создания управляемых условий для производства и предоставления услуг, а также всех связанных с ними аспектов (например, для идентификации и прослеживаемости, сохранения или управления изменениями), применение процесса менеджмента риска приобрело большое значение.

*Оценка результатов деятельности и повышение эффективности рассматривались с учетом мероприятий по мониторингу и пересмотру, описанных в **ГОСТ Р ИСО 31000—2019** подраздел 6.6), а также аспекта структуры, касающегося оценки эффективности и улучшения (**см. ГОСТ Р ИСО 31000—2019, подразделы 5.6 и 5.7**).*

*Документирование и отчетность (см. **ГОСТ Р ИСО 31000—2019**, подраздел 6.7) были внедрены в объеме, которого требовала фактическая необходимость учета и документирования менеджмента риска в зависимости от значимости риска.*

В процессе работы также учитывалось следующее.

Риски, связанные с качеством, могут повлиять на цели в нижеуказанных областях (примеры не являются исчерпывающими):

- обязательства по соблюдению качества продукции, услуг и функционированию;

- *конкуренция и конкуренты;*
- *успешность продукции и услуг, удовлетворенность потребителей и других заинтересованных сторон;*
- *стабильное качество продукции, услуг и процессов;*
- *устойчивый успех, имидж и репутация организации.*

В связи с этим на риски, связанные с качеством, могут влиять факторы неопределенности, которые могут возникать, например, в результате:

- инноваций в сфере продукции и технологических изменений;
- изменений в цепи поставок;
- обязательств по соответствию требованиям;
- мнений заинтересованных сторон относительно этики, принципов, ценностей организации и ожиданий;
- информационной безопасности;
- надежности инфраструктуры.

B.4 Внедрение других стандартов на системы менеджмента (MSS)

*Внедрение принципов, структуры и процессов, приведенных в **ГОСТ Р ИСО 31000** выявило, что следует отказаться от изолированного подхода к управлению организацией и соответствующими рисками в пользу более широкого, интегрированного. Руководитель организации и Совет директоров убедились в том, что пришло время следовать философии менеджмента риска на предприятии (ERM), которая учитывает все виды рисков и управляет ими комплексно и скоординировано.*

Часто риски затрагивают не одну, а многие области деятельности. В особых случаях возможности в одной области (например, в области качества) могут представлять собой угрозу для другой [например, в области защиты окружающей среды или охраны труда и здоровья (OH&S)] и наоборот. Это еще одна причина, почему лучше осуществлять менеджмент областей и соответствующих рисков комплексно и скоординировано, поддерживая необходимые компетенции в различных областях.

Такой комплексный подход также напомнил организации, что обработка риска может создавать новые риски или изменять существующие.

Это означает, что необходимо применять требовательный подход к оценке риска, к любому виду риска любого характера, который влияет на стратегические и оперативные цели. Это позволяет организации выявлять не только угрозы, но и те возможности, которые могут быть использованы для получения конкурентного преимущества. Это также является философией HLS для стандарта на системы менеджмента (MSS).

Большинство элементов, рассматриваемых для интеграции менеджмента риска в систему менеджмента качества (см. выше), целесообразны и применимы для менеджмента риска в других областях: защита окружающей среды и охрана труда и здоровья, а также информационная безопасность.

В некоторых MSS, например, ***ГОСТ Р ИСО 14001, ГОСТ Р ИСО/МЭК 27001*** и ***ГОСТ Р ИСО 45001***, содержатся требования к оценке и обработке риска. Организации преимущественно сосредотачиваются на управлении потенциальными угрозами и могут упускать из виду возможности, предоставляемые ситуацией.

Эти соображения привели к решению:

а) *создать единую «интегрированную систему менеджмента», охватывающую гармонично и скоординировано три области: качество, защита окружающей среды, безопасностью труда и охраной здоровья;*

б) *провести сертификацию по **ГОСТ Р ИСО 45001** к первой половине 2019 года;*

в) *возложить на руководителя направления QM ответственность и полномочия по координации создания, внедрения, поддержания и постоянного улучшения IMS со встроенной структурой и процессом менеджмента риска; QM также является руководителем, ответственным за поддержку всей организации в области менеджмента риска;*

г) *все владельцы процессов в организации также являются владельцами риска, т. е. имеют подотчетность и полномочия в области менеджмента риска в пределах сферы своей ответственности, а также предоставляют знания и навыки, относящиеся к конкретной области для поддержки QMS.*

Организация также рассмотрела следующие общепринятые концепции.

Риски, связанные с охраной окружающей среды, и риски, связанные с безопасностью труда и охраной здоровья (OH&S), — это те риски, на которые влияют или которые касаются вопросов, имеющих отношение к окружающей среде и безопасности труда и охране здоровья соответственно.

Риски, связанные с охраной окружающей среды, — это, главным образом, риски для окружающей среды, возникающие в связи с тем, что экологический аспект оказывает воздействие на окружающую среду.

Риски, связанные с безопасностью труда и охраной здоровья (OH&S), — это, главным образом, риски для здоровья и безопасности работников, возникающие в связи с тем, что опасное событие или воздействие, связанное с выполнением работы, причинит вред (травму или ущерб здоровью людей).

Неопределенность, как правило, проявляется в отношении оперативного контроля и механизмов, предназначенных для управления экологическими аспектами, а также аспектами техники безопасности и гигиены труда. Существует вероятность того, что средства управления/механизмы выйдут из строя или станут неэффективными, что может привести к неблагоприятному воздействию/нежелательному эффекту.

Риски, связанные с окружающей средой и с техникой безопасности и гигиеной труда, также относятся к категории рисков для организации, возникающих из-за неопределенности того, что проблемы или вопросы, связанные с окружающей средой или техникой безопасности и гигиеной труда, могут вызвать одно или несколько последствий, как неблагоприятных, так и благоприятных. Эти риски могут касаться следующих вопросов (но не ограничиваться ими):

- обязательства по соблюдению нормативно-правовых требований, ответственность за качество продукции, судебные издержки и расходы, связанные с травмами;
- благополучие, работоспособность или производительность труда работников;
- разрешение на строительство и текущую деятельность организации;
- имидж и репутация организации, а также доверие к бизнесу организации;
- конкуренция и конкуренты;
- изменчивость погоды и изменение климата;
- ущерб от природных явлений, который также может включать в себя неблагоприятное воздействие на окружающую среду;
- устойчивость бизнеса.

B.5 Интеграция со стандартом на менеджмент информационной безопасности (MSS) *(ГОСТ Р ИСО/МЭК 27001)*

Организация взяла на себя новые задачи, возникающие в результате глобализации и цифровой трансформации, которые побуждают предприятия использовать деловые возможности, предлагаемые новыми рынками и новыми информационно-коммуникационными технологиями. Руководители организации отдавали себе отчет в том, что изменения, связанные с использованием новых возможностей, могут создавать другие угрозы и другие возможности практически для всех областей, рассматриваемых в рамках системы менеджмента. Осознание того, что риски, связанные с информационной безопасностью, влияют на среду организации, стало причиной поиска возможностей для улучшения информационной безопасности.

Структурированное и систематическое применение процесса менеджмента риска привело организацию к внедрению технологии Industry 4.0 и Internet of Things (IoT), а также плана цифровых инноваций.

Примеры факторов, которые необходимо учитывать в этом контексте включают в себя внедрение, замену или реконфигурацию средств информационного обеспечения и технического оснащения или оборудования (анализ данных большого объема, искусственный интеллект, а также облако и GPS, там, где это необходимо) для мониторинга и управления:

- производственными процессами, с целью повышения результативности, обеспечения сбалансированных потоков материалов и полуфабрикатов, а также результативности (дефектности конечной продукции);
- жизненным циклом продукции для улучшения менеджмента цепи поставок (в том числе и менеджмент риска);
- инфраструктурой производства для проведения профилактического технического обслуживания при частичной или полной замене традиционных процессов технического обслуживания (оперативное техническое обслуживание может быть дорогостоящим и опасным);
- устройством и инфраструктурой для обеспечения охраны труда и безопасности здоровья (OH&S), а также средствами индивидуальной защиты (носимых) для осуществления мониторинга и управления в режиме реального времени для улучшения условий труда и самочувствия;
- экологических аспектов.

Учитывая, что внедрение новых информационно-коммуникационных технологий привело к необходимости управления рисками, связанными с новыми технологиями, было принято решение также внедрить положения ***ГОСТ Р ИСО/МЭК 27001****. Высшее руководство организации руководствовалось следующими положениями*:

а) *в контексте систем менеджмента информационной безопасности риски информационной безопасности могут быть определены как влияние неопределенности на цели информационной безопасности;*

б) *риски информационной безопасности связаны с возможностью того, что угрозы будут использовать уязвимости и тем самым причинят вред организации;*

в) *цели информационной безопасности связаны с основными последствиями инноваций в следующих областях:*

г) *результативность управления организацией, поскольку она основана на пирамиде DIKW data, information, knowledge and wisdom (т. е. данные, информация, знания, вместе с методами применения, средствами обеспечения и системами для их обработки);*

д) *уверенность в том, что информация организации надлежащим образом и на постоянной основе защищена от угроз (сбоев и/или кибератак);*

е) *имидж и репутация, связанные со способностью организации защищать персональные данные, данные и ноу-хау потребителей, а также свои собственные данные;*

ж) *сохранение качества информации связано со следующими требованиями информационной безопасности:*

1) *конфиденциальность (свойство, заключающееся в том, что информация не предоставляется и не разглашается неуполномоченным лицам, организациям или процессам),*

2) *целостность (свойство, при котором информация является точной и полной),*

3) *доступность информации (свойство быть доступной и пригодной к использованию по требованию уполномоченного субъекта),*

4) *устойчивость бизнеса.*

Существуют также некоторые важные и косвенные воздействия информационной безопасности на цели других «областей» в рамках деятельности организации.

Когда организация решила воспользоваться возможностями, предоставляемыми новыми технологиями, связанными с информационно-коммуникационными технологиями, потенциальные ожидаемые выгоды были в следующих областях:

- *защита окружающей среды;*
- *предотвращение производственного травматизма и причинения вреда здоровью;*
- *повышение производительности труда и качества предлагаемых продукции и услуг;*
- *повышение эффективности организации с точки зрения трех основных показателей (люди, планета и прибыль).*

Все возможности, предоставляемые новыми информационно-коммуникационными технологиями, создают ряд серьезных угроз, которые наряду с уязвимостями аппаратного и программного обеспечения потенциально могут привести к возникновению новых рисков, связанных с информационно-коммуникационными технологиями. В этой связи организация должна определить необходимость создания, внедрения, поддержания в рабочем состоянии и постоянного улучшения системы менеджмента информационной безопасности в соответствии с требованиями ***ГОСТ Р ИСО/МЭК 27001***.

В.6 Выводы

Применение менеджмента риска в системах менеджмента, основанное на требованиях одного или нескольких MSS, в соответствии с ***ГОСТ Р ИСО 31000***, должно быть в центре внимания организации.

Реализация этого проекта оказалась выигрышным выбором.

Это было сделано для интеграции концепций из разных областей в одной системе управления. Проект представляет собой пример принятия целостного подхода, использующего преимущества синергии, обеспечиваемой интеграцией руководящих принципов ***ГОСТ Р ИСО 31000*** и требований некоторых MSS (таких как ***ГОСТ Р ИСО 9001, ГОСТ Р ИСО 14001, ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО 45001***).

Для управления всеми рисками, связанными с возможностями и угрозами, следует применять систематический, всеобъемлющий и актуальный подход, поскольку это помогает организации достигать стратегических бизнес-целей, одновременно создавая и защищая ценность для всех соответствующих заинтересованных сторон.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных национальных стандартов международным стандартам, использованным в качестве ссылочных в примененном международном документе

Таблица ДА.1

Обозначение и наименование ссылочного национального стандарта	Степень соответствия	Обозначение и наименование ссылочного международного стандарта
ГОСТ Р ИСО 31000—2019	IDT	ISO 31000:2018 «Менеджмент риска. Принципы и руководство»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:
- IDT — идентичный стандарт.

Приложение ДБ
(справочное)

Сопоставление структуры настоящего стандарта со структурой примененного в нем международного документа

Таблица ДБ.1

Структура настоящего стандарта			Структура международного документа IWA 31:2020		
Разделы	Пункты	Подпункты	Разделы	Пункты	Подпункты
Приложения		A	Приложения		A
		B			B
		—			C
		ДА			—
		ДБ			—

Примечание — Сопоставление структуры стандартов приведено начиная с приложения А, т. к. предыдущие разделы стандартов и их иные структурные элементы (за исключением предисловия) идентичны.

Библиография

[1] ISO Handbook. The Integrated Use of Management System Standards (IUMSS), 2018. Доступно по адресу: https://www.iso.org/publication/PUB100435.html (дата обращения: 11 августа 2025 г.)

УДК 658.5.011:006.354 ОКС 03.100.01

Ключевые слова: менеджмент риска, управление организацией, системы менеджмента

Редактор *М.В. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *Р.А. Ментова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 03.09.2025. Подписано в печать 18.09.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов, 117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru