ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 71440— 2024

Информационные технологии

ОЦЕНКА ПРОЦЕССОВ

Руководство по определению рисков в процессах

(ISO/IEC TR 33015:2019, NEQ)

Издание официальное

Москва
Российский институт стандартизации
2024

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) и Комиссией Российской академии наук по техногенной безопасности

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 7 июня 2024 г. № 740-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного документа ISO/IEC TR 33015:2019 «Информационные технологии. Оценка процесса. Руководство по определению риска процесса» (ISO/IEC TR 33015:2019 «Information technology — Process assessment — Guidance for process risk determination», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

*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 (*gost.e-ecolog.ru

© ISO, 2019
© IEC, 2019
© Оформление. ФГБУ «Институт стандартизации», 2024

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 4
4 Общие сведения 6
4.1 Определение рисков, связанных с процессами 6
4.2 Цели и ожидаемые результаты определения рисков 7
4.3 Значимость результатов определения рисков в процессе 8
5 Процесс определения рисков 8
5.1 Примерные шаги для определения рисков 8
5.2 Порядок определения рисков в процессе 9
6 Рекомендации по определению рисков в процессах 11
6.1 Инициирование определения рисков 11
6.2 Определение исходных целей и данных для оценки 12
6.3 Определение профиля процесса 13
6.4 Принципы определения рисков в процессе 16
6.5 Оценка рисков, связанных с процессами 17
6.6 Использование определения рисков для выбора поставщика 18
6.7 Сопоставимость результатов оценки 19
Приложение А (справочное) Пример классификации типов рисков 20
Приложение Б (справочное) Пример качественной оценки рисков, связанных с процессами 23
Приложение В (справочное) Пример формирования профиля процесса 26
Приложение Г (справочное) Типовые показатели, модели и методы прогнозирования рисков 29
Приложение Д (справочное) Рекомендации по определению допустимых значений рисков 35

Введение

Настоящий стандарт может быть использован самостоятельно, а также во взаимосвязи с другими национальными стандартами в области системной и программной инженерии и оценки процессов, призванных обеспечить согласованную основу качества процессов. В настоящем стандарте рассматриваются процессы жизненного цикла систем по ГОСТ Р 57193, а также иные процессы, применимые в жизненном цикле систем, включая оказание услуг. Результаты могут быть применены либо в целях повышения эффективности выполнения процессов, либо для выявления и анализа рисков, связанных с применением процессов.

Примечание — Как частный случай в качестве рассматриваемой системы может выступать организация, выпускающая продукцию или оказывающая услуги. В рамках организации выполняются различные процессы, подлежащие оценке.

В состав рекомендаций, связанных с определением рисков в процессах, входят:

- инициирование определения рисков в процессе;
- определение исходных целей и данных для оценки;
- определение профиля процесса;
- принципы определения рисков в процессе;
- оценка рисков, связанных с процессами;
- использование определения рисков в процессе для выбора поставщика;
- сопоставление результатов оценки.

Цель разработки настоящего стандарта состоит в обеспечении оценки различных показателей рисков при выполнении процессов, применяемых в жизненном цикле систем.

Настоящий стандарт предназначен для применения сторонами, заинтересованными в определении рисков в процессах, а также специалистами оценивающих организаций и разработчиками методов и инструментариев, поддерживающих оценку процессов и системный анализ рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

ОЦЕНКА ПРОЦЕССОВ

Руководство по определению рисков в процессах

Information technologies.
Processes assessment.
Guidance for processes risk determination

Дата введения — 2024—09—30

1 Область применения

Настоящий стандарт содержит руководство по определению рисков в процессах, применимое в рамках любых вариантов отношений между заказчиком и поставщиком, а также для любой организации, желающей определить риски при выполнении процессов.

Настоящий стандарт предназначен для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем различного функционального назначения и программных средств, а также при выведении их из эксплуатации.

Примечание — Настоящий стандарт не содержит рекомендаций по конкретным организационным структурам, критериям управления, моделям жизненного цикла или методам разработки и выполнения процессов.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ IEC 61508-3 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 3. Требования к программному обеспечению

ГОСТ Р 27.101—2021 Надежность в технике. Надежность выполнения задания и управление непрерывностью деятельности. Термины и определения

ГОСТ Р 51897 (ISO Guide 73:2009) Менеджмент риска. Термины и определения

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 51901.7/ISO/TR 31004:2013 Менеджмент риска. Руководство по внедрению ИСО 31000

ГОСТ Р 51901.16 (МЭК 61164:2004) Менеджмент риска. Повышение надежности. Статистические критерии и методы оценки

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

ГОСТ Р 57193 Системная и программная инженерия. Процессы жизненного цикла систем

ГОСТ Р 58494 Оборудование горно-шахтное. Многофункциональные системы безопасности угольных шахт. Система дистанционного контроля опасных производственных объектов

ГОСТ Р 58771 Менеджмент риска. Технологии оценки риска

ГОСТ Р 59329—2021 Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы

ГОСТ Р 59330—2021 Системная инженерия. Защита информации в процессе управления моделью жизненного цикла системы

Издание официальное

ГОСТ Р 59331—2021 Системная инженерия. Защита информации в процессе управления инфраструктурой системы

ГОСТ Р 59332—2021 Системная инженерия. Защита информации в процессе управления портфелем проектов

ГОСТ Р 59333—2021 Системная инженерия. Защита информации в процессе управления человеческими ресурсами системы

ГОСТ Р 59334—2021 Системная инженерия. Защита информации в процессе управления качеством системы

ГОСТ Р 59335—2021 Системная инженерия. Защита информации в процессе управления знаниями о системе

ГОСТ Р 59336—2021 Системная инженерия. Защита информации в процессе планирования проекта

ГОСТ Р 59337—2021 Системная инженерия. Защита информации в процессе оценки и контроля проекта

ГОСТ Р 59338—2021 Системная инженерия. Защита информации в процессе управления решениями

ГОСТ Р 59339—2021 Системная инженерия. Защита информации в процессе управления рисками для системы

ГОСТ Р 59340—2021 Системная инженерия. Защита информации в процессе управления конфигурацией системы

ГОСТ Р 59341—2021 Системная инженерия. Защита информации в процессе управления информацией системы

ГОСТ Р 59342—2021 Системная инженерия. Защита информации в процессе измерений системы

ГОСТ Р 59343—2021 Системная инженерия. Защита информации в процессе гарантии качества для системы

ГОСТ Р 59344—2021 Системная инженерия. Защита информации в процессе анализа бизнеса или назначения системы

ГОСТ Р 59345—2021 Системная инженерия. Защита информации в процессе определения потребностей и требований заинтересованной стороны для системы

ГОСТ Р 59346—2021 Системная инженерия. Защита информации в процессе определения системных требований

ГОСТ Р 59347—2021 Системная инженерия. Защита информации в процессе определения архитектуры системы

ГОСТ Р 59348—2021 Системная инженерия. Защита информации в процессе определения проекта

ГОСТ Р 59349—2021 Системная инженерия. Защита информации в процессе системного анализа

ГОСТ Р 59350—2021 Системная инженерия. Защита информации в процессе реализации системы

ГОСТ Р 59351—2021 Системная инженерия. Защита информации в процессе комплексирования системы

ГОСТ Р 59352—2021 Системная инженерия. Защита информации в процессе верификации системы

ГОСТ Р 59353—2021 Системная инженерия. Защита информации в процессе передачи системы

ГОСТ Р 59354—2021 Системная инженерия. Защита информации в процессе аттестации системы

ГОСТ Р 59355—2021 Системная инженерия. Защита информации в процессе функционирования системы

ГОСТ Р 59356—2021 Системная инженерия. Защита информации в процессе сопровождения системы

ГОСТ Р 59357—2021 Системная инженерия. Защита информации в процессе изъятия и списания системы

ГОСТ Р 59853 Информационные технологии. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения

ГОСТ Р 59989—2022 Системная инженерия. Системный анализ процесса управления качеством системы

ГОСТ Р 59990—2022 Системная инженерия. Системный анализ процесса оценки и контроля проекта

ГОСТ Р 59991—2022 Системная инженерия. Системный анализ процесса управления рисками для системы

ГОСТ Р 59992—2022 Системная инженерия. Системный анализ процесса управления моделью жизненного цикла системы

ГОСТ Р 59993—2022 Системная инженерия. Системный анализ процесса управления инфраструктурой системы

ГОСТ Р 59994—2022 Системная инженерия. Системный анализ процесса гарантии качества для системы

ГОСТ Р ИСО 9000 Системы менеджмента качества. Основные положения и словарь

ГОСТ Р ИСО 13379-1 Контроль состояния и диагностика машин. Методы интерпретации данных и диагностирования. Часть 1. Общее руководство

ГОСТ Р ИСО 13381-1 Контроль состояния и диагностика машин. Прогнозирование технического состояния. Часть 1. Общее руководство

ГОСТ Р ИСО 17359 Контроль состояния и диагностика машин. Общее руководство

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 15026 Информационная технология. Уровни целостности систем и программных средств

ГОСТ Р ИСО/МЭК 15026-4 Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 4. Гарантии жизненного цикла

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

ГОСТ Р ИСО/МЭК 33001 Информационные технологии. Оценка процесса. Понятия и терминология

ГОСТ Р ИСО/МЭК 33002 Информационные технологии. Оценка процесса. Требования к проведению оценки процесса

ГОСТ Р ИСО/МЭК 33003 Информационные технологии. Оценка процесса. Требования к системе измерения процесса

ГОСТ Р ИСО/МЭК 33004 Информационные технологии. Оценка процесса. Требования к эталонным моделям процесса, моделям оценки процесса и моделям зрелости

ГОСТ Р ИСО/МЭК 33020—2017 Информационные технологии. Оценка процесса. Система измерения процесса для оценки возможностей процесса

ГОСТ Р МЭК 61069-1 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 1. Терминология и общие концепции

ГОСТ Р МЭК 61069-2 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 2. Методология оценки

ГОСТ Р МЭК 61069-3 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 3. Оценка функциональности системы

ГОСТ Р МЭК 61069-4 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 4. Оценка производительности системы

ГОСТ Р МЭК 61069-5 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 5. Оценка надежности системы

ГОСТ Р МЭК 61069-6 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 6. Оценка эксплуатабельности системы

ГОСТ Р МЭК 61069-7 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 7. Оценка безопасности системы

ГОСТ Р МЭК 61069-8 Измерение, управление и автоматизация промышленного процесса. Определение свойств системы с целью ее оценки. Часть 8. Оценка других свойств системы

ГОСТ Р МЭК 61508-1 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 1. Общие требования

ГОСТ Р МЭК 61508-2 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 2. Требования к системам

ГОСТ Р МЭК 61508-4 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 4. Термины и определения

ГОСТ Р МЭК 61508-5 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 5. Рекомендации по применению методов определения уровней полноты безопасности

ГОСТ Р МЭК 61508-6 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 6. Руководство по применению ГОСТ Р МЭК 61508-2 и ГОСТ Р МЭК 61508-3

ГОСТ Р МЭК 61508-7 Функциональная безопасность систем электрических, электронных, программируемых электронных, связанных с безопасностью. Часть 7. Методы и средства

ГОСТ Р МЭК 62264-1 Интеграция систем управления предприятием. Часть 1. Модели и терминология

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.

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 27.101, ГОСТ Р 59853, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 33001, ГОСТ Р 51897, ГОСТ Р 59989, ГОСТ Р 59991, ГОСТ Р 59994, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, а также следующие термины с соответствующими определениями:

3.1

вероятностное пространство: Тройка, состоящая из пространства элементарных событий, заданной на нем сигма-алгебры событий и вероятностной меры.

[ГОСТ Р ИСО 3534-1—2019, пункт 2.68]

3.2

вероятность события: Действительное число из замкнутого промежутка [0, 1], приписываемое событию.

[ГОСТ Р ИСО 3534-1—2019, пункт 2.5]

Примечание — Вероятность события оценивается с помощью вероятностной меры, устанавливаемой в рамках вероятностного пространства.

3.3

допустимый риск: Риск, который в данной ситуации считают приемлемым при существующих общественных ценностях.

[ГОСТ Р 51898—2002, пункт 3.7]

3.4

качество используемой информации в системе: Совокупность свойств используемой информации, обусловливающих ее пригодность для последующего использования в соответствии с целевым назначением в системе.

[ГОСТ Р 59341—2021, пункт 3.1.13]

3.5

качество функционирования системы: Совокупность свойств, обусловливающих пригодность системы в соответствии с ее целевым назначением.

[ГОСТ Р 59341—2021, пункт 3.1.14]

3.6

моделируемая система: Система, для которой решение задач системного анализа осуществляется с использованием ее формализованной модели, позволяющей исследовать критичные сущности системы в условиях ее создания и/или применения, учитывающей структурные связи между переменными или постоянными элементами формализованного представления, задаваемые условия и ограничения.

Примечание — В качестве модели системы могут выступать формализованные сущности, объединенные целевым назначением. Например, при проведении системного анализа в принимаемых допущениях, ограничениях и предположениях модель может формально описывать функциональные подсистемы и элементы, процессы, реализуемые действия, множество активов и/или выходных результатов или множество этих или иных сущностей в их целенаправленном применении в задаваемых условиях.

[ГОСТ Р 59994—2022, пункт 3.1.4]

3.7 **модель рассматриваемой системы:** Формализованное описание реальной рассматриваемой системы с предположениями и допущениями, позволяющее исследовать критичные сущности этой системы в условиях ее создания и/или применения, учитывающей структурные связи между переменными или постоянными элементами формализованного представления, задаваемые условия и ограничения.

3.8

ограничение: Составная часть требования или самостоятельное требование, описывающие внешнее ограничивающее условие (связанное с внешними по отношению к объекту воздействующими факторами), наложенное на объект, его конструкцию, процесс разработки, изготовления, эксплуатации, ремонта или утилизации.

[ГОСТ Р 59194—2020, пункт 3.1.14]

3.9 **определение рисков в процессе:** Систематическая оценка и анализ выбранных процессов в соответствии с профилем процесса, проводимые с целью выявления рисков, связанных с процессом, для выполнения конкретного установленного требования.

3.10

риск: Влияние неопределенности на достижение поставленных целей.

Примечание 1 — Под влиянием неопределенности понимается отклонение от ожидаемого результата. Оно может быть положительным и/или отрицательным, может создавать или приводить к возникновению возможностей и угроз.

Примечание 2 — Цели могут иметь различные аспекты и категории и определяться на различных уровнях.

Примечание 3 — Риск часто выражается через его источники, потенциальные события, их последствия и вероятность.

[ГОСТ Р 51897—2021, статья 2.1]

3.11 **риск, связанный с процессом:** Риск, возникающий из-за недостатков в выполнении, менеджменте или развертывании процесса.

3.12

системная инженерия (systems engineering): Междисциплинарный подход, управляющий полным техническим и организаторским усилием, требуемым для преобразования ряда потребностей заинтересованных сторон, ожиданий и ограничений в решение и для поддержки этого решения в течение его жизни.

[ГОСТ Р 57193—2016, пункт 4.1.47]

3.13

система-эталон: Реальная или гипотетичная система, которая по своим интегральным показателям прогнозируемых рисков нарушения качества и/или безопасности принимается в качестве эталона для полного удовлетворения требований заинтересованных сторон рассматриваемой системы и рационального решения задач системного анализа.

[Адаптировано из ГОСТ Р 59343—2021, пункт 3.1.14]

3.14

системный анализ процесса управления рисками для системы: Научный метод системного познания, предназначенный для решения практических задач системной инженерии путем представления рассматриваемых системных процессов, системы и/или соответствующего проекта в виде приемлемой моделируемой системы.

Примечания

1 Метод включает:

- измерение и оценку специальных показателей, связанных с критичными сущностями рассматриваемой системы, прогнозирование рисков, интерпретацию и анализ приемлемости получаемых результатов для рассматриваемых системных процессов, системы (и/или ее элементов) и/или проекта;
- определение с использованием моделирования существенных угроз и условий, способных при том или ином развитии событий негативно повлиять на свойства рассматриваемых системных процессов, системы (и/или ее элементов) и/или проекта;
- обоснование с использованием моделирования упреждающих мер противодействия угрозам, обеспечивающих желаемые свойства рассматриваемых процесса, системы (и/или ее элементов) и/или проекта при задаваемых ограничениях в задаваемый период времени;
- обоснование с использованием моделирования предложений по обеспечению и повышению качества, безопасности и/или эффективности рассматриваемой системы (и/или ее элементов) и достижению целей системной инженерии при задаваемых ограничениях в задаваемый период времени.

2 К специальным критичным сущностям системы могут быть отнесены отдельные характеристики (например, физические параметры, характеристики качества, безопасности, размеры, стоимость), достигаемые эффекты, выполняемые функции, действия или защищаемые активы. При этом в состав рассматриваемых могут быть включены характеристики, эффекты, функции, действия и активы, свойственные не только самой системе, но и иным системам (подсистемам), не вошедшим в состав рассматриваемой системы. Например, это могут быть характеристики, эффекты, функции, действия и активы, свойственные обеспечивающим системам, привлекаемым информационным системам и/или базам данных, охватываемым по требованиям заказчика.

[ГОСТ Р 59991—2022, пункт 3.1.9]

3.15 **системный аналитик:** Специалист, обладающий знаниями и компетенциями, необходимыми для решения задач системного анализа.

3.16

требование: Требуемая (ожидаемая) количественная или качественная характеристика или свойство объекта, а также связанные ограничения и условия.

[ГОСТ Р 59194—2020, пункт 3.1.21]

3.17

целостность моделируемой системы: Состояние моделируемой системы, которое отвечает целевому назначению модели системы в течение задаваемого периода прогноза.

[ГОСТ Р 59991—2022, пункт 3.1.10]

4 Общие сведения

4.1 Определение рисков, связанных с процессами

Цель оценки процессов состоит в понимании текущего и прогнозного состояния процессов, существующих в организации или применяемых в жизненном цикле рассматриваемых систем. Результаты оценки процесса могут быть применены в целях повышения эффективности выполнения процессов либо для выявления и проработки количественной и/или качественной оценки рисков, связанных с выполнением процессов (см. ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994).

Основное внимание в настоящем стандарте уделено использованию результатов оценки процессов для выявления рисков, связанных с процессами, определения их значимости для конкретного требования или категории требований системной инженерии, анализа профилей процессов. Это может быть использовано для снижения рисков или в качестве помощи при принятии решений. Классификация типов рисков, связанных с процессами, существующими в организации, их качественная оценка и профили процессов представлены в приложениях А — В.

Качественная оценка рисков, связанных с процессами, по результатам оценки процесса основана на сопоставлении слабых и сильных сторон. Слабые стороны представлены оценками свойств процесса, которые отличаются от полного достижения целей. Путем сравнения достижения рейтингов свойств процесса с профилем процесса выявляются недостатки, которые могут свидетельствовать о наличии одного или нескольких конкретных рисков.

Примечания

1 Конкретное требование или категория требований может подразумевать развертывание процессов организации в отношении новой или существующей задачи, договора, категории договоров или внутреннего обязательства, продукта или услуги, или любого другого требования системной инженерии. Конкретное требование или категория требований определяет цель(и) определения рисков в процессе.

2 Определение рисков в процессе по-возможности должно учитывать все критичные угрозы и условия, куда могут входить стратегические, организационные, финансовые, кадровые и многие другие факторы и ограничения.

Количественная оценка рисков, связанных с процессами в жизненном цикле рассматриваемых систем, основана на применении математических моделей, позволяющих осуществлять прогнозирование рисков (см. приложения Г, Д). Возможные показатели, модели, методы и рекомендации по количественной оценке рисков приведены в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7. Примеры количественного прогнозирования рисков и решения задач системного анализа приведены в ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Примечание — С учетом специфики системы для количественной оценки рисков допускается использование любых научно обоснованных методов и моделей, обеспечивающих достижение целей.

Соответствие базовой области оценки конкретному требованию или категории требований системной инженерии будет влиять на значимость результатов определения рисков в процессе. При оценке процессов в отношении данной характеристики качества процесса в ГОСТ Р ИСО/МЭК 33002 рекомендовано определение контекста процесса как части области оценки. Контекст процесса описывает отношения и зависимости между применением набора процессов и их влиянием на выпускаемую продукцию, оказываемую услугу или на организацию разработчика. Согласование объема оценки с конкретным требованием или категорией требований выполняется относительно влияния содержимого выбранных процессов на исследуемые риски и сопоставимости контекста процесса с предполагаемым его применением.

Оценку конкретного процесса проводят специально для определения рисков, связанных с этим процессом, или выбирают из набора уже существующих результатов.

В первом случае целевая область оценки, включающая контекст процесса, должна быть определена в качестве исходных данных для оценки (см. 6.3). Если результаты выбирают из набора уже существующих результатов, необходимо провести специальный анализ и убедиться в значимости выбранного результата оценки.

В любом случае в отношении данного контекста процесса следует определить профиль процесса с желаемым уровнем качества (например, в отношении разработки конкретной системы). Согласно 4.3.2 целевой уровень качества процесса следует задавать с учетом существующих конкретных требований к определению рисков, соблюдая тем самым соответствие конкретным типам рисков, подлежащих системному анализу (см. ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994).

4.2 Цель и ожидаемые результаты определения рисков

Целью определения рисков в конкретном процессе является выявление существенных угроз и рисков, связанных с применением этого процесса, и определение значимости выявленных рисков для системы, конкретного требования или категории требований системной инженерии (см. В.2.3).

В итоге успешного определения рисков в процессе достигаются следующие результаты:

- установлена связь рисков с конкретным требованием или категорией требований;
- определены виды оцениваемых рисков, соответствующие конкретному требованию или категории требований системной инженерии (если применимо);
- определены исходные цели и данные для оценки, включая объем оценки и контекст процесса;

- установлен профиль процесса в соответствии с исходными целями оценки и определения риска в процессе;

- определены уровни качества процесса в соответствии с контекстом процесса и выбранным профилем процесса;

- проведен анализ любых расхождений между целевыми и оцененными характеристиками качества процесса;

- проведен анализ конкретных типов рисков, связанных с процессом.

Примечание — Определения уровней качества процессов и типовых показателей рисков приведены в ГОСТ Р ИСО/МЭК 33002, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994.

4.3 Значимость результатов определения рисков в процессе

4.3.1 Влияние объема оценки и контекста процесса на результаты определения рисков

Недопустимые нарушения реализации процесса в сравнении с выбранным эталоном процесса (или системой-эталоном) для модели рассматриваемой системы или модели процесса могут служить причиной возникновения конкретных рисков в процессе. Для каждого типа риска определяют соответствующий объем оценки, включая определенный контекст процесса в рассматриваемой системе.

Если оценку проводят специально для определения рисков, связанных с процессом, или если результат оценки выбирают из набора имеющихся вариантов, изначальный объем оценки, включая контекст процесса, будет оказывать влияние на значимость результатов для рассматриваемой системы.

По результатам оценки определяют типы рисков, на которые следует обратить внимание в соответствии с конкретным требованием или категорией требований системной инженерии. В зависимости от выявленного типа риска следует определить соответствующий целевой объем оценки, который может послужить основой для определения профиля возможностей процесса для рассматриваемой системы. Пример классификации типов рисков, связанных с процессами, приведен в приложении А.

4.3.2 Категоризация рисков, связанных с процессом

Типы рисков определяют согласно целям определения рисков в процессах для рассматриваемой системы. Они связаны с применением процессов для выполнения конкретного требования или категории требований системной инженерии.

Для конкретного требования типы рисков, связанных с конкретным процессом, можно группировать в категории. Сделать это можно путем сопоставления выявленных основных причин высокого риска с недостатками выполняемого процесса для рассматриваемой системы (см. приложение А). При рассмотрении конкретного типа риска для рассматриваемой системы необходимо определить исходные цели и данные для оценки, профиля процесса и критерии для сбора информации.

4.3.3 Определение рекомендаций по рейтингу

Конкретные рекомендации по рейтингу, включая критерии сбора информации, могут быть разработаны заинтересованными сторонами для обеспечения понимаемости используемой логики рейтингования и улучшения сопоставимости результатов определения рисков в процессе (см. 6.5—6.7).

5 Процесс определения рисков

5.1 Примерные шаги для определения рисков

Примерные шаги для определения рисков в процессе с использованием рекомендаций ГОСТ Р ИСО/МЭК 33002 по оценке процесса отражены на рисунке 1.

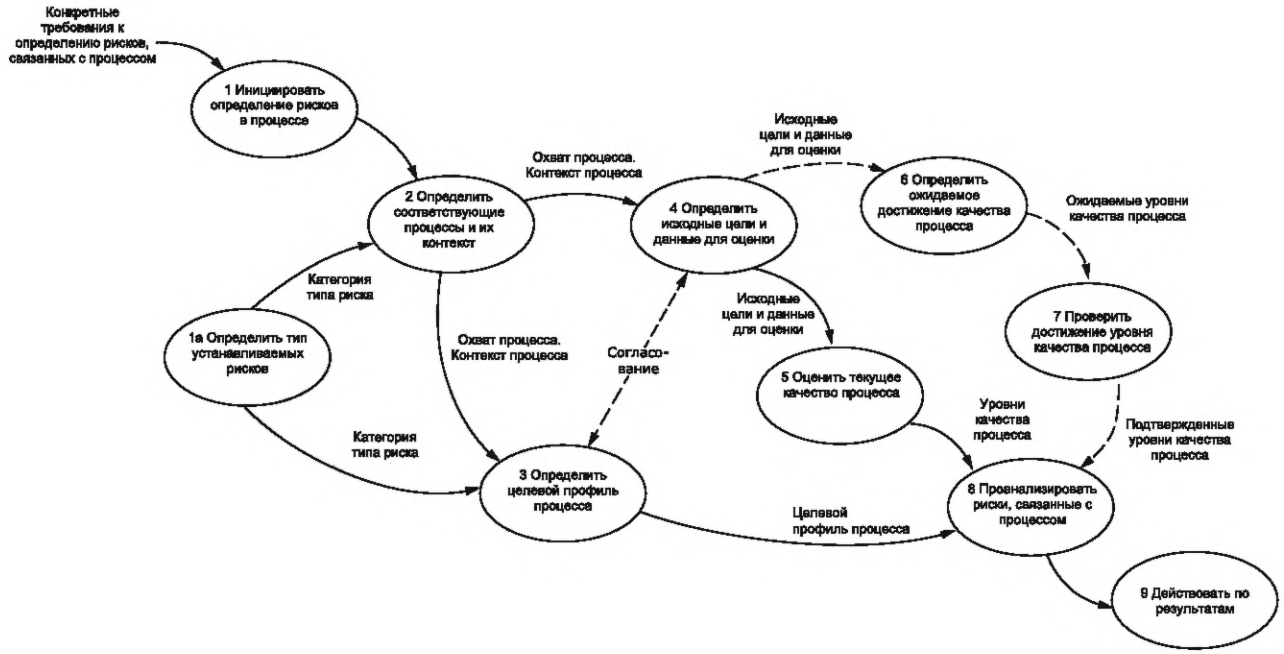


Рисунок 1 — Примерные шаги для определения рисков в процессе

Овалы на рисунке 1 представляют собой шаги в процессе, а стрелки — информацию, передаваемую между этими шагами.

5.2 Порядок определения рисков в процессе

5.2.1 Шаг 1. Инициировать определение рисков в процессе

Необходимо разработать и утвердить план определения рисков в процессе для рассматриваемой системы. Его применяют для мониторинга достигнутых результатов. В плане должно быть отражено следующее:

- цель определения рисков в процессе;
- используемый метод оценки процесса;
- охват оценки (так, в приложении к организации охват оценки характеризуется организационными единицами, чьи процессы должны стать предметом определения рисков);
- профиль процесса (добавляется после его определения на шаге 3);
- основные роли и обязанности;
- ресурсы;
- соответствующие этапы, точки контроля и механизмы отчетности.

Чтобы привести область оценки в соответствие с конкретным требованием или категорией требований системной инженерии в отношении влияния выбранных процессов на исследуемые риски, а также обеспечить сопоставимость контекста процессов с предполагаемым их применением для конкретного требования или категории требований, системными аналитиками может быть осуществлена категоризация рисков (см. приложение А).

5.2.2 Шаг 2. Определить соответствующие процессы и их контекст

Системные аналитики определяют соответствующие процессы и связанные с ними эталонные и оценочные модели процессов, а также контекст предполагаемого применения процессов для конкретного требования или категории требований системной инженерии (см. 6.3).

5.2.3 Шаг 3. Определить целевой профиль процесса

Профиль процесса в рассматриваемой системе определяют системные аналитики (см. 6.4). Профиль процесса может включать набор целевых профилей, отражающих достаточное качество процесса для выполнения заданного требования с учетом допустимых рисков, связанных с процессом (степень достаточности подлежит научному обоснованию с использованием математического моделирования системы или процесса в системе).

5.2.4 Шаг 4. Определить исходные цели и данные для оценки

Необходимо определить исходные цели и данные для определения рисков в рассматриваемой системе, связанные с процессом. Этот шаг может быть выполнен также путем выбора из набора существующих вариантов оценки (см. 6.3).

Исходные цели и данные для оценки процесса содержат следующее:

- характеристику качества процесса и систему измерения процесса (см. 6.3.2);
- эталон процесса и модель процесса (для качественной оценки рисков) или систему-эталон, математическую модель рассматриваемой системы (для количественного прогнозирования рисков) (определены на шаге 2);
- идентифицированные процессы и контекст процесса (определены на шаге 2) в соответствии с профилем процесса (определен на шаге 3);
- критерии сбора информации (см. 6.5.3).

Исходные цели и данные для оценки могут также содержать конкретные правила оценки или рекомендации согласно описанию в 6.5.4.

Дополнительные рекомендации приведены в 6.3.

5.2.5 Шаг 5. Оценить текущее качество процесса

Необходимо провести оценку качества процесса по ГОСТ Р ИСО/МЭК 33002, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994 на основе определенных исходных целей и данных для оценки. Результат качественной оценки достижения текущих характеристик процесса может иметь, например, форму набора профилей процесса по ГОСТ Р ИСО/МЭК 33002.

Дополнительные рекомендации см. в 6.5.

5.2.6 Шаг 6. Определить ожидаемое достижение качества процесса

Определение степени достижения качества процесса должно быть основано на одной или нескольких оценках процесса, которые:

- соответствуют предъявленным требованиям по ГОСТ Р ИСО/МЭК 33002, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994;
- являются моделируемым представлением текущих характеристик процесса относительно заданных исходных целей и данных для оценки;
- могут быть выполнены специально для определения рисков в процессе или уже были выполнены в ходе недавней самооценки либо после недавней независимой оценки.

Результаты оценки процесса могут быть использованы повторно.

В организации многие организационные подразделения хранят результаты оценок процессов. При наличии некоторого количества подходящих оценок системные аналитики могут использовать их результаты в качестве основы для обоснования достижения качества рассматриваемых процессов. В противном случае организация может провести самооценку.

Дополнительные рекомендации см. в 6.7.

5.2.7 Шаг 7. Проверить достижение уровня качества процесса

Если организационное подразделение представляет информацию о профиле процесса, который оно предлагает использовать для выполнения конкретного требования, системным аналитикам следует рассмотреть предложенный профиль процесса и определить, насколько он заслуживает доверия, после чего принять решение о том, какие дальнейшие действия необходимы для формирования доверия к нему. Могут быть выполнены следующие действия:

- проверка факта того, что в основе профиля процесса используется одна или более оценок процесса, выполненных на соответствие требованиям;
- проверка достоверности достижения качества процесса по любой улучшенной характеристике путем ее сопоставления с определенными исходными целями и данными для оценки;
- проверка актуальности результатов оценки.

Примечание — Поскольку подробная информация о базовой оценке (например, список собранных доказательств или план оценки) может быть недоступна системным аналитикам, в проверке могут использоваться соответствующие оценки самого системного аналитика.

Руководитель может принять предложенный профиль или принять решение о проведении независимой оценки процесса на соответствующем уровне. Сюда может входить выборка процессов или комплексная независимая оценка всех процессов, указанных в профиле оцениваемого процесса. После проведения проверки системные аналитики смогут сравнить полученный результат с утверждени-

ем организации о достижении качества процесса и создать профиль, который будет использоваться для последующего анализа рисков.

Если при определении рисков в процессе решается вопрос о выборе из нескольких конкурирующих поставщиков, руководитель может проверить предложенный профиль процесса по каждому поставщику с помощью независимой оценки (в т. ч. одного и того же метода оценки и той же модели соответствующего процесса). В результате у руководителя может быть больше аргументов в оценке каждого поставщика, а у поставщиков — больше уверенности в справедливости процесса отбора со стороны приобретающей стороны.

Если несколько организационных единиц (субподрядчики, партнеры в совместном предприятии или отдельные подразделения организации) будут принимать участие в выполнении определенного бизнес-требования, предлагаемый профиль процесса будет результатом совместных усилий всех организационных единиц.

Дополнительная информация приведена в 6.6 и 6.7.

5.2.8 Шаг 8. Проанализировать риск, связанный с процессом

Риск, связанный с процессом, оценивается по показателям рисков с учетом возможных потенциальных последствий в случае реализации угроз, повлекших нарушения реализации процесса (см. 6.6).

Выбранный метод определения рисков в процессе должен содержать определенный подход к анализу риска. В приложении А описан один из возможных подходов, другие возможные подходы приведены в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

5.2.9 Шаг 9. Действовать по результатам

Если определение рисков в процессе было проведено для понимания пригодности другой организации по конкретному договору, руководителю следует учитывать результаты проведенной оценки рисков, связанных с процессом, не только при принятии решений о заключении договора, но и при установлении договорных обязательств, связанных с текущей деятельностью по управлению рисками (см. ГОСТ Р 59991). Если определение рисков в процессе было проведено организацией для оценки достижения качества своих собственных процессов в отношении конкретных характеристик, требований или категории требований системной инженерии, руководитель может принять решение о принятии программы улучшения процессов для устранения всех выявленных проблем в отношении выявленных рисков.

6 Рекомендации по определению рисков в процессах

6.1 Инициирование определения рисков

Согласно ГОСТ Р ИСО/МЭК 33002 при оценке любого процесса определяют руководителя оценки процесса и возможные ограничения в самой оценке. Руководителем определения рисков в процессе и руководителем оценки процесса может выступать одно и то же лицо, но на практике это может быть не так. В частности, когда определение рисков в процессах выполняется в контексте выбора поставщика, результаты могут быть запрошены организацией-заказчиком в лице руководителя из набора оценок, имеющихся у поставщика и выполненных в рамках ответственности различных иных руководителей оценки.

Сначала руководитель принимает решение о том, следует ли выполнять определение рисков в процессе. Определение рисков в процессе может быть реализовано как самостоятельный проект с соответствующим управлением, бюджетом, этапами и подотчетностью. При этом управление проектом должно быть согласованным с используемой моделью для оценки процесса.

Руководителю следует создать группу системных аналитиков в интересах определения исходных целей и данных для оценки процесса и профиля процесса, а также для оценки рисков, связанных с процессом (в частном случае группа может состоять из одного системного аналитика).

6.2 Определение исходных целей и данных для оценки

6.2.1 Общая информация

Согласно ГОСТ Р ИСО/МЭК 33002, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994 при оценке любого процесса определяют исходные цели и данные для оценки. При этом могут быть использованы имеющиеся результаты проведенных ранее оценок.

Владельцы результатов оценки процесса и любые ограничения на их использование, а также любые меры контроля над информацией, вытекающие из соглашения о конфиденциальности, определяют во входных данных оценки и отражают все действующие соглашения о конфиденциальности, влияющие на общую программу улучшения процесса или определение рисков в процессе.

6.2.2 Выбор характеристик качества процесса

Характеристика качества процесса — это оцениваемое свойство, значимое для качества. Среди характеристик качества процесса могут быть такие, например, как возможности, безопасность или целостность процесса. В ходе определения рисков в процессе определяют характеристики качества процесса, которые могут быть связаны со значительными рисками в контексте организации. Это может быть подкреплено классификацией различных типов рисков (см. приложение А). Оценка степени достижения качества процесса должна быть основана на модели процесса по ГОСТ Р ИСО/МЭК 33003, на анализе возможностей процесса по ГОСТ Р ИСО/МЭК 33020 или на использовании математических моделей для оценки (см. ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994).

6.2.3 Выбор эталонных моделей процесса

Определение рисков в процессе требует выбора подходящей эталонной модели (моделей) процесса, системы-эталона и/или математической модели рассматриваемой системы.

Эталонная модель процесса описывает набор процессов с точки зрения цели и результатов (см. ГОСТ Р ИСО/МЭК 33004). Эталонная модель процесса имеет заявленную область использования. Вербальные модели процессов по ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 12207 являются примерами эталонных моделей процессов в областях системной и программной инженерии соответственно. Существует множество других эталонных моделей процессов. Примеры приемлемых показателей системы-эталона и математических моделей рассматриваемых систем приведены в ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994.

Системным аналитикам следует определить, какая эталонная модель (модели) процесса, системы-эталона или математической модели рассматриваемой системы лучше всего подходит для определения рисков в процессе.

6.2.4 Выбор модели процесса для оценки

На основе выбранной эталонной модели (моделей) процесса и выбранных характеристик качества процесса определяют соответствующую вербальную модель процесса (для качественной оценки рисков), математическую модель рассматриваемой системы или систему-эталон с известными или задаваемыми показателями (для количественного прогнозирования рисков).

При качественных оценках рисков, если необходимо сделать выбор между действующими моделями для оценки процесса, ключевым критерием выбора будет соответствие набора показателей устанавливаемому профилю риска. При количественных оценках рисков ориентируются на критерии, связанные с допустимым риском (см. приложения Г, Д).

6.2.5 Выбор набора процессов

Выбранная вербальная модель процесса должна быть адаптирована к набору процессов, реализуемых в жизненном цикле рассматриваемой системы и необходимых для достижения целей системы и выполняемых процессов. Примерный подход описан в таблице 1.

Таблица 1 — Выбор набора процессов

Шаг	Действие	Обоснование
Выберите начальный набор процессов	Выбор подходящих процессов из состава стандартных процессов соглашения и технического управления по ГОСТ Р 57193 или иных специфических процессов	Процессы соглашения и технического управления с учетом специфики вносят непосредственный существенный вклад в поставку продукции

Окончание таблицы 1

Шаг	Действие	Обоснование
Проверьте выбранные процессы	Анализ и исключение процессов, не относящихся к рассматриваемому требованию для определения рисков в процессе	Некоторые процессы, например процессы приобретения, могут быть неактуальными с точки зрения конкретных требований к определению рисков в процессе
Добавьте дополнительные процессы	Добавление процессов организационного обеспечения проекта и технических процессов по ГОСТ Р 57193 или иных специфических процессов	Процессы организационного обеспечения проекта и технические процессы по ГОСТ Р 57193 имеют особое значение для установления высокого уровня возможностей процессов в организации. Например, если свойство «Управление результативностью» (РА 2.1) используется для технического процесса системного анализа, то необходимо использовать и процессы «Планирование проекта» и «Оценка и контроль проекта»

6.2.6 Определение контекста процесса

Согласно 4.3.1 сопоставимость контекста процесса с предполагаемым применением процессов для конкретного требования или категории требований системной инженерии определяет значимость результатов определения рисков в процессе.

Например, если целью определения рисков в процессе является определение связанных с процессом рисков для качества конкретного продукта, то оценку необходимо проводить на экземплярах с применением процесса системного анализа данного конкретного продукта.

Если определение рисков в процессе применяют для выбора поставщика, разработку продукта или услуги планируют на основе конкретных требований заказчика. Определение рисков в процессе поможет спрогнозировать качество работы организации поставщика в случае его выбора. Поскольку оценка по факту не может быть выполнена в рамках разработки конкретного продукта или услуги, запрашиваемой заказчиком (так как разработка еще не начата), системные аналитики должны определить контекст процесса для целевого продукта. Здесь необходимо учитывать контекст процесса комплексирования продукта, который рассматривают в рамках оценки и который служит основой для определения рисков в рассматриваемом процессе.

6.3 Определение профиля процесса

Руководителю оценки (или по его поручению системному аналитику) необходимо определить для каждого выбранного процесса его профиль, отражающий необходимые свойства процесса, а также необходимые качественные и/или количественные показатели для оценки каждого свойства процесса. При качественной оценке следует использовать такие описательные рейтинги свойств, как «Полное соответствие» или «Значительная степень соответствия». Рейтинг «Не требуется» присваивается любым свойствам процесса, которые не считаются необходимыми. Рейтинг «Частичное соответствие» при качественной оценке использовать не следует, поскольку это будет означать, что некоторые аспекты достижения могут быть непредсказуемыми согласно ГОСТ Р ИСО/МЭК 33020. Если степень достижения свойства процесса не рассматривают как отвечающую определению рисков, связанных с выполнением конкретного процесса, допустимо использовать пустой целевой рейтинг. Это не означает, что свойство не нужно оценивать в ходе оценки.

При количественной оценке рекомендуют использовать вероятностные показатели рисков (см. ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994).

Набор целевых профилей процесса выражает достижение одной или нескольких целей процесса, которые руководитель (системный аналитик) считает адекватными при условии приемлемости рисков, связанных с процессом, для удовлетворения заданного требования (при определении рисков в процессе) или достижении целей (при поиске способов улучшения процесса).

Примечание — Для преемственности с международными и национальными стандартами, разработанными с учетом серии стандартов «Информационные технологии. Оценка процесса», в обозначениях

свойств и в некоторых процессах сохранены задействованные ранее обозначения из ГОСТ Р ИСО/МЭК 33002, ГОСТ Р ИСО/МЭК 33003, ГОСТ Р ИСО/МЭК 33004, ГОСТ Р ИСО/МЭК 33020.

Таблица 2 и рисунок 2 иллюстрируют пример достижения целевого свойства процесса для такой характеристики качества, как «Возможности процесса». Свойства процесса (PA 1.1 и т. д.) и качественной оценки («Полное соответствие» и т. д.) определены в ГОСТ Р ИСО/МЭК 33020. На рисунке 2 приведен пример достижения качества процессов, представленных в виде набора профилей по свойствам. При этом использованы рейтинги свойств процесса, приведенные в ГОСТ Р ИСО/МЭК 33020—2017, разделе 6. Требуемые рейтинги свойств процесса для TEC.3 «Определение системных требований» соответствуют уровню возможностей 2, требуемые оценки для MAN.5 «Управление конфигурацией» соответствуют уровню возможностей 3, а требуемые оценки для TEC.4 «Определение архитектуры» соответствуют уровню возможностей 4. В рамках процесса MAN.2 «Оценка и контроль проекта» не указано, что для свойства PA 2.2 не требуется никакого рейтинга. Это может означать, что требуемый рейтинг «Уровень возможностей 1» считается достаточным.

Таблица 2 — Пример экспертного рейтингования свойств процесса

Выбранный процесс из эталонной модели процесса	Свойства процесса	Требуемый рейтинг свойств процесса
TEC.3 Определение системных требований	PA 1.1 PA 2.1, PA 2.2	Полное соответствие Значительная степень соответствия
TEC.4 Определение архитектуры	PA 1.1, PA 2.1, PA 2.2, PA 3.1, PA 3.2, PA 3.3 PA 4.1, PA 4.2	Полное соответствие Значительная степень соответствия
MAN.5 Управление конфигурацией	PA 1.1, PA 2.1, PA 2.2 PA 3.1, PA 3.2, PA 3.3	Полное соответствие Значительная степень соответствия
MAN.1 Планирование проекта	PA 1.1, PA 2.1, PA 2.2, PA 3.1, PA 3.2, PA 3.3	Полное соответствие
MAN.2 Оценка и контроль проекта	PA 1.1, PA 2.1 PA 2.2 PA 3.1, PA 3.2, PA 3.3	Полное соответствие Не требуется Значительная степень соответствия

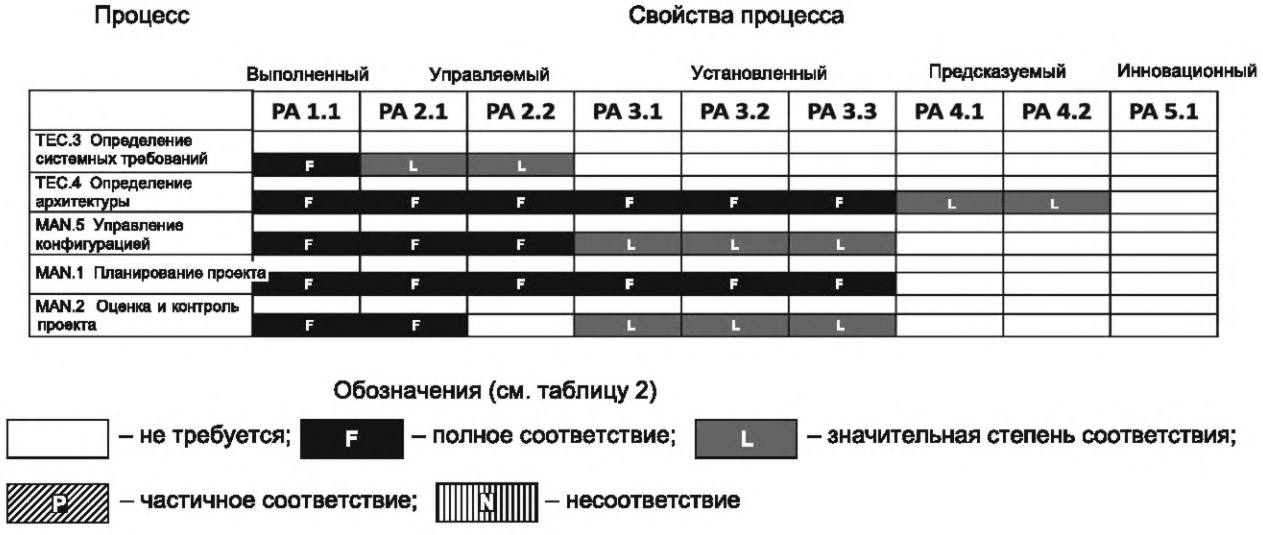


Рисунок 2 — Пример достижения качества процессов, представленных в виде набора профилей по свойствам

Метод установления рисков в процессе должен располагать средствами определения целевого достижения свойств процесса на основе анализа заданного требования. Возможный способ заключается в сопоставлении выявленных первопричин возникновения риска с недостатками в достижении требуемых свойств, характеризующих качество процесса (см. 4.3.2 и приложение А).

Один из иллюстрирующих подходов к формированию профиля оцениваемого процесса показан в таблице 3.

Таблица 3 — Формирование профиля процесса

Шаг	Действие	Обоснование
Определить набор процессов	Выбор набора процессов, определенных в исходных целях и данных для оценки (см. 6.3.5)	Этот шаг обеспечивает соответствие профиля процесса целям определения рисков в процессе
Задать требуемые по умолчанию рейтинги свойств для начального набора процессов	Присвоение рейтинга «Полное соответствие» уровням возможностей с первого по пятый	Это обеспечивает полный учет выбранных процессов
Адаптировать рейтинги свойств	Уменьшение рейтинга тех свойств, которые не являются необходимыми для идентифицированного риска	Такой подход гарантирует, что: - выбранные процессы будут выполнены в полном объеме; - будут внедрены методы управления, позволяющие избежать нарушения сроков, перерасхода бюджета и проблем с качеством продукции; - процессы будут внедрены в соответствии с проверенной передовой практикой, что дает уверенность в том, что будущие результаты будут соответствовать прошлым достижениям
Проанализировать и скорректировать требуемые рейтинги свойств процесса	Присвоение рейтингов свойствам уровня 4 или 5 или удаление рейтинга для уровня 3	Добавление свойства уровней 4 и 5 для некоторых процессов иногда может быть оправданным с целью снижения рисков, связанных с процессом (см. рисунок 1). На рисунке 1 профиль процесса определения архитектуры TEC.4 содержит свойства процесса уровня возможностей 4. Удаление свойств процесса уровня 3 может быть оправданным (см. рисунок 2). На рисунке показано, что профиль процесса для анализа требований к программному обеспечению DEV.1 содержит свойства процесса только уровней возможностей 1 и 2. Целевой уровень возможностей процессов технического управления и процессов организационного обеспечения проекта определяется степенью поддержки ими свойств процесса, применяемых к первоначальному набору процессов. Другие процессы, обеспечивающие реализацию проекта, также должны быть включены в заявленные целевые возможности, если они имеют отношение к рассматриваемому требованию (для определения рисков в процессе)

Следует учитывать, что профиль процесса может потребоваться для рассмотрения конкретных рейтингов свойств организационного процесса, а не для разработки продукции или оказания услуг. Например, в качестве требования может выступать создание устойчивого процесса управления конфигурацией (как самоцель). Тогда в наборе процессов будет лишь этот единственный процесс. Пример формирования профиля процесса приведен в приложении В.

Примеры количественных показателей рисков приведены в приложении Г.

6.4 Принципы определения рисков в процессе

6.4.1 Общая информация

Согласно 4.3.3 заинтересованные стороны могут разработать конкретные рекомендации по рейтингованию, включая определение критериев сбора информации. В состав этих рекомендаций должны входить пояснения, касающиеся:

- определения области применения рейтингов;
- определения категорий различных типов риска;
- определения целевого вклада в оценку;
- определения критериев сбора информации по конкретным типам рисков;
- рейтинговых правил в отношении конкретных типов рисков;
- рекомендации по необходимым навыкам оценщиков.

6.4.2 Рекомендации по определению целевого вклада в оценку

Организация может установить конкретные рекомендации по выбору исходных целей и данных для оценки в отношении определенных типов рисков, соответствующих конкретным требованиям. В эти рекомендации могут входить следующие пояснения:

- по модели процесса, соответствующей контексту организации или системы;
- выбору стандартного процесса в отношении определенных типов рисков, подлежащих определению;
- методу описания целевого контекста процесса в отношении типов рисков, подлежащих определению;
- способу подтверждения квалификации оценщиков.

6.4.3 Критерии для сбора информации

Конкретные критерии для сбора информации могут поддержать значимость результатов определения рисков в процессе. Эти критерии могут быть установлены в отношении целей определения рисков в процессе и тем самым согласованы с определенными типами исследуемых рисков. В критерии должно входить следующее:

- количество и тип объективных доказательств, необходимых для подтверждения возможности выполнения каждого свойства процесса;
- учет контекста процесса при выборе объективных доказательств;
- класс оценки с учетом независимости оценщиков.

Например, при определении связанных с процессом рисков в отношении качества продукции могут потребоваться указания контекста процесса в терминах конкретного набора требований заинтересованных сторон относительно выпуска продукции. В этом случае рекомендации могут касаться того, чтобы каждая оценка свойств процесса рассматривала степень достижения результатов процесса в отношении данного набора требований заинтересованных сторон. В рекомендациях также может быть указано, что количество и тип объективных доказательств подходят с точки зрения достаточности охвата набора требований заинтересованных сторон.

Для определения рисков в процессе поставки возможны, например, рекомендации, чтобы каждая оценка свойств процесса подтверждалась как минимум тремя устными утверждениями, полученными на разных этапах сбора данных, и как минимум одним документальным свидетельством. В рекомендациях также может быть указано, что если документ был официально запрошен компетентным оценщиком, но организационное подразделение заявило о невозможности его предоставления, то это утверждение может быть учтено вместо требуемого документального свидетельства.

6.4.4 Правила в отношении рейтингов

Рекомендации могут определять конкретные правила оценки или содержать разъяснения для определенной модели процесса. Эти правила должны учитывать следующие зависимости рейтингов свойств процесса:

- между различными процессами на одном и том же уровне качества;
- в рамках процессов на разных уровнях качества;
- между различными процессами на разных уровнях качества.

6.5 Оценка рисков, связанных с процессами

6.5.1 Вывод о рисках на основании результатов оценки

Качество продукции или услуг в значительной степени зависит от используемых процессов. Риски, связанные с процессами, могут возникнуть, например, в результате ненадлежащего управления процессами, т. е. отсутствия соответствующих процессов или их развертывания способом, который не позволяет достичь требуемых рейтинговых оценок свойств процессов.

Характеристики качества процесса могут быть оценены с использованием подхода, определенного в ГОСТ Р ИСО/МЭК 33002, возможности процесса — по ГОСТ Р ИСО/МЭК 33020.

Результатом качественной оценки процесса является набор профилей процесса. Требуемые свойства процесса могут быть представлены в виде набора целевых профилей процесса (см. 6.4 и рисунок 2).

Профили целевого и оцениваемого процессов могут быть представлены на одной диаграмме (см. рисунок 3). Свойства процесса (PA 1.1 и др.) и рейтинги («Полное соответствие» и т. д.) описаны в ГОСТ Р ИСО/МЭК 33020.

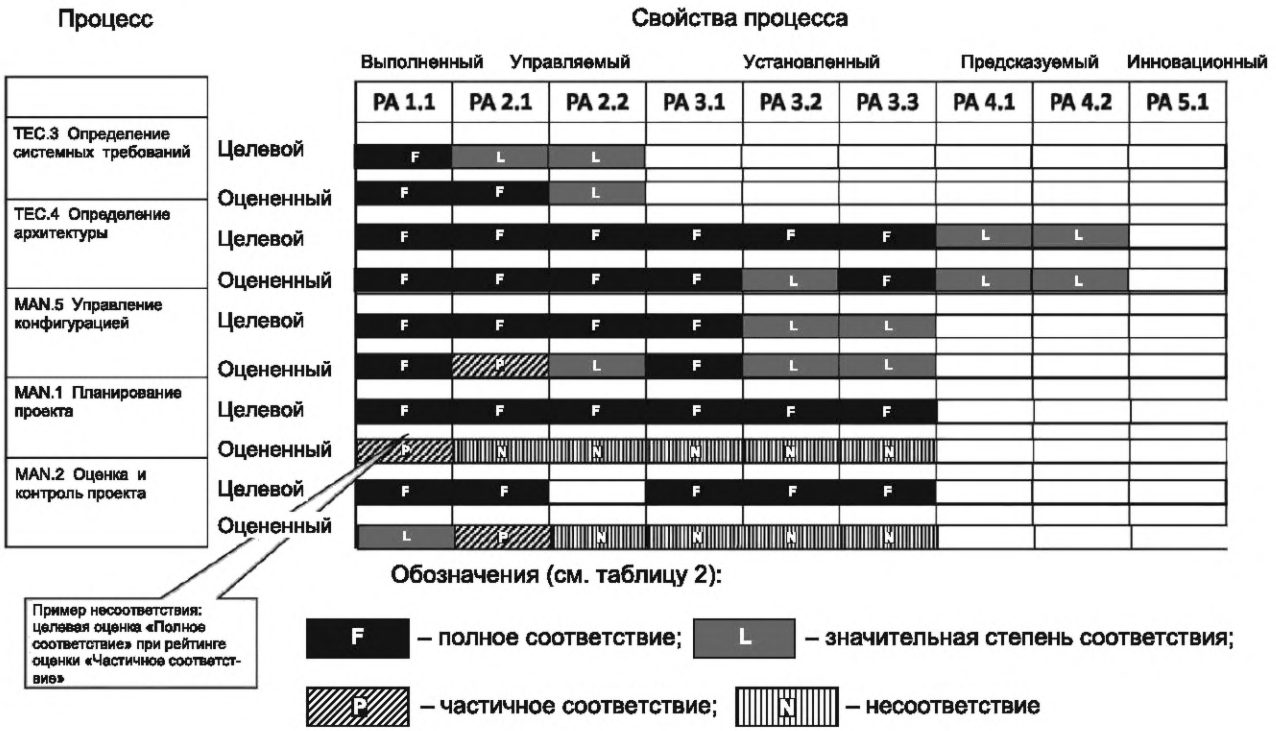


Рисунок 3 — Целевые и оцененные профили процессов

Риск, связанный с процессом, можно определить по наличию несоответствий между целевым и оцененным профилями процесса. Несоответствием считаются следующие ситуации:

- профиль процесса требует, чтобы определенное свойство процесса было обеспечено в полной мере, в то время как рейтинг свойства процесса не свидетельствует о полном соответствии;
- профиль процесса требует, чтобы определенное свойство процесса было обеспечено в значительной степени, в то время как рейтинг свойства процесса не свидетельствует о значительном соответствии.

Потенциальное последствие несоответствия зависит от уровня качества процесса и свойства процесса, в котором возникает несоответствие (см. таблицу 4). Определения свойств процесса (PA 1.1 и др.) приведены в ГОСТ Р ИСО/МЭК 33020.

Таблица 4 — Потенциальные последствия несоответствий свойств процесса

Свойство процесса с несоответствием	Возможное последствие
РА 1.1 Результатив-ность процесса	Отсутствующие информационные продукты; результаты процесса не достигнуты
РА 2.1 Управление результативностью	Превышение затрат или сроков; неэффективное использование ресурсов; нечеткие обязанности, неконтролируемые решения и неопределенность в отношении того, будут ли достигнуты цели по срокам и затратам
РА 2.2 Управление документированной информацией	Непредсказуемое качество и целостность продукта, неконтролируемые версии, увеличение затрат на поддержку, проблемы интеграции и увеличение затрат на повторную работу
РА 3.1 Определение процесса	Выявленные на базе предыдущих проектов лучшие практики и извлеченные уроки не используются организацией; отсутствие основы для совершенствования процессов в масштабах всей организации
РА 3.2 Развертывание процесса	Внедренный процесс не учитывает лучшие практики и уроки, извлеченные из предыдущих проектов; непоследовательная работа процесса в рамках организации; отсутствует необходимая документированная информация
РА 3.3 Контроль процесса	Потеря эффективности; несоответствия не устраняются; упущенные возможности для понимания процесса и определения улучшений
РА 4.1 Количественный анализ	Отсутствие количественной оценки достигаемых целей результативности процесса и заданных бизнес-целей; отсутствие количественных возможностей для раннего выявления проблем результативности
РА 4.2 Количественный контроль	Результативность процесса не является стабильной или предсказуемой; не достигнуты количественные показатели результативности и определенные бизнес-цели
РА 5.1 Инновации процесса	Нет четкого определения возможностей для совершенствования; отсутствует возможность эффективного изменения процесса для достижения соответствующих целей его совершенствования

Риск, связанный с процессом, оценивают по вероятности возникновения негативных последствий в результате выявленного несоответствия и по ее потенциальным последствиям. Выбранный метод определения рисков в процессе должен содержать определенный подход к анализу рисков, связанных с процессом. Пример возможного подхода с качественными оценками рисков приведен в приложении Б, а с использованием количественных оценок рисков на вероятностном уровне — см. ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994.

6.5.2 Анализ недостатков

Выявление несоответствий указывает на наличие недостатков в процессе. Для каждого выявленного несоответствия системный аналитик в отношении заданного требования или бизнес-цели может установить и зафиксировать следующее:

- характер недостатка;
- источник или причину недостатка;
- потенциальные последствия недостатка.

6.6 Использование определения рисков для выбора поставщика

Определение рисков в процессе может играть заметную роль при выборе поставщика, например, в процессе приобретения. Одним из результатов этого процесса является выбор одного или нескольких поставщиков на основании оценки их предложений, возможностей процесса и других факторов. При-

обретающая сторона может определить риск в процессе при заключении договора поставки с одним поставщиком либо определить риск в процессе с привлечением конкурирующих поставщиков.

Поставщики также могут осуществить определение риска в своих процессах до принятия решения о подаче заявки для участия в конкурсе на заключение договора поставки. Определение рисков в процессе может быть инициировано и по ряду других причин, например поставщиком в ходе выполнения проекта для определения рисков, связанных с завершением работ.

Для оценки текущего уровня соответствующей характеристики качества процесса на этапе 3 определения рисков в процессе могут быть применены методы самооценки и независимой оценки. При заключении двустороннего договора покупатель может предложить потенциальным поставщикам предоставить наборы профилей процессов для самооценки вместе с предложением о заключении договора поставки. Наборы профилей процессов получают в результате оценки соответствия заданной эталонной модели процесса.

После этого покупатель может выбрать один из следующих вариантов действий:

- принять результаты проведенной самооценки;
- провести и принять результаты тотальной независимой оценки с возможным привлечением экспертов из собственной организации и указать это в качестве условия заключения договора;
- инициировать ограниченную независимую оценку для проверки соответствия самооценки реальным характеристикам качества процесса поставщика. Преимущество такого подхода заключается в меньшем нарушении обычной деятельности поставщиков в результате многочисленных оценок процессов, поскольку результат одной оценки может быть предложен для рассмотрения многими заинтересованными сторонами (в качестве заинтересованных сторон могут выступать приобретающие стороны, пользователи продукции или услуг). Приобретающие стороны также получают регламентированный и обоснованный подход к определению рисков в процессах поставщика с возможностью снизить затраты на оценку за счет повторного использования результатов и применения самооценки поставщика.

6.7 Сопоставимость результатов оценки

Системным аналитикам для определения рисков в процессе может потребоваться сравнение рисков, например, рисков, определенных в вероятностном выражении, с допустимыми рисками по ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994.

Сравнение результатов различных качественных оценок может быть также проведено путем сравнения профилей процессов. Это возможно только в том случае, если все они содержат аналогичные процессы из одной эталонной модели процесса и основаны на сопоставимых входных данных оценки, включая контекст процесса. При этом необходимо рассмотреть ряд факторов, позволяющих определить, является ли сравнение результатов различных оценок правомерным. Этими факторами, среди прочего, могут быть:

- рассматриваемые процессы для оценки;
- используемые модели для оценки соответствующих процессов;
- количество и тип объективных свидетельств, используемых для определения набора профилей процессов;
- личность, навыки, знания и опыт системных аналитиков.

Приложение А
(справочное)

Пример классификации типов рисков

А.1 Общая информация

Согласно 4.3.2 значимость результатов определения рисков в процессах может быть подкреплена анализом и классификацией конкретных типов рисков для обеспечения исходными данными на последующих шагах оценки процессов.

Сделать это возможно путем сопоставления выявленных основных причин возникновения неприемлемых рисков с недостатками свойств, характеризующих качество процесса.

Пример классификации содержится в таблице А.1.

Таблица А.1 — Пример классификации типов рисков, связанных с процессами

Категория типа риска	Тип риска	Возможные причины возникновения риска	Возможные последствия
А	Риск в отношении качества продукции	Отсутствие или недостаточность информационных продуктов; непоследовательность информационных продуктов; недостаточная эффективность работы поставщика	Неприемлемое качество продукции; несоблюдение требований заинтересованных сторон или законодательства; неудовлетворенность клиентов; инциденты, связанные с безопасностью; инциденты системы защиты
В	Существующий риск организации	Отсутствие определений стандартных процессов; отсутствие развертывания стандартных процессов; неподходящие стандартные процессы	Превышение сроков или затрат; отсутствие единообразия результатов работы в течение времени или в различных организационных подразделениях; снижение эффективности выполнения процессов; дублирование работы/повторно выполняемая работа; отсутствие эффекта синергии; препятствия для сотрудничества между организационными подразделениями
С	Потенциальный риск организации	Отсутствие количественного измерения развернутых процессов; отсутствие совершенствования стандартных процессов; несогласованность стандартных процессов с бизнес-целями организации	Недостаточная возможность прогнозировать результативность; недостаточная возможность своевременно обнаруживать проблемы в применении стандартных процессов; недостаточная оптимизируемость стандартных процессов с точки зрения затрат/времени/ресурсов; недостаточная возможность реагирования на технологические изменения

Далее приведены примеры сопоставлений и соответствующие аргументы исходя из определенного уровня возможностей процесса согласно ГОСТ Р ИСО/МЭК 33020.

А.2 Категория А: связанные с процессом риски в отношении качества продукции

В таблицах А.2—А.4 приведены примеры классификации типов риска на основе следующих признаков:

++ — недостаточное достижение качества процесса по рассматриваемому свойству является значительным свидетельством наличия идентифицированного типа риска;

+ — недостаточное достижение качества процесса по рассматриваемому свойству является дополнительным свидетельством наличия идентифицированного типа риска;

о — недостаточное достижение качества процесса по рассматриваемому свойству аргументированно не может быть свидетельством наличия идентифицированного типа риска.

Пример классификации по причинам возникновения риска, связанного с процессом выпуска продукции, представлен в таблице А.2.

Таблица А.2 — Категория А: причины возникновения риска с учетом свойств процесса

Категория типа риска	Причина возникновения риска	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5
А	Отсутствие или недостаточность информационных продуктов	++	++	+	o	o
	Непоследовательность информационных продуктов	++	++	+	o	o
	Недостаточная эффективность работы поставщика	++	+	o	o	o
	Неадекватное управление деятельностью или информационными продуктами	++	++	+	o	o

Результат оценки возможностей процесса по ГОСТ Р ИСО/МЭК 33020 может свидетельствовать о наличии риска, связанного с процессом и влияющего на качество выпускаемой продукции.

Важными критериями для определения риска, связанного с производством продукции, являются:

- степень правильности и полноты обработки соответствующими процессами данного набора общих требований и изменений, связанных с выпуском продукции;
- сопровождение выполнения этих процессов соответствующим набором дополнительных процессов;
- адекватность управления выполнением этих процессов и связанных с ними информационных продуктов.

Результатом этого является вывод о том, что несоответствия в достижении свойств процесса РА 1.1, РА 2.1 и РА 2.2 являются значимыми показателями в отношении качества выпускаемой продукции.

При определении контекста процесса для настройки исходных целей и данных для оценки и согласованного профиля процесса следует использовать набор общих требований и изменений, связанных с выпуском продукции.

При оценке свойства процесса РА 1.1 степень достижения результатов процесса следует оценивать относительно данного набора требований заинтересованных сторон. Количество и тип объективных доказательств должны соответствовать данному набору требований заинтересованных сторон.

Примечание — Определение рисков категории А для разработки определенной продукции может способствовать улучшению процесса с целью снижения рисков.

А.3 Категория В: существующие организационные риски

Пример классификации по причинам возникновения риска, связанного с процессами организации, представлен в таблице А.3.

Таблица А.3 — Категория В: причины возникновения риска с учетом свойств процесса

Категория типа риска	Причина возникновения риска	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5
В	Отсутствие определения стандартных процессов	o	o	++	o	o
	Отсутствие развертывания стандартных процессов	o	o	++	o	o
	Неподходящие стандартные процессы	+	+	++	o	o

Результаты оценки возможностей процесса по ГОСТ Р ИСО/МЭК 33020 могут быть расценены как свидетельство наличия рисков, связанных с процессами и влияющих на достижение бизнес-целей организации на данный момент времени.

Для оценки текущих рисков организации важным является представление того, в какой степени определены и развернуты стандартные процессы и в какой степени эти процессы являются эффективными.

Это позволяет сделать вывод, что несоответствия в достижении свойств процесса РА 3.1, 3.2, 3.3 и частично РА 1.1, 2.1 и 2.2 являются признаками наличия рисков для организации. Несоответствия в достижении свойств

РА 3.1, 3.2 и 3.3 непосредственно провоцируют возникновение указанных рисков независимо от того, могут ли несоответствия в выполнении и управлении этими процессами (РА 1.1, 2.1 и 2.2) служить доказательством неэффективности или непригодности определенных процессов.

Определение контекста процесса для настройки исходных целей и данных для оценки и согласованного профиля процесса необходимо согласовать с основным порядком применения процессов, принятым в организации. В этом случае исходные цели и данные для оценки могут быть применены в отношении значительного числа разработок при формировании обоснованного заключения.

Примечания

1 Оценка рисков категории В может способствовать улучшению процессов и совершенствованию развертывания стандартных процессов в организации.

2 Оценка зрелости организации может помочь в расширении охвата различных организационных единиц.

А.4 Категория С: будущие организационные риски

Пример классификации по причинам возникновения риска, связанного с процессами при развитии организации, представлен в таблице А.4.

Таблица А.4 — Категория С: причины возникновения риска с учетом свойств процесса

Категория типа риска	Причина возникновения риска	Уровень 1	Уровень 2	Уровень 3	Уровень 4	Уровень 5
С	Отсутствие количественного измерения развернутых процессов	о	о	+	++	++
	Отсутствие совершенствования стандартных процессов	о	о	+	++	++
	Несогласованность стандартных процессов с бизнес-целями организации	о	о	+	++	++

Результат оценки возможностей процесса по ГОСТ Р ИСО/МЭК 33020 может служить свидетельством наличия рисков, связанных с процессом и влияющих на достижение бизнес-целей организации в будущем.

Это позволяет сделать вывод, что несоответствия в достижении свойств процесса РА 4.1, 4.2 и 5.1 и частично РА 3.1, 3.2 и 3.3 являются существенными признаками возникновения рисков для организации в будущем. Несоответствия в достижении свойств РА 4.1 — РА 5.1 непосредственно способствуют возникновению вышеупомянутых рисков.

При определении будущих рисков организации, связанных с процессами, можно предположить, что стандартные процессы уже определены, развернуты и приведены в соответствие с преобладающим в организации порядком применения процессов. Несоответствия в определении, развертывании и обеспечении этих процессов (РА 3.1, 3.2 и 3.3) могут свидетельствовать о том, что это предположение неверно.

При определении будущих рисков для организации, связанных с процессами, контекст процесса играет лишь вспомогательную роль. Любая оценка должна концентрироваться на полном множестве стандартных процессов, которые определяют набор рассматриваемых процессов в исходных целях и условиях оценки.

Приложение Б
(справочное)

Пример качественной оценки рисков, связанных с процессами

Б.1 Общая информация

В примере подхода к анализу рисков, связанных с процессами, описанными в данном приложении, риск оценивают на основе анализа каждого процесса и определяют по наличию несоответствий между целевым профилем процесса и оцененными свойствами процесса.

Несоответствия присутствуют в отношении каждого процесса в следующих случаях:

- профиль процесса требует, чтобы определенное свойство процесса было обеспечено в полной мере, в то время как рейтинг свойства процесса не свидетельствует о полном соответствии;
- профиль процесса требует, чтобы определенное свойство процесса было обеспечено в значительной степени, в то время как рейтинг свойства процесса не свидетельствует о значительной степени соответствия.

Общий риск, связанный с каждым процессом, определяется по качественным оценкам относительно возникновения негативных последствий в результате выявленного несоответствия и по потенциальным последствиям.

Б.2 Качественная оценка

Качественная оценка возможности возникновения негативных последствий определяется степенью несоответствия между целевым и оцененным профилями процесса.

Несоответствия свойств процесса возникают, когда оцененный рейтинг свойств процесса не соответствует требуемому рейтингу. Условия несоответствия свойств процесса могут быть охарактеризованы, например, как показано в таблице Б.1.

Таблица Б.1 — Условия несоответствия свойства процесса

Требуемый рейтинг свойства процесса	Рейтинг свойства оцениваемого процесса	Несоответствие (свойства процесса)
Полное соответствие	Полное соответствие	Отсутствует
	Значительная степень соответствия	Незначительное
	Частичное соответствие	Значительное
	Несоответствие	Значительное
Значительная степень соответствия	Полное соответствие	Отсутствует
	Значительная степень соответствия	Отсутствует
	Частичное соответствие	Значительное
	Несоответствие	Значительное

Качественная оценка вероятности возникновения негативных последствий зависит от степени несоответствий в свойствах процесса и от уровней качества процесса, на которых они возникают (см. таблицу Б.2).

Таблица Б.2 — Несоответствия на уровнях качества процесса

Количество несоответствий в свойствах процесса и на уровнях качества процесса	Несоответствие на уровне качества процесса	Оценка вероятности возникновения негативных последствий
Отсутствие значительных и незначительных несоответствий	Отсутствует	Самая низкая
Отсутствие несоответствий на уровне 1 и незначительные несоответствия на уровнях 2, 3, 4 или 5	Небольшое	—
Незначительное несоответствие на уровне 1 или одно значительное несоответствие на уровнях 2, 3, 4 или 5	Значительное	—
Основное несоответствие на уровне 1 или более одного основного несоответствия на уровнях 2, 3, 4 или 5	Существенное	Самая высокая

Наивысшая степень возникновения негативных последствий связана с существенным несоответствием на уровне качества процесса, возникающим либо из-за значительного несоответствия в свойствах процесса на уровне 1, либо в результате двух или более несоответствий на уровнях 2—5. Одно незначительное несоответствие на уровне 1 или два и более значительных несоответствия на уровнях 2—5 представляют собой значительное несоответствие на уровне качества процесса и умеренную оценку вероятности возникновения негативных последствий. Незначительные несоответствия в пределах на уровнях 2—5 представляют собой незначительное несоответствие на уровне качества процесса и низкую вероятность возникновения негативных последствий.

Б.3 Последствия

Потенциальные последствия, связанные с несоответствиями отдельных свойств процесса, приведены в таблице 4. Для целей анализа качественных оценок риска, связанного с процессом, серьезность последствий зависит от уровня качества процесса, в рамках которого возникают несоответствия. Это показано в таблице Б.3.

Например, если выбранный процесс оценен как не полностью соответствующий, т. е. свойство РА 1.1 не достигнуто полностью, то результаты процесса могут быть не достигнуты (самая высокая степень серьезности последствий).

Таблица Б.3 — Негативные последствия

Уровень качества процесса, при котором возникает несоответствие	Характер последствий	Серьезность последствий
5 — Инновационный процесс	Невозможность улучшить процесс и оценить улучшения	Самая низкая
4 — Предсказуемый процесс	Невозможность количественной оценки результативности или раннего выявления проблем	—
3 — Установленный процесс	Непоследовательное выполнение процессов в рамках организации	—
2 — Управляемый процесс	Превышение затрат или сроков; непредсказуемое качество продукции	—
1 — Выполненный процесс	Отсутствующие информационные продукты; результаты процесса не достигнуты	Самая высокая

Б.4 Риск, связанный с процессом

Риск, связанный с каждым процессом, зависит от возможности возникновения негативных последствий в результате выявленного несоответствия и от самих последствий.

Наивысший риск возникает в случае существенного несоответствия на более низком уровне возможностей процесса, как показано в таблице Б.4.

Если риски идентифицированы на двух или более уровнях возможностей процесса, то за качественную оценку риска для данного процесса принимают оценку самого высокого уровня возможностей.

Таблица Б.4 — Риск, связанный с каждым уровнем возможностей процесса

Уровень возможностей процесса, в котором возникают несоответствия	Небольшое несоответствие	Значительное несоответствие	Существенное несоответствие
5 — Инновационный процесс	Низкий риск	Низкий риск	Низкий риск
4 — Предсказуемый процесс	Низкий риск	Низкий риск	Средний риск
3 — Установленный процесс	Низкий риск	Средний риск	Средний риск
2 — Управляемый процесс	Средний риск	Средний риск	Высокий риск
1 — Выполненный процесс	Средний риск	Высокий риск	Высокий риск

Б.5 Определение процессов с наивысшим риском

Риск, связанный с каждым процессом, можно свести в таблицу (см. таблицу Б.4) и определить процесс(ы) с наивысшей степенью риска.

Если несколько процессов связаны с одинаково высокой степенью риска, наиболее важные для достижения целей процессы (в отношении заданных требований) можно определить с помощью профессионального суждения системных аналитиков. При этом, несмотря на то, что технические процессы зачастую имеют наибольшее значение, в некоторых случаях не меньшее значение могут иметь обеспечивающие процессы.

Б.6 Подход к анализу

Для каждого процесса группа системных аналитиков выполняет следующие действия:

- изучает каждое свойство процесса в рамках профиля процесса и выявляет любые несоответствия в свойствах процесса (таблица Б.1);
- рассматривает несоответствия в свойствах процесса и определяет любые несоответствия на уровне возможностей процесса (таблица Б.2);
- определяет серьезность последствий (таблица Б.3) и потенциальный риск, связанный с процессом, который ассоциируют с каждым несоответствием на уровне возможностей процесса (таблица Б.4);
- определяет, какое несоответствие на уровне возможностей процесса представляет собой наивысшую степень риска, и принимает его качественную оценку риска, связывая ее с данным процессом.

Затем группе системных аналитиков необходимо определить, какой процесс(ы) сопряжен с наибольшей степенью риска. Если два или более процессов представляют одинаковую степень риска, приоритет рисков можно задать на основе факторов, являющихся внешними по отношению к действиям в рамках процесса, таких как оценка вероятности возникновения риска и весомость последствий для организации.

Примечание — Там, где это возможно, качественную оценку рисков рекомендуется сопровождать количественными оценками с использованием научно обоснованных методов прогнозирования рисков (см. приложения Г, Д).

Приложение В
(справочное)

Пример формирования профиля процесса

В.1 Общая информация

Ценность профиля процесса заключается в том, что его понимание способствует качественной оценке рисков в процессе. Содержимое профиля процесса отражает некоторую описательную характеристику достижения целей процесса для выполнения определенных требований системной инженерии.

Профиль процесса выводят из определенных требований системной инженерии и прослеживают до одного или нескольких свойств, характеризующих качество процесса, или показателей качества, безопасности и/или эффективности рассматриваемой системы, которые характеризуют степень выполнения этих требований в рассматриваемой системе. В свою очередь сами требования позволяют руководителю выбрать соответствующие свойства процесса и с помощью показателей определить требуемый рейтинг для каждого свойства процесса или соответствующий уровень качества процесса и оценку уровня качества процесса.

В целом руководителю рекомендуется выбрать одну или несколько существующих вербальных моделей процессов и использовать описание процессов в выбранных моделях для характеристики качества процесса. Если для выполнения требований системной инженерии необходимо определить один или несколько дополнительных процессов, у руководителя есть два варианта:

- определить процесс для демонстрации соответствия по ГОСТ Р ИСО/МЭК 33004, ГОСТ Р 57193 или иному стандарту, в котором описан необходимый процесс, чтобы получить соответствующий профиль процесса;
- если процесс оригинален и не соответствует требованиям, приведенным в ГОСТ Р ИСО/МЭК 33004, ГОСТ Р 57193 или в ином стандарте, в котором описан необходимый процесс, то использовать профиль процесса, отметив при этом его несоответствие для целей определения рисков.

В результате будет сформирован набор целевых профилей различных процессов, применимых к предполагаемому использованию в рассматриваемой системе (с рейтингами свойств процессов).

Примечания

1 Работа по определению и использованию профилей процессов может быть выполнена системными аналитиками.

2 К программному обеспечению, которое должно соответствовать критически важным для безопасности человека требованиям системной инженерии в конкретной области применения, предъявляют иные требования, нежели к программному обеспечению, используемому для создания персональных веб-сайтов. Некоторые из выбранных процессов в любой области применения должны относиться к более высоким уровням качества процесса для достижения приемлемых рисков, связанных с процессом, в то время как другие процессы, которые оказывают меньшее влияние на риск, связанный с процессом, должны быть эффективными на более низких уровнях качества процесса.

3 Уровень зрелости в модели зрелости организации может быть составлен с учетом набора целевых профилей процессов.

В.2 Определение профиля процесса

В.2.1 Общая информация

Определение профиля процесса может быть выполнено с помощью следующих действий:

- определение цели;
- определение пользователей;
- определение требований системной инженерии;
- определение области применения;
- определение характеристик;
- определение существенности угроз и условий в процессе;
- определение критериев для сбора и обработки информации;
- определение модели процесса;
- описание профиля процесса;
- определение показателей достижения качества процесса.

Процесс определения профиля процесса также может быть представлен в виде схемы.

В.2.2 Определение цели

Руководитель выбирает или определяет цель для профиля оцениваемого процесса:

- в интересах удовлетворения определенных потребностей;
- для оценки достижения качества процесса внутри рассматриваемой организации;

- для оценки достижения качества процесса в другой организации, связанной с выполнением оцениваемого процесса;

- для определения необходимости улучшений с учетом каждого несоответствия между фактическим достижением качества процесса и профилем процесса.

В.2.3 Определение пользователей

Руководитель выбирает или определяет пользователей для профилей процессов. Профили процессов могут варьироваться в зависимости от пользователей. Например, общеотраслевое сообщество пользователей может использовать различные бизнес-модели предприятий. Корпоративное сообщество пользователей должно соответствовать конкретной бизнес-модели предприятия. Аналогичным образом профиль оцениваемого процесса, ориентированный на группу специалистов или проект, должен соответствовать более конкретным потребностям команды или проекта. В основе сообщества пользователей может быть:

- сообщество пользователей определенной отрасли, например автомобилестроения, медицинского оборудования, телекоммуникаций, ИТ-услуг;

- сообщество пользователей на уровне конкретного предприятия с конкретной бизнес-моделью, что позволяет учитывать процессы и характеристики предприятия, которые могут обеспечить конкурентное преимущество по сравнению с другими предприятиями;

- уровень группы специалистов проекта в рамках предприятия с определенным набором требований системной инженерии, например группы специалистов по проектам в области программного обеспечения в компании-поставщике для определения конкретных рекомендаций по совершенствованию проектов;

- профессиональное или техническое сообщество пользователей для определения различных уровней достижимого качества процесса.

В.2.4 Определение требований системной инженерии

Руководитель выбирает или определяет требования системной инженерии, которые могут быть использованы при формировании профиля процессов. Например, руководитель может определить требование системной инженерии в отношении программного обеспечения для медицинского оборудования с выделением обязательной проблематики обеспечения безопасности людей (как пациентов, так и операторов). Другим примером могут служить требования системной инженерии на основе финансовых критериев или критериев качества при ограничениях, связанных с обеспечением безопасности. Подробнее требования системной инженерии, которые могут быть использованы при формировании профиля процессов, приведены в ГОСТ Р 57193, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994.

В.2.5 Определение области применения

Руководитель выбирает или определяет область применения профилей процессов. Область применения должна определять создание целевых профилей процессов в отношении выбора модели каждого процесса. Пользователей профилей процессов необходимо также направить на выбор профиля для его целевого назначения и целей соответствующей организации, например поставщика системы или поставщика программного обеспечения.

Область применения может быть определена в широком смысле, например для систем, программного обеспечения или ИТ-услуг (или более конкретно: например, программное обеспечение для электрических блоков управления и контроля скорости автомобиля). Чем более конкретна выбранная область применения, тем более понятным является определение конкретных процессов, характеристик качества процесса и, следовательно, тем выше качество профилей процессов и их применимость для конкретных пользователей. С другой стороны, слишком узкое определение снижает общую применимость профилей процессов. Более широко задаваемая область применения, как правило, охватывает большее число пользователей. С другой стороны, слишком широкое определение области применения приведет к менее полезным рекомендациям и потенциальной необходимости большей адаптации профиля с учетом специфики его применения конкретными пользователями.

В.2.6 Определение характеристик

Руководитель определяет характеристику или выбирает описание характеристики для соответствующей области применения. Характеристика или описание характеристики должны отражать уровни связанного с процессом риска или создания полезных свойств, которые присутствуют при применении. Следовательно, описание характеристики должно четко определять критерии, указывающие на необходимость использования нескольких ее форм, на основании которых определяется количество необходимых наборов профилей процессов и создание каждого набора.

Характеристика может быть основана на одном или нескольких критериях полезности характеристики (или на сочетании критериев). Этими критериями среди прочего могут быть: критерии критичности бизнеса или услуги, критерии критичности безопасности, финансовые или операционные критерии, критерии качества, функциональные критерии, критерии своевременности доставки. Например, описание характеристики, использующее критерии критичности безопасности, должно привести к созданию нескольких уровней безопасности, например в диапазоне от критического для безопасности человека, умеренной важности для безопасности, низкой важности для безопасности или даже не имеющего отношения к безопасности.

Для выбранного процесса может потребоваться другая характеристика качества процесса, соответствующая меняющемуся риску, связанному с процессом. Каждая отдельная характеристика может привести к созданию отдельного профиля оцениваемого процесса. Правильно определенная характеристика будет четко направлять пользователей в формировании адекватного набора целевых профилей процессов с соответствующими свойствами процесса для снижения рисков, связанных с процессом, и удовлетворения требований системной инженерии для области применения и ожиданий пользователей.

В.2.7 Определение существенности угроз и условий в процессе

В условиях неопределенности руководитель определяет существенность угроз и условий в процессе. Для этого используются методы, требования к которым сформулированы в ГОСТ Р 59991—2022, подраздел 7.5, примеры задач определения существенных угроз и условий отражены в том же стандарте (см. А.1.3).

В.2.8 Определение критериев для сбора и обработки информации

Руководитель определяет критерии для сбора и обработки информации, используемой при определении профиля процесса. Критерии должны учитывать тип собираемой информации, размер выборки данных, способы обеспечения репрезентативности собранных данных для пользователей, связь информации с рассматриваемыми угрозами и условиями, влияющими на выполнение процесса, возможность отслеживания данных и результатов выполнения процесса.

В.2.9 Определение модели процесса

Руководитель должен определить, какая эталонная модель процесса может быть использована. Для выбора модели рассматриваемого процесса учитываются возможные показатели, модели, методы и рекомендации по ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 33003, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59329 — ГОСТ Р 59357, ГОСТ Р 59989 — ГОСТ Р 59994, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

Обоснование сделанного выбора подлежит документированию.

В.2.10 Описание профиля процесса

В описании профиля каждого процесса предоставляются:

- имя и идентификатор процесса;
- цель процесса;
- эталонная модель процесса;
- информация о прослеживаемости от собираемых данных до характеристик требуемого уровня качества процесса или свойств процесса;
- требуемые свойства процесса и рейтинг свойств для каждой определенной характеристики вместе с обоснованием требуемых свойств процесса. В обосновании указывается, какие базовые и общие модели, методы, методики необходимы для оценки требуемых свойств процесса;
- рекомендации по использованию.

В качестве дополнительной может быть представлена информация:

- о способах идентификации процессов, влияющих на достижение требований системной инженерии в области применения;
- о дополнительных процессах, методах и методиках, которые помогают достичь реализации требований системной инженерии.

В.2.11 Определение показателей достижения качества процесса

Степень достижения качества процесса оценивается выбранным показателем (показателями). Полное определение профиля процесса включает в себя оценку целевого использования процесса и любую дополнительную информацию, связанную с использованием в соответствии с 6.3. Рекомендации по количественным показателям см. в приложении Г.

Приложение Г
(справочное)

Типовые показатели, модели и методы прогнозирования рисков

В данном приложении приведены ссылки на стандарты системной инженерии, содержащие рекомендации по типовым количественным показателям, моделям и методам прогнозирования рисков во всех системных процессах, свойственных жизненному циклу систем по ГОСТ Р 57193 (см. таблицу Г.1). Эти показатели, методы и модели в полной мере применимы для формирования профиля процессов, а также для решения задач системного анализа.

Таблица Г.1 — Ссылки на типовые модели и методы прогнозирования рисков

Системный процесс	Вероятностные показатели риска	Типовые модели и методы
Процессы приобретения и поставки продукции и услуг для системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59329—2021 (приложение В)
Процесс управления моделью жизненного цикла системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); обобщенный риск нарушения реализации процесса с учетом дополнительных специфических системных требований (в том числе на примере требований по защите информации)	По ГОСТ Р 59330—2021 (приложение В), ГОСТ Р 59992—2022 (приложение В)
Процесс управления инфраструктурой системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); обобщенный риск нарушения реализации процесса с учетом дополнительных специфических системных требований (в том числе на примере требований по защите информации)	По ГОСТ Р 59331—2021 (приложение В), ГОСТ Р 59993—2022, (приложение В)
Процесс управления портфелем проектов	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59332—2021 (приложение В)
Процесс управления человеческими ресурсами системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59333—2021 (приложение В)

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели риска	Типовые модели и методы
Процесс управления качеством системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); обобщенный риск нарушения реализации процесса с учетом дополнительных специфических системных требований (в том числе на примере требований по защите информации)	По ГОСТ Р 59334—2021 (приложение В), ГОСТ Р 59989—2022 (приложение В)
Процесс управления знаниями о системе	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59335—2021 (приложение В)
Процесс планирования проекта	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59336—2021 (приложение В)
Процесс оценки и контроля проекта	Для системных процессов риски по ГОСТ Р 59337—2021 (подраздел 6.3) (с учетом дополнительных специфических системных требований на примере требований по защите информации) и по ГОСТ Р 59990—2022 (подраздел 6.3)	По ГОСТ Р 59337—2021 (приложение В), ГОСТ Р 59990—2022 (приложение В)
Процесс управления решениями	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59338—2021 (приложение В)
Процесс управления рисками для системы	Для системных процессов риски по ГОСТ Р 59339—2021 (подраздел 6.3) (с учетом дополнительных специфических системных требований на примере требований по защите информации); интегральные риски нарушения качества системы в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза по ГОСТ Р 59991—2022 (подраздел 6.3)	По ГОСТ Р 59339—2021 (приложение В), ГОСТ Р 59991—2022 (приложение В)
Процесс управления конфигурацией системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59340—2021 (приложение В)

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели риска	Типовые модели и методы
Процесс управления информацией системы	Риск нарушения надежности реализации процесса как такового (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примерах требований к надежности и своевременности представления, полноты и достоверности выходной информации, требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примерах требований к надежности и своевременности представления, полноты и достоверности выходной информации, требований по защите информации)	По ГОСТ Р 59341—2021 (приложение В)
Процесс измерений системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59342—2021 (приложение В)
Процесс гарантии качества для системы	Для системных процессов риски по ГОСТ Р 59339—2021 (подраздел 6.3); интегральные риски нарушения качества системы по ГОСТ Р 59991—2022 (подраздел 6.3)	По ГОСТ Р 59994—2022 (приложение В)
Процесс анализа бизнеса или назначения системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59344—2021 (приложение В)
Процесс определения потребностей и требований заинтересованной стороны для системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59345—2021 (приложение В)
Процесс определения системных требований (на примере требований по защите информации)	Частные показатели риска реализации угроз безопасности информации, направленных на нарушение функционирования системы, в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения функционирования системы); частные показатели риска реализации угроз утечки конфиденциальной информации в условиях отсутствия мер защиты, предлагаемых к применению в ходе формирования системных требований, и в условиях их применения (показатели остаточного риска нарушения требований по защите конфиденциальной информации в системе или о системе);	По ГОСТ Р 59346—2021 (приложения В, Д)

Продолжение таблицы Г.1

Системный процесс	Вероятностные показатели риска	Типовые модели и методы
	интегральные показатели риска реализации угроз, направленных на нарушение функционирования системы в течение ее жизненного цикла, в условиях отсутствия и применения мер защиты, предлагаемых в ходе формирования системных требований. Примечание — Приведенные показатели демонстрируют возможности модификации показателей прогнозируемых рисков.	
Процесс определения архитектуры системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59347—2021 (приложение В)
Процесс определения проекта	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59348—2021 (приложение В)
Процесс системного анализа	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59349—2021 (приложение В)
Процесс реализации системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59350—2021 (приложение В)
Процесс комплексирования системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); - риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); - риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59351—2021 (приложение В)

Окончание таблицы Г.1

Системный процесс	Вероятностные показатели риска	Типовые модели и методы
Процесс верификации системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); - риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); - риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59352—2021 (приложение В)
Процесс передачи системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); - риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); - риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59353—2021 (приложение В)
Процесс аттестации системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59354—2021 (приложение В)
Процесс функционирования системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59355—2021 (приложение В)
Процесс сопровождения системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59356—2021 (приложение В)
Процесс изъятия и списания системы	Риск нарушения надежности реализации процесса (без учета дополнительных требований); риск нарушения дополнительных специфических системных требований (на примере требований по защите информации); риск нарушения реализации процесса с учетом дополнительных специфических системных требований (на примере требований по защите информации)	По ГОСТ Р 59357—2021 (приложение В)

Методический подход к прогнозированию интегрального риска нарушения качества системы в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза приведен в ГОСТ Р 59991—2022 (В.4 приложения В). Интегральную вероятность сохранения качества системы в сценарных условиях комбинации используемых системных процессов в течение задаваемого периода прогноза вычисляют как дополнение до единицы вероятностного значения интегрального риска нарушения качества системы.

Примером практического подхода к прогнозированию рисков является ГОСТ Р 58494, в котором положения системной инженерии адаптированы к системам дистанционного контроля промышленной безопасности в опасном производстве.

Примечания

1 Другие возможные показатели, модели, методы и рекомендации по оценке рисков приведены в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р МЭК 61069-1 — ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-5 — ГОСТ Р МЭК 61508-7.

2 Примеры прогнозирования рисков и решения задач системного анализа, связанные с прогнозированием рисков в процессах, приведены в ГОСТ Р 59331, ГОСТ Р 59333, ГОСТ Р 59335, ГОСТ Р 59338, ГОСТ Р 59341, ГОСТ Р 59345, ГОСТ Р 59346, ГОСТ Р 59347, ГОСТ Р 59356.

Приложение Д
(справочное)

Рекомендации по определению допустимых значений рисков

С точки зрения количественной оценки рисков, характеризующих приемлемый уровень целостности рассматриваемых процессов и системы, предъявляемые требования системной инженерии подразделяют на требования при допустимых рисках, обосновываемых по прецедентному принципу (см. ГОСТ Р 59339, ГОСТ Р 59343, ГОСТ Р 59991), и требования при рисках, свойственных реальной или гипотетичной системе-эталону. При формировании требований системной инженерии осуществляют обоснование достижимости целей рассматриваемых процессов и системы, учитывают важность и специфику системы, ограничения на стоимость создания и эксплуатации системы, другие требования и условия, включая требования к специальным показателям, связанным с критичными сущностями, характеризующими качество процессов и системы в целом.

Требования при принимаемых рисках, свойственных системе-эталону, являются наиболее жесткими, они не учитывают специфики рассматриваемой системы, а ориентируются лишь на мировые технические и технологические достижения для удовлетворения требований заинтересованных сторон и рационального решения задач системного анализа. Полной проверке на соответствие этим требованиям подлежат система в целом, составляющие ее подсистемы и реализуемые процессы жизненного цикла. Выполнение этих требований является гарантией обеспечения качества рассматриваемых процессов и системы. Вместе с тем проведение работ системной инженерии с ориентацией на риски, свойственные системе-эталону, характеризуются существенно бóльшими затратами по сравнению с требованиями, ориентируемыми на допустимые риски, обосновываемые по прецедентному принципу. Это заведомо удорожает разработку самой системы, увеличивает время до ее принятия в эксплуатацию и удорожает эксплуатацию.

Требования системной инженерии при допустимых рисках, свойственных конкретной системе или ее аналогу и обосновываемых по прецедентному принципу, являются менее жесткими, а их реализация — менее дорогостоящей по сравнению с требованиями для рисков, свойственных системе-эталону. Использование данного варианта требований обусловлено тем, что на практике может оказаться нецелесообразной (из-за использования ранее зарекомендовавших себя технологий, по экономическим или по другим соображениям) или невозможной ориентация на допустимые риски, свойственные системе-эталону. Вследствие этого минимальной гарантией обеспечения качества для рассматриваемых процессов и системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

Ссылочные рекомендации по определению допустимых значений показателей приведены в таблице Д.1 (учет дополнительных специфических системных требований в ссылочных стандартах дан на примере требований по защите информации). При этом период прогноза для расчетных показателей подбирают таким образом, чтобы вероятностные значения рисков не превышали допустимые. В этом случае для задаваемых при моделировании условий имеют место гарантии удержания рисков для рассматриваемого процесса в течение задаваемого периода прогноза.

Таблица Д.1 — Ссылки для определения допустимых значений рисков

Системный процесс	Определение допустимых значений рисков при ориентации на обоснование по прецедентному принципу и обоснование для системы-эталона
Процессы приобретения и поставки продукции и услуг для системы	По ГОСТ Р 59329—2021 (приложение Г)
Процесс управления моделью жизненного цикла системы	По ГОСТ Р 59330—2021 (приложение Г), ГОСТ Р 59992—2022 (приложение Г)
Процесс управления инфраструктурой системы	По ГОСТ Р 59331—2021 (приложение Д), ГОСТ Р 59993—2022 (приложение Г)
Процесс управления портфелем проектов	По ГОСТ Р 59332—2021 (приложение Г)
Процесс управления человеческими ресурсами системы	По ГОСТ Р 59333—2021 (приложение Д)
Процесс управления качеством системы	По ГОСТ Р 59334—2021 (приложение Г), ГОСТ Р 59989—2022 (приложение Г)
Процесс управления знаниями о системе	По ГОСТ Р 59335—2021 (приложение Д)
Процесс планирования проекта	По ГОСТ Р 59336—2021 (приложение Г)

Окончание таблицы Д.1

Системный процесс	Определение допустимых значений рисков при ориентации на обоснование по прецедентному принципу и обоснование для системы-эталона
Процесс оценки и контроля проекта	По ГОСТ Р 59337—2021 (приложение Г), ГОСТ Р 59990—2022 (приложение Г)
Процесс управления решениями	По ГОСТ Р 59338—2021 (приложение Д)
Процесс управления рисками для системы	По ГОСТ Р 59339—2021 (приложение Д), ГОСТ Р 59991—2022 (приложение Д)
Процесс управления конфигурацией системы	По ГОСТ Р 59340—2021 (приложение Г)
Процесс управления информацией системы	По ГОСТ Р 59341—2021 (приложение Д)
Процесс измерений системы	По ГОСТ Р 59342—2021 (приложение Г)
Процесс гарантии качества для системы	По ГОСТ Р 59343—2021 (приложение Д), настоящая таблица
Процесс анализа бизнеса или назначения системы	По ГОСТ Р 59344—2021 (приложение Г)
Процесс определения потребностей и требований заинтересованной стороны для системы	По ГОСТ Р 59345—2021 (приложение Д)
Процесс определения системных требований	По ГОСТ Р 59346—2021 (приложение Е)
Процесс определения архитектуры системы	По ГОСТ Р 59347—2021 (приложение Д)
Процесс определения проекта	По ГОСТ Р 59348—2021 (приложение Г)
Процесс системного анализа	По ГОСТ Р 59349—2021 (приложение Д)
Процесс реализации системы	По ГОСТ Р 59350—2021 (приложение Г)
Процесс комплексирования системы	По ГОСТ Р 59351—2021 (приложение Г)
Процесс верификации системы	По ГОСТ Р 59352—2021 (приложение Г)
Процесс передачи системы	По ГОСТ Р 59353—2021 (приложение Г)
Процесс аттестации системы	По ГОСТ Р 59354—2021 (приложение Г)
Процесс функционирования системы	По ГОСТ Р 59355—2021 (приложение Д)
Процесс сопровождения системы	По ГОСТ Р 59356—2021 (приложение Д)
Процесс изъятия и списания системы	По ГОСТ Р 59357—2021 (приложение Г)

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.020

Ключевые слова: безопасность, гарантии, качество, модель, риск, система, управление

Редактор *Л.В. Коретникова*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 17.06.2024. Подписано в печать 27.06.2024. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,18.

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.
gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru