ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59992— 2022

Системная инженерия

СИСТЕМНЫЙ АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ МОДЕЛЬЮ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ

Издание официальное

Москва
Российский институт стандартизации
2022

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 17 августа 2022 г. № 772-ст

4 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 (www.rst.gov.ru)

© Оформление. ФГБУ «РСТ», 2022

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

Введение

На основе использования системного анализа настоящий стандарт расширяет комплекс национальных стандартов системной инженерии для оценки достижимости требуемого качества, безопасности и эффективности системы, прогнозирования рисков, связанных с реализацией системных процессов, и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах. Выбор и применение системных процессов в жизненном цикле системы осуществляют по ГОСТ Р 57193. В общем случае применительно к системам различного функционального назначения системный анализ используют для следующих системных процессов:

- процессов соглашения — процессов приобретения и поставки продукции и услуг для системы;
- процессов организационного обеспечения проекта — процессов управления моделью жизненного цикла, инфраструктурой, портфелем проектов, человеческими ресурсами, качеством, знаниями;
- процессов технического управления — процессов планирования проекта, оценки и контроля проекта, управления решениями, рисками, конфигурацией, информацией, измерений, гарантии качества;
- технических процессов — процессов анализа бизнеса или назначения, определения потребностей и требований заинтересованной стороны, определения системных требований, определения архитектуры, определения проекта, системного анализа (т. е. непосредственно к самому себе как к процессу), реализации, комплексирования, верификации, передачи системы, аттестации, функционирования, сопровождения, изъятия и списания системы.

Стандарт устанавливает основные требования системной инженерии по системному анализу процесса управления моделью жизненного цикла системы, специальные требования к используемым количественным показателям, способам формализации, моделям, методам и используемым критериям при решении задач системного анализа. Для планируемого и реализуемого процесса управления моделью жизненного цикла применение настоящего стандарта при создании (модернизации, развитии), эксплуатации системы и выведении ее из эксплуатации обеспечивает решение задач системного анализа с использованием специальных показателей, связанных с критичными сущностями модели жизненного цикла системы, частных и интегральных показателей прогнозируемых рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

СИСТЕМНЫЙ АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ МОДЕЛЬЮ ЖИЗНЕННОГО ЦИКЛА СИСТЕМЫ

System engineering. System analysis of system life cycle model management process

Дата введения — 2022—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа процесса управления моделью жизненного цикла для систем различных областей применения.

Для практического применения в приложениях А—Д приведены примеры перечней решаемых задач системного анализа и угроз нарушения нормальной реализации процесса управления моделью жизненного цикла системы, типовые модели и методы прогнозирования рисков, рекомендации по определению допустимых значений показателей рисков, а также рекомендации по перечню методик системного анализа процесса.

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем, выведении их из эксплуатации и реализующими процесс управления моделью жизненного цикла системы — см. примеры систем в [1]—[21].

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ 2.102 Единая система конструкторской документации. Виды и комплектность конструкторских документов

ГОСТ 2.114 Единая система конструкторской документации. Технические условия

ГОСТ 2.602 Единая система конструкторской документации. Ремонтные документы

ГОСТ 3.1001 Единая система технологической документации. Общие положения

ГОСТ 7.32 Система стандартов по информации, библиотечному и издательскому делу. Отчет о научно-исследовательской работе. Структура и правила оформления

ГОСТ 15.016 Система разработки и постановки продукции на производство. Техническое задание. Требования к содержанию и оформлению

ГОСТ 34.201 Информационные технологии. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем

ГОСТ 34.601 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 34.602 Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы

ГОСТ 33981 Оценка соответствия. Исследование проекта продукции

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

ГОСТ Р 2.601 Единая система конструкторской документации. Эксплуатационные документы

Издание официальное

ГОСТ Р 15.101 Система разработки и постановки продукции на производство. Порядок выполнения научно-исследовательских работ

ГОСТ Р 15.301 Система разработки и постановки продукции на производство. Продукция производственно-технического назначения. Порядок разработки и постановки продукции на производство

ГОСТ Р 22.10.01 Безопасность в чрезвычайных ситуациях. Оценка ущерба. Термины и определения

ГОСТ Р ИСО 3534-1 Статистические методы. Словарь и условные обозначения. Часть 1. Общие статистические термины и термины, используемые в теории вероятностей

ГОСТ Р ИСО 3534-2 Статистические методы. Словарь и условные обозначения. Часть 2. Прикладная статистика

ГОСТ Р ИСО 7870-1 Статистические методы. Контрольные карты. Часть 1. Общие принципы

ГОСТ Р ИСО 7870-2 Статистические методы. Контрольные карты. Часть 2. Контрольные карты Шухарта

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

ГОСТ Р ИСО 11231 Менеджмент риска. Вероятностная оценка риска на примере космических систем

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

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/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 15704 Промышленные автоматизированные системы. Требования к стандартным архитектурам и методологиям предприятия

ГОСТ Р ИСО/МЭК 16085 Менеджмент риска. Применение в процессах жизненного цикла систем и программного обеспечения

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

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

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р ИСО/МЭК 27003 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27005—2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 50779.41 (ИСО 7879—93) Статистические методы. Контрольные карты для арифметического среднего с предупреждающими границами

ГОСТ Р 50779.70 (ИСО 28590:2017) Статистические методы. Процедуры выборочного контроля по альтернативному признаку

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 51275 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

ГОСТ Р 51583 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения

ГОСТ Р 51897/Руководство ИСО 73:2009 Менеджмент риска. Термины и определения

ГОСТ Р 51901.1 Менеджмент риска. Анализ риска технологических систем

ГОСТ Р 51901.5 (МЭК 60300-3-1:2003) Менеджмент риска. Руководство по применению методов анализа надежности

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 53647.1 Менеджмент непрерывности бизнеса. Часть 1. Практическое руководство

ГОСТ Р 54124 Безопасность машин и оборудования. Оценка риска

ГОСТ Р 54145 Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Общая методология

ГОСТ Р 56923/ISO/IEC TR 24748-3:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 3. Руководство по применению ИСО/МЭК 12207 (Процессы жизненного цикла программных средств)

ГОСТ Р 56939 Защита информации. Разработка безопасного программного обеспечения. Общие требования

ГОСТ Р 57102/ISO/IEC TR 24748-2:2011 Информационные технологии. Системная и программная инженерия. Управление жизненным циклом. Часть 2. Руководство по применению ИСО/МЭК 15288

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

ГОСТ Р 57272.1 Менеджмент риска применения новых технологий. Часть 1. Общие требования

ГОСТ Р 57839 Производственные услуги. Системы безопасности технические. Задание на проектирование. Общие требования

ГОСТ Р 58045 Авиационная техника. Менеджмент риска при обеспечении качества на стадиях жизненного цикла. Методы оценки и критерии приемлемости риска

ГОСТ Р 58412 Защита информации. Разработка безопасного программного обеспечения. Угрозы безопасности информации при разработке программного обеспечения

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 Системная инженерия. Защита информации в процессах приобретения и поставки продукции и услуг для системы

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

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

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

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

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

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

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

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

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

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

ГОСТ Р 59340 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 Системная инженерия. Защита информации в процессе измерений системы

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

ГОСТ Р 59344 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 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 Системная инженерия. Защита информации в процессе определения проекта

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

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

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

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

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

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

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

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

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

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

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

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 62508 Менеджмент риска. Анализ влияния на надежность человеческого фактора

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, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 51275, ГОСТ Р 51897, ГОСТ Р 59330, ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р МЭК 61508-4, а также следующие термины с соответствующими определениями:

3.1.1

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

[ГОСТ Р 51898—2002, пункт 3.7]

3.1.2

жизненный цикл (life cycle): Развитие системы, продукции, услуги, проекта или другой создаваемой человеком сущности от замысла до списания.

[ГОСТ Р 57193—2016, пункт 4.1.19]

3.1.3 **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.

3.1.4

модель жизненного цикла (life cycle model): Структурная основа процессов и действий, относящихся к жизненному циклу, которая также служит в качестве общего эталона для установления связей и понимания.

[ГОСТ Р 57193—2016, пункт 4.1.20]

3.1.5 **надежность реализации процесса управления моделью жизненного цикла системы:** Свойство процесса управления моделью жизненного цикла системы сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса в заданных условиях его реализации в приемлемые сроки.

3.1.6 **обобщенный риск нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований:** Сочетание вероятности того, что будут нарушены надежность реализации процесса управления моделью жизненного цикла системы либо заданные дополнительные специфические системные требования, либо и то, и другое, с тяжестью возможного ущерба.

Примечание — Примером дополнительных специфических системных требований могут выступать, например, требования по защите информации — см. ГОСТ Р 59330.

3.1.7

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, пункт 3.2]

3.1.8

система (system): Комбинация взаимодействующих элементов, организованных для достижения одной или нескольких поставленных целей.

Примечания

1 Система может рассматриваться как какой-то продукт или как предоставляемые услуги, обеспечивающие этот продукт.

2 На практике интерпретация данного термина нередко уточняется с использованием ассоциативного существительного, например «система самолета». В некоторых случаях слово «система» может заменяться контекстно зависимым синонимом, например словом «самолет», хотя это может впоследствии затруднить восприятие системных принципов.

Адаптировано из ГОСТ Р 57193—2016, пункт 4.1.44

3.1.9 **система-эталон:** Реальная или гипотетичная система, которая по своим показателям обобщенного риска нарушения реализации рассматриваемого процесса с учетом дополнительных специфических системных требований принимается в качестве эталона для более полного удовлетворения требований заинтересованных сторон системы и рационального решения задач системного анализа.

3.1.10

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]

3.1.11 **системный анализ процесса управления моделью жизненного цикла системы:** Научный метод системного познания, предназначенный для решения практических задач системной инженерии путем представления рассматриваемых системы и/или процесса управления моделью жизненного цикла системы в виде приемлемой моделируемой системы.

Примечания

1 Метод содержит:

- измерение и оценку специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы, прогнозирование рисков, интерпретацию и анализ приемлемости получаемых результатов для рассматриваемых системы (и/или ее элементов) и/или процесса;
- определение с использованием моделирования существенных угроз и условий, способных при том или ином развитии событий негативно повлиять на модель жизненного цикла рассматриваемой системы (и/или ее элементов);
- обоснование с использованием моделирования упреждающих мер противодействия угрозам, обеспечивающих желаемые свойства рассматриваемых системы (и/или ее элементов) и/или процесса 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, охватываемым по требованиям заказчика.

3.1.12

стадия (stage): Период в пределах жизненного цикла некоторой сущности, который относится к состоянию ее описания или реализации.

[ГОСТ Р 57193—2016, пункт 4.1.41]

Примечания

1 Стадии относятся к периодам значительного продвижения системы и достижения запланированных сроков на протяжении жизненного цикла.

2 Стадии могут перекрывать друг друга.

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

4 Основные положения системной инженерии по системному анализу процесса управления моделью жизненного цикла системы

4.1 Общие положения

4.1.1 Организации используют процесс управления моделью жизненного цикла системы для обеспечения уверенности при создании (модернизации, развитии) и эксплуатации системы в ее эффективности.

Модель жизненного цикла системы представляет собой последовательность стадий и этапов, которые могут перекрываться и/или повторяться в соответствии с областью применения, масштабами, сложностью, потребностью в изменениях и возможностях системы. Выполнение процесса осуществляют для достижения конкретных целей и получения выходных результатов в жизненном цикле системы.

Для анализа достижимости требуемого качества, безопасности и эффективности системы, прогнозирования рисков, связанных с реализацией процесса управления моделью жизненного цикла системы, и обоснования эффективных предупреждающих мер по снижению этих рисков или их удержанию в допустимых пределах используют системный анализ процесса.

4.1.2 Проведение системного анализа процесса управления моделью жизненного цикла системы способствует рациональному решению задач системной инженерии на основе научно обоснованных целенаправленных технических и организационных усилий в жизненном цикле системы. Сами решаемые задачи системной инженерии связывают с целями рассматриваемой системы, ее масштабами, имеющими место вызовами и возможными угрозами нарушения качества, безопасности и эффективности системы в ее жизненном цикле. В общем случае проведение системного анализа связано с решением задач эффективного развития и комплексной безопасности сложных систем, включая задачи:

- реализации государственной стратегии в экономике;
- безопасности и устойчивого развития регионов и крупных городов;
- функционирования и развития сложных народнохозяйственных, инженерно-технических, энергетических, транспортных систем, систем связи и коммуникаций;
- защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера;
- безопасности оборонно-промышленного комплекса;
- развития критических технологий (например, базовых и критических военных и промышленных технологий для создания перспективных видов вооружения, военной и специальной техники; базовых технологий силовой электротехники; компьютерного моделирования; информационных и когнитивных технологий; технологий атомной энергетики; технологий информационных, управляющих, навигационных систем; технологий и программного обеспечения распределенных и высокопроизводительных вычислительных систем; технологий мониторинга и прогнозирования состояния окружающей среды, предотвращения и ликвидации ее загрязнения; технологий поиска, разведки, разработки месторождений полезных ископаемых и их добычи; технологий предупреждения и ликвидации чрезвычайных ситуаций природного и техногенного характера);
- безопасности критической информационной инфраструктуры, информационной и информационно-психологической безопасности;
- безопасности и защищенности, управления ресурсами эксплуатации критически и стратегически важных объектов и систем;
- энергетической и промышленной безопасности (в том числе функционирования и развития топливно-энергетического комплекса, нефтяной, газовой и нефтехимической промышленности, электроэнергетики, трубопроводного транспорта);
- ядерной и радиационной безопасности;
- безопасности горнодобывающей промышленности;
- качества и безопасности строительного комплекса, в том числе обоснования прочности, устойчивости и долговечности создаваемых объектов и конструкций;
- безопасности железнодорожного, авиационного и водного транспорта;
- биологической безопасности;
- продовольственной безопасности;
- экологической безопасности и охраны природы;
- безопасности освоения континентальных шельфов;
- безопасности систем жизнеобеспечения и жизнедеятельности человека;
- снижения экономических, экологических и социальных ущербов от природных и природно-техногенных катастроф и нарушений качества, безопасности и эффективности критически и стратегически важных объектов и систем.

Решение задач системной инженерии с использованием системного анализа процесса управления моделью жизненного цикла системы базируется:

- на формулировании непротиворечивых целей системного анализа в жизненном цикле рассматриваемой системы (см. 4.2 и 4.3);
- математически корректных постановках задач системного анализа, обеспечивающих научно обоснованное достижение сформулированных целей системного анализа применительно к рассматриваемым процессу (его выходным результатам и выполняемым действиям) и системе (см. 5.1, приложение А);
- выборе и/или разработке основных и вспомогательных показателей для всесторонних оценок и прогнозов, на определении способов формализации, выборе и/или разработке формализованных моделей, методов и критериев системного анализа для решения поставленных задач (см. 6.2, 6.3);
- использовании результатов системного анализа для принятия решений в системной инженерии.

4.1.3 При проведении системного анализа процесса управления моделью жизненного цикла системы руководствуются основными принципами, определенными в ГОСТ Р 59991. Все применяемые принципы должны быть согласованы с принципом целенаправленности осуществляемых действий.

4.1.4 Основные усилия системной инженерии при проведении системного анализа процесса управления моделью жизненного цикла системы сосредоточивают:

- на определении выходных результатов и действий, предназначенных для достижения целей процесса;
- определении потенциальных угроз и возможных сценариев возникновения и развития угроз для рассматриваемых модели жизненного цикла системы и процесса управления этой моделью;
- измерениях и оценках специальных показателей, связанных с критичными сущностями модели жизненного цикла системы;
- определении и прогнозировании рисков, подлежащих системному анализу;
- получении результатов системного анализа в виде, пригодном для решения задач системной инженерии, включая обоснование мер, направленных на практическое противодействие угрозам и достижение поставленных целей.

4.2 Стадии и этапы жизненного цикла системы

Процесс управления моделью жизненного цикла системы, подлежащий системному анализу, может быть использован на любой стадии жизненного цикла системы. Стадии и этапы работ по созданию (модернизации, развитию) и эксплуатации системы устанавливают в договорах, соглашениях и технических заданиях (ТЗ) с учетом специфики и условий функционирования системы. Перечень этапов и конкретных работ в жизненном цикле системы формируют с учетом требований ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.601, ГОСТ 34.602, ГОСТ Р 15.301, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 31000, ГОСТ Р 51583, ГОСТ Р 56923, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839. Процесс управления моделью жизненного цикла может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости содержать другие процессы.

4.3 Цели системного анализа

4.3.1 Цели системного анализа процесса управления моделью жизненного цикла системы формулируют исходя из назначения системы, решаемых задач системной инженерии и целей самого процесса. Определение целей процесса управления моделью жизненного цикла системы осуществляют по ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р 56923, ГОСТ Р 57102, ГОСТ Р 57193 в соответствии со спецификой, создаваемой (модернизируемой) и/или применяемой системы.

В общем случае главная цель процесса управления моделью жизненного цикла системы состоит в определении, сопровождении и обеспечении гарантий наличия в организации необходимых политик, процессов, моделей, инструментариев и процедур для их использования в жизненном цикле системы.

4.3.2 В системном анализе объектами исследований являются критичные сущности модели жизненного цикла рассматриваемой системы, непосредственно рассматриваемый процесс управления моделью жизненного цикла системы и связанные с ним системные процессы. Критичные сущности и процесс поэлементно и/или в совокупности представляют в виде моделируемой системы, принимаемой (с необходимым обоснованием) в качестве приемлемой для достижения поставленных целей системного анализа. Результаты моделирования, получаемые для моделируемой системы, распространяют на рассматриваемые процессы и модель жизненного цикла системы и используют надлежащим образом для решения задач системного анализа (с соответствующей интерпретацией результатов моделирования и выработкой практических рекомендаций) и прикладного решения задач системной инженерии при разработке (развитии, модернизации) и эксплуатации рассматриваемой системы, а также ее выведении из эксплуатации.

4.3.3 В общем случае основными целями системного анализа процесса управления моделью жизненного цикла системы являются:

- оценка специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы, и прогнозирование рисков, интерпретация и анализ приемлемости получаемых результатов, включая сравнение достигаемых или прогнозируемых значений показателей с допустимым уровнем на предмет выполнения задаваемых ограничений;
- определение с использованием моделирования существенных угроз и условий, способных при том или ином развитии событий в жизненном цикле негативно повлиять на свойства рассматриваемой системы (и/или ее элементов);

- определение и обоснование с использованием моделирования в жизненном цикле системы упреждающих мер противодействия угрозам и условий, обеспечивающих желаемые свойства рассматриваемых процесса и системы (и/или ее элементов) при задаваемых ограничениях в задаваемый период прогноза;

- обоснование с использованием моделирования предложений по обеспечению и повышению качества, безопасности и/или эффективности рассматриваемой системы (и/или ее элементов), включая совершенствование непосредственно самого системного анализа процесса управления моделью жизненного цикла системы.

5 Общие требования системной инженерии к системному анализу процесса управления моделью жизненного цикла системы

5.1 Общие требования системной инженерии к системному анализу процесса управления моделью жизненного цикла системы должны быть направлены на достижение сформулированных непротиворечивых целей системного анализа рассматриваемого процесса и практичное решение задач, математически корректно поставленных для достижения этих целей. Предъявляемые требования системной инженерии к системному анализу процесса управления моделью жизненного цикла системы должны обеспечивать:

а) решение основных задач системного анализа, главными из которых являются:

1) задачи оценки специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы,

2) задачи прогнозирования рисков, свойственных процессу управления моделью жизненного цикла системы,

3) задачи обоснования допустимых значений специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы, и допустимых рисков,

4) задачи определения существенных угроз и условий для рассматриваемых системы и процесса управления моделью жизненного цикла системы с использованием специальных показателей и прогнозируемых рисков,

5) комплекс задач поддержки принятия решений по обеспечению качества, безопасности и/или эффективности рассматриваемой системы в ее жизненном цикле;

б) решение вспомогательных задач совершенствования непосредственно самого системного анализа процесса управления моделью жизненного цикла системы.

5.2 Формальные постановки задач системного анализа должны быть ориентированы на достижение сформулированных целей при задаваемых условиях и ограничениях (природных, технических, ресурсных, стоимостных, временных, социальных, экологических). Пример перечня решаемых задач системного анализа процесса управления моделью жизненного цикла системы приведен в приложении А.

5.3 Общие требования системной инженерии устанавливают в ТЗ на разработку, модернизацию или развитие системы. Эти требования и методы их выполнения детализируют в ТЗ на составные части системы, в конструкторской, технологической и эксплуатационной документации, в спецификациях на поставляемые продукцию и/или услуги. Содержание требований формируют с учетом нормативно-правовых документов Российской Федерации, специфики, уязвимостей и угроз системе (см., например, ГОСТ 2.102, ГОСТ 2.114, ГОСТ 2.602, ГОСТ 3.1001, ГОСТ 7.32, ГОСТ Р 59330, ГОСТ Р 59337, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59355, [1]—[21]).

Поскольку элементы процесса управления моделью жизненного цикла системы могут использоваться на этапах, предваряющих получение и утверждение ТЗ, соответствующие требования системной инженерии к системному анализу этого процесса могут быть оговорены в рамках соответствующих договоров и соглашений.

5.4 Требования системной инженерии к системному анализу процесса управления моделью жизненного цикла системы призваны обеспечивать управление техническими и организационными усилиями по его планированию и реализации.

5.5 Область применения системного анализа процесса управления моделью жизненного цикла системы должна охватывать:

- специальные критичные сущности, контролируемые организацией применительно к модели жизненного цикла рассматриваемой системы (и/или ее элементам) для обеспечения ее качества, безопасности и эффективности, включая критичные сущности, связанные с достижением целей системной инженерии;

- критичные сущности, связанные с учетом дополнительных специфических системных требований к управлению моделью жизненного цикла системы (например, требований по защите информации — см. ГОСТ Р 59330);

- проектные и запроектные условия возникновения и развития возможных угроз качеству, безопасности и эффективности системы, связанные с моделью ее жизненного цикла.

Пример перечня возможных угроз нарушения нормальной реализации процесса управления моделью жизненного цикла системы приведен в приложении Б.

5.6 Системный анализ процесса осуществляют с использованием количественных показателей, моделей, методов и методик (см. приложения В, Г, Д) с учетом рекомендаций ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58771, ГОСТ Р 59330, ГОСТ Р МЭК 61069-2, ГОСТ Р МЭК 61069-3, ГОСТ Р МЭК 61069-4, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7, ГОСТ Р МЭК 61069-8, ГОСТ Р МЭК 61508-5, ГОСТ Р МЭК 61508-7.

6 Специальные требования к количественным показателям

6.1 Общие положения

6.1.1 Для анализа достижимости требуемых качества, безопасности и эффективности системы, прогнозирования рисков, связанных с реализацией системных процессов, и обоснования эффективных предупреждающих действий по снижению этих рисков или их удержанию в допустимых пределах используют устанавливаемые качественные и количественные показатели.

Качественные показатели для оценки рисков обусловливают необходимостью выполнения конкретных требований, задаваемых на вербальном уровне в ТЗ и иных нормативно-правовых документах.

Примечание — Например, ряд качественных показателей в области обеспечения информационной безопасности определен в ГОСТ Р ИСО/МЭК 27005.

6.1.2 Требования к количественным показателям системного анализа в процессе управления моделью жизненного цикла системы должны учитывать:

- критичные сущности системы (и/или ее элементов), связанные с моделью ее жизненного цикла, включая критичные сущности, связанные с достижением целей системной инженерии;

- требования заинтересованных сторон, имеющих интерес к рассматриваемой системе, выходные результаты и выполняемые действия процесса управления моделью жизненного цикла системы;

- потенциальные угрозы для выходных результатов и выполняемых действий процесса управления моделью жизненного цикла системы, а также возможные сценарии возникновения и развития этих угроз;

- практическую интерпретацию оцениваемых специальных показателей и вероятностных результатов прогнозирования рисков при планировании и реализации процесса управления моделью жизненного цикла системы, возможные предупреждающие меры по снижению рисков или их удержанию в допустимых пределах;

- способы дальнейшего использования результатов оценки специальных показателей и прогнозирования рисков для решения задач системного анализа;

- методы использования результатов системного анализа для решения практических задач системной инженерии.

6.1.3 В общем случае состав выходных результатов и выполняемых действий в процессе управления моделью жизненного цикла системы, подлежащие учету при решении задач системного анализа, определяют по ГОСТ 2.114, ГОСТ Р 15.101, ГОСТ 34.201, ГОСТ 34.602, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р 56923, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 59330. При этом учитывают специфику рассматриваемой системы (см., например, [1]—[21]).

6.1.4 Основными выходными результатами процесса управления моделью жизненного цикла системы являются:

- политики организации в отношении жизненного цикла системы, процессов, моделей, инструментариев и процедур;

- документы, определяющие ответственность, подотчетность и полномочия должностных лиц в жизненном цикле системы;

- решения относительно поддержки процессов, моделей, инструментариев и процедур для их использования в организации;
- методики, связанные с совершенствованием модели жизненного цикла системы;
- отчеты о совершенствовании процесса управления моделью жизненного цикла системы.

6.1.5 Для получения выходных результатов процесса управления моделью жизненного цикла системы в общем случае выполняют следующие основные действия:

- определение политик и процедур для управления процессом и реализацию процесса согласно стратегиям организации;
- определение системных процессов, которые реализуют требования настоящего стандарта согласно стратегиям организации;
- определение ролей, ответственности, подотчетности и полномочий должностных лиц для реализации системных процессов и стратегического управления в жизненном цикле системы;
- определение бизнес-критериев, обеспечивающих управление развитием в течение жизненного цикла системы, включая критерии принятия решения относительно контрольных точек и перехода в различные стадии жизненного цикла системы;
- определение моделей жизненного цикла, описывающих необходимые стадии и этапы жизненного цикла систем, согласованные с целями и результатами для каждого этапа;
- сбор и системный анализ статистики, технических данных, результатов оценок и прогнозов для понимания слабых сторон рассматриваемого процесса. Использование результатов системного анализа в качестве обратной связи для совершенствования рассматриваемого процесса и внесения корректирующих изменений в текущие или последующие проекты;
- контроль выполнения рассматриваемого процесса в организации, включая обратную связь от выполняемых проектов относительно эффективности реализуемых системных процессов;
- проведение периодического анализа моделей жизненного цикла системы, используемых в различных проектах, включая анализ их реальной пригодности, адекватности и эффективности в каждом из проектов и оценку соответствующих улучшений;
- определение возможностей улучшения рассматриваемого процесса по результатам системного анализа;
- определение приоритетности в реализации улучшений;
- реализация совершенствующих улучшений, изучение и обобщение положительного опыта, информирование соответствующих заинтересованных сторон о достигнутых эффектах.

6.2 Требования к составу показателей

Используемые показатели должны обеспечивать решение основных и вспомогательных задач системного анализа процесса управления моделью жизненного цикла системы.

Степень достижения целей в жизненном цикле системы оценивают с помощью количественных показателей, которые позволяют сформировать представление о текущих и потенциальных задачах системной инженерии или о возможных причинах недопустимого снижения качества, безопасности и/или эффективности системы, начиная с самых ранних этапов, когда можно предпринять предупреждающие меры. Дополнительно могут быть использованы вспомогательные статистические показатели, характеризующие события, которые уже произошли, и их влияние на качество, безопасность и/или эффективность системы в ее жизненном цикле. Вспомогательные показатели позволяют исследовать произошедшие события, их последствия и сравнивать эффективность применяемых и/или возможных мер и действий непосредственно в процессе управления моделью жизненного цикла системы.

6.3 Требования к количественным показателям

6.3.1 Для решения задач системного анализа используют:

- специальные показатели, связанные с критичными сущностями модели жизненного цикла рассматриваемой системы (например, остаточный ресурс оборудования, оцениваемый с использованием измерения и моделирования);
- риск нарушения надежности реализации процесса управления моделью жизненного цикла системы;
- обобщенный риск нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований.

Примеры типовых моделей и методов прогнозирования рисков приведены в приложении В.

6.3.2 Расчетные риски характеризуют соответствующей вероятностью нанесения ущерба в сопоставлении с возможным ущербом.

6.4 Требования к источникам данных

Источниками исходных данных для расчетов количественных показателей являются (в части, свойственной процессу управления моделью жизненного цикла системы):

- источники, позволяющие сформировать данные, обеспечивающие оценку специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы;
- временны́е данные применения технологий противодействия угрозам и/или функционирования вспомогательных систем управления качеством и рисками, планируемых к использованию или используемых в рамках модели жизненного цикла рассматриваемой системы (в том числе данные о срабатывании исполнительных механизмов этих систем);
- текущие и статистические данные о состоянии параметров контролируемых критичных сущностей модели жизненного цикла рассматриваемой системы (привязанные к временам и условиям изменения состояний);
- текущие и статистические данные о самой системе или системах-аналогах, характеризующие не только данные о нарушениях надежности реализации рассматриваемого процесса, но и события, связанные с нарушениями и появлением предпосылок к нарушениям из-за реализации угроз применительно к модели жизненного цикла системы (привязанные к временам и условиям наступления событий, характеризующих соответствующие нарушения и предпосылки к нарушениям);
- текущие и статистические данные результатов контроля состояния рассматриваемой системы и вспомогательных систем управления качеством и рисками;
- наличие и готовность персонала системы, данные об ошибках персонала (привязанные к временам и условиям наступления событий, последовавших из-за этих ошибок и характеризующих нарушения и предпосылки к нарушениям) в самой системе или в системах-аналогах в части моделей их жизненного цикла;
- данные из различных моделей угроз (например, модели угроз безопасности информации) и метаданные, позволяющие сформировать перечень потенциальных угроз и возможные сценарии возникновения и развития угроз нарушения нормальной реализации процесса управления моделью жизненного цикла системы.

Типовые исходные данные для моделирования приведены в приложении В.

7 Требования к методам системного анализа процесса управления моделью жизненного цикла системы

7.1 Общие положения

7.1.1 В системной инженерии используют любые научно обоснованные формализованные методы, обеспечивающие достижение целей и решение поставленных задач системного анализа процесса управления моделью жизненного цикла системы.

7.1.2 Требования к формализованным методам системного анализа процесса управления моделью жизненного цикла системы включают:

- требования к моделям и методам оценки специальных показателей и обоснования их допустимых значений;
- требования к моделям и методам прогнозирования рисков и обоснования допустимых рисков;
- требования к методам определения существенных угроз и условий;
- требования к методам поддержки принятия решений в жизненном цикле системы.

7.1.3 При обосновании и формулировании требований к методам системного анализа руководствуются положениями 7.2—7.6 с учетом специфики системы и рекомендаций ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.602, ГОСТ 33981, ГОСТ IEC 61508-3, ГОСТ Р ИСО 3534-1, ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО 31000, ГОСТ Р 50779.41, ГОСТ Р 50779.70, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57272.1, ГОСТ Р 57839, ГОСТ Р 58045, ГОСТ Р 58412, ГОСТ Р 59330, ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7.

7.2 Требования к моделям и методам оценки специальных показателей

Модели и методы оценки специальных показателей должны быть связаны с целями рассматриваемой системы, ее масштабами, имеющими место вызовами и возможными угрозами для системы.

В качестве исходных используются данные, получаемые по факту, например в процессе функционирования системы. В общем случае с использованием расчетных специальных показателей применение моделей и методов должно способствовать рациональному решению задач системной инженерии, например задач, приведенных в 4.1.2.

7.3 Требования к моделям и методам прогнозирования рисков

7.3.1 Выбираемые и/или разрабатываемые модели и методы прогнозирования рисков должны обеспечивать достижение сформулированных целей системного анализа для условий неопределенности и практичное решение задач, поставленных для достижения этих целей (см. 4.3 и приложение А).

7.3.2 Прогнозирование рисков используют для формального решения задач системного анализа, связанных с ранним распознаванием и оценкой развития предпосылок к нарушению качества, безопасности и/или эффективности системы, обоснованием эффективных предупреждающих мер по снижению рисков или удержанию рисков в допустимых пределах, определением существенных угроз, поддержкой принятия решений в системной инженерии, в том числе по выполнению процесса управления моделью жизненного цикла системы. В зависимости от целей решаемых задач прогнозируемый риск связывают с заранее определенным периодом прогноза (например, на месяц, год, на несколько лет), с возможными сценариями возникновения и развития угроз, ожидаемых для этого периода.

7.3.3 Для прогнозирования рисков при решении поставленных задач должны быть:

- определены потенциально существенные угрозы или условия, для которых при том или ином развитии событий возможно негативное воздействие на систему (см. приложение Б);
- определены количественные показатели прогнозируемых рисков, выбраны, адаптированы или разработаны модели и методы прогнозирования рисков, методики системного анализа (см. приложения В, Г, Д);
- реализованы сбор и обработка исходных данных, обеспечивающих применение моделей, методов и методик для прогнозирования рисков;
- предусмотрены способы использования результатов прогнозирования рисков для эффективного управления моделью жизненного цикла системы.

7.4 Требования к методам обоснования допустимых рисков

7.4.1 Допустимые риски выступают в качестве количественных норм эффективности мер противодействия угрозам (при выполнении процесса управления моделью жизненного цикла системы, обеспечении качества, безопасности и эффективности рассматриваемой системы). Значения допустимых рисков определяют применительно к риску нарушения надежности реализации процесса как такового и риску нарушения реализации процесса с учетом дополнительных специфических системных требований.

7.4.2 Методы обоснования допустимых рисков определяют до начала планирования и реализации рассматриваемого процесса и задают во внутренних документах организации. Допустимые риски могут быть установлены в договорах, соглашениях и ТЗ в качественной и/или количественной форме с учетом специфики системы. Основными являются методы количественного обоснования допустимых рисков по прецедентному принципу или с использованием ориентации на риски, свойственные системе-эталону, которая выбирается в качестве аналога для моделируемой системы. Общее описание методов обоснования допустимых рисков, применимых для процесса управления моделью жизненного цикла системы, приведено в ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р 59991 (см. также приложение Д).

7.5 Требования к методам определения существенных угроз и условий

7.5.1 Методы определения существенных угроз и условий, способных при том или ином развитии событий негативно повлиять на процесс управления моделью жизненного цикла системы или саму систему (и/или ее элементы), должны быть целенаправлены на раннее распознавание и оценку развития предпосылок к нарушению реализации рассматриваемого процесса и нарушению качества, безопасности и/или эффективности системы.

7.5.2 Определение существенных угроз и условий осуществляют по оценкам специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы, а также с использованием прогнозирования рисков. Общий алгоритм определения существенных угроз и условий, применимый для процесса управления моделью жизненного цикла системы, приведен в ГОСТ Р 59991 (см. также ГОСТ Р 59346).

Примечание — Противодействие выявленным угрозам по результатам системного анализа осуществляют согласно ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27003, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р 51583, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193 с учетом специфики системы и реализуемой стадии ее жизненного цикла.

7.6 Требования к методам поддержки принятия решений

7.6.1 Методы поддержки принятия решений в системной инженерии должны учитывать результаты прогнозирования рисков, обоснования допустимых рисков, эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах, определения существенных угроз и условий применительно к процессу управления моделью жизненного цикла системы. Применение методов должно быть ориентировано:

- на обеспечение надежности реализации процесса управления моделью жизненного цикла системы и обоснование мер для достижения его целей и целей системного анализа процесса;
- противодействие угрозам и определение сбалансированных решений системной инженерии при средне- и долгосрочном планировании (в части модели жизненного цикла системы);
- обоснование предложений по повышению качества, безопасности и/или эффективности системы и совершенствование системного анализа и методов решения задач системного анализа процесса управления моделью жизненного цикла системы.

Устанавливаемые при этом значения допустимых рисков играют роль ограничений для формального решения основных и вспомогательных задач системного анализа. В зависимости от целей решаемых задач допустимый риск связывают с заранее определенным периодом прогноза, используемыми сценариями возникновения и развития угроз, возможным ущербом, ожидаемым для этого периода прогноза.

7.6.2 Поддержка принятия решений по обеспечению реализации процесса управления моделью жизненного цикла системы основана на оценках специальных показателей, связанных с критичными сущностями модели жизненного цикла системы, и прогнозировании рисков (см. 7.1—7.3, приложение В). Это позволит определять в жизненном цикле системы приемлемые (для периода прогноза) нормы эффективности мер противодействия угрозам и решать задачи по определению существенных угроз и условий для процесса управления моделью жизненного цикла системы (см. 7.4, 7.5).

7.6.3 Поддержка принятия решений по обоснованию мер, направленных на достижение целей процесса управления моделью жизненного цикла системы и противодействие угрозам, основана на предварительных действиях. Следует заранее определить меры, направленные на обеспечение качества, безопасности и эффективности системы, определение существенных угроз и на восстановление приемлемых условий реализации процесса управления моделью жизненного цикла системы в случае определения предпосылок к нарушению или непосредственно следов произошедших нарушений из-за реализации угроз. Определение мер по обеспечению надежности реализации процесса управления моделью жизненного цикла системы осуществляют по ГОСТ IEC 61508-3, ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.7, ГОСТ Р 56939, ГОСТ Р 57272.1, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 61508-2, ГОСТ Р МЭК 61508-6, ГОСТ Р МЭК 61508-7 с учетом специфики системы и реализуемой стадии ее жизненного цикла. Для обоснования мер, направленных на достижение целей процесса и противодействие угрозам, следует использовать модели, методы и методики системного анализа и рекомендации по определению допустимых значений показателей рисков (см. приложения В, Г, Д).

Причины наступления событий, связанных с выявленными предпосылками к нарушениям качества, безопасности и/или эффективности системы, существенными угрозами и условиями, произошедшими нарушениями в процессе управления моделью жизненного цикла системы, регистрируют для недопущения подобных повторений и/или уточнения предупреждающих мер, обеспечения приемлемых условий реализации процесса и наполнения базы знаний.

7.6.4 Поддержка принятия сбалансированных решений системной инженерии при среднесрочном планировании (в части управления моделью жизненного цикла системы) основана на системном анализе значений расчетных показателей рисков. Срок прогноза — от недели или месяца до одного года, при долгосрочном прогнозе — от одного года до нескольких лет с учетом специфики системы.

При недопустимых значениях прогнозируемых рисков и/или при наступлении реальных нарушений в процессе управления моделью жизненного цикла системы должны быть выявлены их причины и определены меры для целенаправленного планового восстановления надежности выполнения процесса на уровне рисков, не превышающих допустимые.

При средне- и долгосрочном планировании (в части модели жизненного цикла системы) должен быть обеспечен баланс по критерию «эффективность — стоимость». Для обоснования сбалансированных решений системной инженерии при средне- и долгосрочном планировании используют модели, методы и методики системного анализа и рекомендации по снижению рисков и определению допустимых значений показателей рисков (см. приложения В, Г, Д).

7.6.5 Поддержка принятия решений по обоснованию предложений по повышению качества, безопасности и/или эффективности системы и совершенствованию непосредственно самого системного анализа должна быть основана на изучении значений расчетных показателей рисков при сроке прогноза от нескольких месяцев до нескольких лет. Реализация этих предложений должна быть учтена в долгосрочных планах организации.

Для обоснования предложений по повышению качества, безопасности и/или эффективности системы и совершенствованию непосредственно самого системного анализа процесса управления моделью жизненного цикла системы следует также использовать модели, методы и методики системного анализа и рекомендации по определению допустимых значений показателей рисков (см. приложения В, Г, Д).

Примечание — Примеры решения задач системного анализа в приложении к различным процессам см. в ГОСТ Р 54124, ГОСТ Р 58494, 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 А
(справочное)

Пример перечня решаемых задач системного анализа

А.1 В общем случае перечень решаемых задач системного анализа процесса управления моделью жизненного цикла системы формируют для достижения целей в жизненном цикле рассматриваемой системы с учетом ее масштабов, имеющих место вызовов и возможных угроз. В перечень основных включают следующие задачи системного анализа.

А.1.1 Задачи оценки специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы, для предотвращения ущерба и уменьшения размеров возможных негативных последствий. К таким задачам относят:

- задачи обработки и контроля данных о состоянии системы на различных стадиях и этапах ее жизненного цикла;
- задачи оценки остаточного ресурса системы и ее элементов;
- задачи оценки возможных прямых и косвенных экономических, экологических и социальных ущербов из-за нарушения реализации процесса управления моделью жизненного цикла системы.

А.1.2 Задачи обоснования допустимых значений специальных показателей, связанных с критичными сущностями модели жизненного цикла рассматриваемой системы, и допустимых рисков. Например, для моделируемой системы, представляющей собой промышленное оборудование, задают допустимые значения для характеристик остаточного ресурса оборудования, а также допустимое количество запасных частей и расходных материалов на складе.

А.1.3 Задачи определения существенных угроз и условий для модели жизненного цикла рассматриваемой системы с использованием специальных показателей и прогнозируемых рисков. К таким задачам относятся:

- задачи определения существенных факторов опасности — например, природных факторов, факторов, связанных с новыми технологиями и несовершенством применяемых технологий, факторов, воздействующих на информационные ресурсы системы;
- задачи анализа рисков при технической диагностике и оценке остаточного ресурса системы и ее элементов;
- задачи системной инженерии при проектировании, испытаниях и эксплуатации системы по показателям «эффективность — стоимость» (в части, связанной с моделью жизненного цикла рассматриваемой системы).

А.1.4 Комплекс задач поддержки принятия решений в системной инженерии (в части модели жизненного цикла рассматриваемой системы), связанных с обеспечением требуемого качества, безопасности и эффективности системы. К таким задачам относят задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам модели жизненного цикла системы по какому-либо из критериев оптимизации, например:

- задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам по критерию минимизации обобщенного риска нарушения реализации процесса с учетом дополнительных специфических системных требований в течение пяти лет при ограничениях на ресурсы, затраты и допустимые риски реализации отдельных существенных угроз, а также при иных корректных ограничениях;
- задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам по критерию минимизации общих затрат на реализацию кратко-, средне- и/или долгосрочных планов технического обслуживания системы при ограничениях на допустимые риски нарушения реализации процесса управления моделью жизненного цикла системы, а также при иных корректных ограничениях;
- комбинации перечисленных выше или иных оптимизационных задач применительно к системе или ее отдельным элементам.

А.2 В перечень вспомогательных задач системного анализа включают задачи совершенствования непосредственно самого системного анализа процесса управления моделью жизненного цикла системы. К таким задачам относят:

- задачи программно-целевого планирования системного анализа процесса управления моделью жизненного цикла системы и ее элементов;
- задачи оценки влияния процесса управления моделью жизненного цикла системы на ее качество, безопасность и эффективность;
- задачи обоснования способов повышения эффективности процесса управления моделью жизненного цикла системы.

Приложение Б
(справочное)

Пример перечня угроз нарушения нормальной реализации процесса управления моделью жизненного цикла системы

Перечень угроз нарушения нормальной реализации процесса управления моделью жизненного цикла системы может включать (в части, свойственной этому процессу):

- природные и природно-техногенные угрозы — по ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 54124, ГОСТ Р МЭК 61069-5, ГОСТ Р МЭК 61069-6, ГОСТ Р МЭК 61069-7;
- угрозы со стороны человеческого фактора — по ГОСТ Р МЭК 62508;
- угрозы, связанные с объективными и субъективными факторами, воздействующими на защищаемую информацию, — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51275;
- угрозы безопасности оборудования и коммуникаций, используемых в процессе работы системы, — по ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 59330, ГОСТ Р 59339;
- угрозы компрометации информационной безопасности приобретающей стороны (заказчика) — по ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27005—2010, приложение С;
- угрозы возникновения ущерба репутации и/или потери доверия поставщика (производителя) к конкретному заказчику, качество, безопасность или эффективность систем которого были скомпрометированы из-за нарушения рассматриваемого процесса;
- прочие соответствующие угрозы качеству, безопасности и эффективности системы, связанные с процессом управления моделью жизненного цикла системы.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Общие положения

В.1.1 Для прогнозирования рисков в процессе управления моделью жизненного цикла системы применяют любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. Применение типовых методов и моделей настоящего стандарта обеспечивает оценку следующих показателей:

- риска нарушения надежности реализации процесса управления моделью жизненного цикла системы без учета требований по защите информации — см. В.2;
- обобщенного риска нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований — см. В.3, В.4.

В.1.2 Риск нарушения надежности реализации процесса управления моделью жизненного цикла системы без учета дополнительных специфических системных требований характеризуют:

- риском невыполнения необходимых действий процесса, определяемым вероятностью невыполнения необходимых действий процесса;
- риском нарушения сроков выполнения необходимых действий, определяемым вероятностью нарушения сроков выполнения необходимых действий процесса.

Вероятностные оценки обеспечивают уровень адекватности, достаточный для решения задач системного анализа, при условии многократной повторяемости анализируемых событий или в предположении такой повторяемости.

В.1.3 Обобщенный риск нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований характеризуют сочетанием риска нарушения надежности реализации процесса управления моделью жизненного цикла системы без учета дополнительных специфических системных требований и риска нарушения этих дополнительных требований в рассматриваемом процессе.

В.1.4 Возможный ущерб, оцениваемый тяжестью последствий для системы и ее заинтересованных сторон в случае реализации угроз, сопоставляют с расчетными вероятностными показателями рисков

В.1.5 Для моделируемой системы нарушение реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований характеризуется переходом моделируемой системы в такое элементарное состояние, при котором имеет место или оказывается возможным ущерб по следующим причинам: либо из-за невыполнения необходимых действий процесса, либо из-за нарушения сроков выполнения необходимых действий, либо из-за нарушения дополнительных специфических системных требований, либо из-за комбинации перечисленных причин.

В.1.6 В общем случае исходя из целей системного анализа риски оценивают на разных исходных данных. При использовании одних и тех же моделей для расчетов это может приводить к различным оценкам и интерпретациям рисков. Различия связаны с неодинаковой тяжестью возможного ущерба для заинтересованных сторон (из-за невыполнения необходимых действий процесса, нарушения сроков выполнения необходимых действий процесса, нарушений дополнительных специфических системных требований), недоступностью или неполнотой статистических данных, используемых каждой из этих сторон в качестве исходных данных при системном анализе.

В.1.7 Выполнение или невыполнение действий и требований при моделировании отслеживается с использованием индикаторной функции $Ind(\alpha)$, которая позволяет учесть критичность последствий, связанных с невыполнением заданных условий согласно собираемой статистике

$$Ind(\alpha) = \begin{cases} 1, & \text{если условие } \alpha \text{ выполнено,} \\ 0, & \text{если условие } \alpha \text{ не выполнено.} \end{cases} \quad (В.1)$$

Условие α, используемое в индикаторной функции, формируют путем анализа выполнения конкретных условий.

В.1.8 При формировании исходных данных для моделирования и проведении разностороннего системного анализа используют статистические методы по ГОСТ Р ИСО 3534-2, ГОСТ Р ИСО 7870-1, ГОСТ Р ИСО 7870-2, ГОСТ Р 50779.41, методы оценки рисков из настоящего приложения и/или по ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59349, 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.

В.2 Прогнозирование риска нарушения надежности реализации процесса без учета дополнительных специфических системных требований

В.2.1 Общие положения

В.2.1.1 Надежность реализации процесса управления моделью жизненного цикла без учета дополнительных специфических системных требований представляет собой свойство процесса сохранять во времени в установленных пределах значения показателей, характеризующих способность выполнения необходимых действий процесса с обеспечением сроков их выполнения в интересах системы.

В.2.1.2 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для моделируемой системы или для системы, выбранной в качестве аналога. Для исследования запроектных сценариев развития угроз при моделировании могут быть использованы гипотетичные исходные данные.

В.2.1.3 Используется предположение, что нарушение надежности реализации процесса управления моделью жизненного цикла системы без учета дополнительных специфических системных требований является следствием невыполнения необходимых действий процесса и/или нарушения сроков выполнения необходимых действий процесса.

В.2.2 Оценка риска невыполнения необходимых действий процесса

В.2.2.1 Общие положения

Риск невыполнения необходимых действий процесса оценивают в виде вспомогательного показателя при проведении оценок обобщенного риска нарушения реализации процесса управления моделью жизненного цикла с учетом дополнительных специфических системных требований — см. В.4.

В реализуемом процессе должны быть выполнены необходимые действия. Невыполнение (в том числе незавершение выполнения) необходимых действий процесса управления моделью жизненного цикла системы — это угроза возможного ущерба. С точки зрения тяжести ущерба в случае невыполнения необходимых действий процесса все действия могут быть распределены по K группам, $K \geq 1$. В общем случае для каждой группы требования к выполнению процесса управления моделью жизненного цикла системы формулируют на уровне инструкций должностных лиц, участвующих в реализации процесса.

В.2.2.2 Метод оценки

При оценке риска вычисляют вероятность невыполнения необходимых действий процесса управления моделью жизненного цикла системы по отдельной группе действий или по всем действиям и делают сопоставление с возможным ущербом.

На основе применения статистических данных вероятность $R_{\text{действий } k}$ невыполнения необходимых действий процесса для k-й группы за задаваемое время $T_{\text{зад } k}$ вычисляют по формуле

$$R_{\text{действий } k}(T_{\text{зад } k}) = G_{\text{наруш } k}(T_{\text{зад } k})/G_k(T_{\text{зад } k}), \quad \text{(В.2)}$$

где $G_{\text{наруш } k}(T_{\text{зад } k})$ и $G_k(T_{\text{зад } k})$ — соответственно количество случаев нарушений при выполнении необходимых действий процесса и общее количество необходимых действий из k-й группы, подлежащих выполнению за заданное время $T_{\text{зад } k}$ согласно статистическим данным.

Вероятность $R_{\text{действий}}(T_{\text{зад}})$ невыполнения необходимых действий процесса по всему множеству действий согласно статистическим данным определяют по формулам:

- для варианта, когда учитывают все действия (как с завершенным выполнением, так и с их невыполнением)

$$R_{\text{действий}}(T_{\text{зад}}) = 1 - \sum_{k=1}^{K} W_k \left[1 - R_{\text{действий } k}(T_{\text{зад } k})\right] / \sum_{k=1}^{K} W_k; \quad \text{(В.3)}$$

- для варианта, когда учитывают лишь те случаи, для которых необходимые действия процесса не были выполнены или завершены требуемым образом (именно они определяют возможные ущербы от невыполнения процесса)

$$R_{\text{действий}}(T_{\text{зад}}) = 1 - \sum_{k=1}^{K} W_k \left[1 - R_{\text{действий } k}(T_{\text{зад } k})\right] Ind_{\text{действий}}(\alpha_k) / \sum_{k=1}^{K} W_k, \quad \text{(В.4)}$$

где $T_{\text{зад}}$ — задаваемое суммарное время на реализацию процесса для всего множества действий из различных групп, включающее все частные значения $T_{\text{зад } k}$ с учетом их наложений;

W_k — количество учитываемых действий из k-й группы при многократных реализациях процесса.

Для k-й группы учитывают требование к выполнению действий процесса с использованием индикаторной функции $Ind(\alpha) = Ind_{\text{действий}}(\alpha_k)$.

Индикаторная функция $Ind(\alpha) = Ind_{\text{действий}}(\alpha_k)$ позволяет учесть последствия, связанные с невыполнением необходимых действий процесса, — см. выражение (В.1). Условие α_k означает совокупность условий выполнения в требуемом объеме и завершения всех действий процесса при соблюдении ограничений на задаваемое время $T_{\text{зад } k}$.

Примечания

1 При соблюдении всех условий вероятностные оценки рисков по формулам (В.3), (В.4) совпадают.

2 Практическая ценность расчетов применения формул (В.2)—(В.4) проявляется при общем количестве необходимых действий процесса $G_k(T_{\text{зад } k})$, подлежащих выполнению за заданное время $T_{\text{зад k}}$, не менее 10 и количестве случаев невыполнения необходимых действий процесса $G_{\text{наруш } k}(T_{\text{зад } k}) > 0$, $k = 1, \ldots, K$, $K \geq 1$. Тем самым считают подтвержденными практические условия повторяемости анализируемых событий. При невыполнении этих условий делают предположение о многократной повторяемости анализируемых событий и для расчетов используют адаптированные математические модели для прогнозирования рисков нарушения надежности реализации системных процессов — см., например, В.3, ГОСТ Р 59330 (В.3 приложения В), ГОСТ Р 59341—2021 (В.3 приложения В), ГОСТ Р 59345—2021 (В.2 приложения В) и ГОСТ Р 59347—2021 (В.2 приложения В).

В.2.3 Оценка нарушения сроков выполнения необходимых действий процесса

В.2.3.1 Общие положения

Вероятность нарушения сроков выполнения необходимых действий процесса управления моделью жизненного цикла системы оценивают в виде вспомогательного показателя при проведении оценок обобщенного риска нарушения реализации процесса с учетом дополнительных специфических системных требований — см. В.4.

Каждое осуществляемое действие процесса, чтобы избежать ущербов, должно быть выполнено в задаваемые сроки. Нарушение сроков выполнения необходимых действий — это угроза возможного ущерба. С точки зрения важности, срочности действий и тяжести ущерба в случае нарушения сроков выполнения необходимые действия могут быть условно распределены по I группам, $I \geq 1$. В общем случае для каждой группы требования к своевременности формулируют в следующем виде: срок выполнения действий из i-й группы должен быть не более задаваемого $T_{зад\ i}$, $i = 1,\ldots,I$. Неприемлемость нарушения задаваемых сроков выполнения необходимых действий фиксируют в виде штрафных санкций, особых условий страхования ответственности и иных обязательств, направленных на недопущение нарушений сроков выполнения действий в процессе управления моделью жизненного цикла системы.

В.2.3.2 Метод оценки

При оценке риска вычисляют вероятность нарушения сроков выполнения действий процесса.

На основе применения статистических данных вероятность $R_{св\ i}$ нарушения сроков для однократного действия из i-й группы действий за задаваемое время $T_{зад\ i}$ вычисляют по формуле

$$R_{св\ i}(T_{зад\ i}) = N_{наруш\ i}(T_{зад\ i})/N_i(T_{зад\ i}), \quad (В.5)$$

где $N_{наруш\ i}(T_{зад\ i})$ и $N_i(T_{зад\ i})$ — соответственно количество случаев нарушений сроков выполнения необходимых действий и общее количество действий процесса из i-й группы за заданное время $T_{зад\ i}$ согласно статистическим данным.

Вероятность $R_{св}(T_{зад})$ нарушения сроков выполнения необходимых действий процесса по всему множеству действий процесса, реализуемых согласно статистическим данным, вычисляют по формулам:

- для варианта, когда учитывают все действия (как с выполненными, так и с нарушенными сроками их выполнения)

$$R_{св}(T_{зад}) = 1 - \sum_{i=1}^{I} M_i \left[1 - R_{св\ i}(T_{зад\ i})\right] / \sum_{i=1}^{I} M_i; \quad (В.6)$$

- для варианта, когда учитывают лишь те случаи, для которых сроки выполнения действий были нарушены (именно они определяют возможные ущербы от несвоевременного выполнения действий)

$$R_{св}(T_{зад}) = 1 - \sum_{i=1}^{I} M_i \left[1 - R_{св\ i}(T_{зад\ i})\right] Ind_{св}(\alpha_i) / \sum_{i=1}^{I} M_i, \quad (В.7)$$

где $T_{зад}$ — задаваемое суммарное время для выполнения всех действий, включающее в себя все частные значения $T_{зад\ i}$ с учетом их наложений,

M_i — количество учитываемых действий при многократных выполнениях процесса.

Для действий из i-й группы учитывают требование к срокам их выполнения с использованием индикаторной функции $Ind(\alpha) = Ind_{св}(\alpha_i)$. Индикаторная функция $Ind(\alpha) = Ind_{св}(\alpha_i)$ позволяет учесть последствия, связанные с несвоевременностью выполнений действий процесса. Условие α_i означает выполнение действий при ограничении на уровне задаваемого срока $T_{зад\ i}$.

Примечания

1 При соблюдении всех учитываемых условий вероятностные оценки рисков по формулам (В.6), (В.7) совпадают.

2 Практическая ценность расчетов применения формул (В.5)—(В.7) проявляется при общем количестве действий процесса $N_i(T_{зад\ i})$ за заданное время $T_{зад\ i}$ не менее 10 и количестве случаев нарушений сроков выполнения необходимых действий $N_{наруш\ i}(T_{зад\ i}) > 0$, $i = 1,\ldots,I$, $I \geq 1$. Тем самым считают подтвержденными практические условия повторяемости анализируемых событий. При невыполнении этих условий делают предположение о многократной повторяемости анализируемых событий и для расчетов используют адаптированные математические модели для прогнозирования рисков — см., например, приложение В.3, ГОСТ Р 59330 (В.3 приложения В), ГОСТ Р 59341—2021 (В.3 приложения В), ГОСТ Р 59345—2021 (В.2 приложения В) и ГОСТ Р 59347—2021 (В.2 приложения В).

В.3 Прогнозирование риска нарушения дополнительных специфических системных требований

В.3.1 Общие положения

Прогнозирование рисков нарушения дополнительных специфических системных требований осуществляют на основе применения специальных математических моделей, учитывающих специфику самих требований, а также технологий, мер и способов их выполнения.

Для прогнозирования риска нарушения дополнительных специфических системных требований применительно к процессу управления моделью жизненного цикла системы в полной мере применимы модели и методы прогнозирования риска нарушения дополнительных специфических системных требований из ГОСТ Р 59993—2022 (В.3 приложения В), изложенные применительно к процессу управления инфраструктурой системы. При этом для расчета вероятностных показателей применительно к моделируемой системе, где анализируемые сущности могут быть представлены в виде «черного ящика», используют исходные данные, формально определяемые применительно к процессу управления моделью жизненного цикла системы следующим образом:

σ — частота возникновения источников угроз нарушения дополнительных специфических системных требований в рассматриваемом процессе;

β — среднее время развития угроз с момента возникновения источников угроз до нарушения нормальных условий (например, до нарушения установленных дополнительных специфических системных требований в системе или до инцидента);

$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики возможностей по обеспечению выполнения дополнительных специфических системных требований в моделируемой системе;

$T_{диаг}$ — среднее время системной диагностики возможностей по обеспечению выполнения дополнительных специфических системных требований;

$T_{восст}$ — среднее время восстановления нарушенных возможностей по обеспечению выполнения дополнительных специфических системных требований в моделируемой системе;

$T_{зад}$ — задаваемая длительность периода прогноза.

Расчетные показатели:

$P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ — вероятность отсутствия нарушений дополнительных специфических системных требований в моделируемой системе в течение периода прогноза $T_{зад}$;

$R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ — вероятность нарушения дополнительных специфических системных требований в моделируемой системе в течение периода прогноза $T_{зад}$.

Расчет показателей применительно к процессу управления моделью жизненного цикла для моделируемой системы простой и сложной структуры осуществляют в полном соответствии с рекомендациями ГОСТ Р 59993—2022 (В.3 приложения В).

Расчет вероятности нарушения дополнительных специфических системных требований для процесса управления моделью жизненного цикла системы в течение периода прогноза $R_{наруш}(T_{зад}) = R_{наруш}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$ осуществляют как дополнение до единицы значения $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{восст}, T_{зад})$.

В.4 Прогнозирование обобщенного риска

В.4.1 Общие положения

Прогнозирование обобщенного риска нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований применяют при решении задач системного анализа — см. раздел 7. Риски оценивают с использованием расчетных вероятностей невыполнения необходимых действий процесса, нарушения сроков выполнения необходимых действий процесса (см. В.2) и нарушения дополнительных специфических системных требований (см. В.3) в сопоставлении с возможным ущербом.

В.4.2 Метод оценки

Вероятность нарушения надежности реализации процесса управления моделью жизненного цикла системы без учета дополнительных специфических системных требований $R_{без}(T_{зад})$ вычисляют по формулам:

- для варианта, когда учитывают все действия (как с выполненными, так и с нарушенными условиями по выполнению необходимых действий процесса и соблюдению сроков их выполнения)

$$R_{без}(T_{зад}) = 1 - \left\{ \sum_{k=1}^{K} W_k \left[1 - R_{действий\ k}(T_{зад\ k}) \right] + \sum_{i=1}^{I} M_i \left[1 - R_{св\ i}(T_{зад\ i}) \right] \right\} / \left(\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i \right); \quad (В.8)$$

- для варианта, когда учитывают лишь те случаи, для которых условия по выполнению необходимых действий процесса и соблюдению сроков их выполнения были нарушены (именно они определяют возможные ущербы)

$$R_{без}(T_{зад}) = 1 - \left\{ \sum_{k=1}^{K} W_k \left[1 - R_{действий\ k}(T_{зад\ k}) \right] Ind_{действий}(\alpha_k) + \sum_{i=1}^{I} M_i \left[1 - R_{св\ i}(T_{зад\ i}) \right] Ind_{св}(\alpha_i) \right\} / \left(\sum_{k=1}^{K} W_k + \sum_{i=1}^{I} M_i \right), \quad (В.9)$$

где $T_{зад}$ — задаваемое общее время для выполнения всех действий, включающее все частные значения $T_{зад\ k}$, $T_{зад\ i}$ с учетом их наложений, — см. формулы (В.2)—(В.9).

Примечание — При соблюдении всех учитываемых условий вероятностные оценки рисков по формулам (В.8), (В.9) совпадают.

Обобщенную вероятность нарушения реализации процесса управления жизненным циклом системы с учетом дополнительных специфических системных требований $R_{обобщ}(T_{зад})$ в течение периода прогноза $T_{зад}$ вычисляют по формуле

$$R_{\text{обобщ}}(T_{\text{зад}}) = 1 - [1 - R_{\text{без}}(T_{\text{зад}})] \cdot [1 - R_{\text{наруш}}(T_{\text{зад}})]. \quad \text{(В.10)}$$

Здесь вероятность нарушения надежности реализации процесса в течение периода прогноза без учета дополнительных специфических системных требований $R_{\text{без}}(T_{\text{зад}})$ рассчитывают по формулам (В.8) и/или (В.9) в зависимости от целей системного анализа. Вероятность нарушения дополнительных специфических системных требований в системе в течение периода прогноза $R_{\text{наруш}}(T_{\text{зад}}) = R_{\text{наруш}}(\sigma, \beta, T_{\text{меж}}, T_{\text{диаг}}, T_{\text{восст}}, T_{\text{зад}})$ рассчитывают по рекомендациям В.3 для выбранной структуры моделируемой системы.

Обобщенный риск нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований определяют путем сопоставления расчетной вероятности нарушения реализации процесса в течение периода прогноза, рассчитанной по формуле (В.10), с возможным ущербом за этот период.

Приложение Г
(справочное)

Рекомендации по определению допустимых значений показателей, характеризующих риски в процессе управления моделью жизненного цикла системы

С точки зрения риска, характеризующего приемлемый уровень целостности рассматриваемой системы, предъявляемые требования системной инженерии подразделяют на требования при допустимых рисках, обосновываемых по прецедентному принципу (см. ГОСТ Р 59330, ГОСТ Р 59339, ГОСТ Р 59991), и требования при рисках, свойственных реальной или гипотетичной системе-эталону. При формировании требований системной инженерии осуществляют обоснование достижимости целей системы, учитывают важность и специфику системы, ограничения на стоимость ее создания и эксплуатации, другие требования и условия, включая требования к специальным показателям, связанным с критичными сущностями рассматриваемой системы.

Требования системной инженерии 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 и безопасности рассматриваемой системы. Вместе с тем проведение работ системной инженерии с ориентацией на риски, свойственные системе-эталону, характеризуется существенно бóльшими затратами по сравнению с требованиями, ориентируемыми на допустимые риски, обосновываемые по прецедентному принципу. Это заведомо удорожает разработку рассматриваемой системы, увеличивает время до принятия ее в эксплуатацию и удорожает саму эксплуатацию системы.

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 иным соображениям) или невозможной ориентация на допустимые риски, свойственные системе-эталону. Вследствие этого минимальной гарантией обеспечения надежности реализации процесса управления моделью жизненного цикла системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

Типовые допустимые значения количественных показателей рисков для процесса управления моделью жизненного цикла системы отражены в таблице Д.1. 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 имеет место гарантия надежности реализации рассматриваемого процесса в течение задаваемого периода прогноза.

Таблица Д.1 — Пример задания допустимых значений рисков

Показатель	Допустимое значение риска (в вероятностном выражении)	
	при ориентации на обоснование по прецедентному принципу	при ориентации на обоснование для системы-эталона
Риск нарушения надежности реализации процесса управления моделью жизненного цикла системы (без учета дополнительных специфических системных требований)	Не выше 0,05	Не выше 0,01
Обобщенный риск нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований	Не выше 0,10	Не выше 0,05

Приложение Д
(справочное)

Примерный перечень методик системного анализа процесса управления моделью жизненного цикла системы

Д.1 Методика прогнозирования риска нарушения надежности реализации процесса управления моделью жизненного цикла системы (без учета дополнительных специфических системных требований).

Д.2 Методика прогнозирования риска нарушения дополнительных специфических системных требований в процессе управления моделью жизненного цикла системы.

Д.3 Методика прогнозирования обобщенного риска нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований.

Д.4 Методики обоснования допустимых рисков для задаваемой модели угроз безопасности (в терминах обобщенного риска нарушения реализации процесса управления моделью жизненного цикла системы с учетом дополнительных специфических системных требований).

Д.5 Методики определения существенных недостатков процесса управления моделью жизненного цикла системы с использованием прогнозирования рисков.

Д.6 Методики обоснования предупреждающих действий, направленных на достижение целей процесса управления моделью жизненного цикла системы и противодействие угрозам.

Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления моделью жизненного цикла системы.

Примечания

1 Системной основой для создания методик служат положения разделов 5—7 настоящего стандарта, модели и методы приложений В и Г.

2 С учетом специфики системы допускается использование других научно обоснованных методов, моделей, методик.

Библиография

[1] Федеральный закон от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера»

[2] Федеральный закон от 21 июля 1997 г. № 116-ФЗ «О промышленной безопасности опасных производственных объектов»

[3] Федеральный закон от 21 июля 1997 г. № 117-ФЗ «О безопасности гидротехнических сооружений»

[4] Федеральный закон от 24 июля 1998 г. № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»

[5] Федеральный закон от 2 января 2000 г. № 29-ФЗ «О качестве и безопасности пищевых продуктов»

[6] Федеральный закон от 10 января 2002 г. № 7-ФЗ «Об охране окружающей среды»

[7] Федеральный закон от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании»

[8] Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

[9] Федеральный закон от 9 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»

[10] Федеральный закон от 22 июля 2008 г. № 123-ФЗ «Технический регламент о требованиях пожарной безопасности»

[11] Федеральный закон от 30 декабря 2009 г. № 384-ФЗ «Технический регламент о безопасности зданий и сооружений»

[12] Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности»

[13] Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»

[14] Федеральный закон от 28 декабря 2013 г. № 426-ФЗ «О специальной оценке условий труда»

[15] Федеральный закон от 28 июня 2014 г. № 172-ФЗ «О стратегическом планировании в Российской Федерации»

[16] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[17] Указ Президента Российской Федерации от 12 апреля 2021 г. № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности»

[18] Требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды (утверждены приказом ФСТЭК России от 14 марта 2014 г. № 31)

[19] Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации (утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239)

[20] Методические рекомендации по проведению плановых проверок субъектов электроэнергетики, осуществляющих деятельность по производству электрической энергии на тепловых электрических станциях, с использованием риск-ориентированного подхода (утверждены приказом Ростехнадзора от 5 марта 2020 г. № 97)

[21] Методические рекомендации по проведению плановых проверок деятельности теплоснабжающих организаций, теплосетевых организаций, эксплуатирующих на праве собственности или на ином законном основании объекты теплоснабжения, при осуществлении федерального государственного энергетического надзора с использованием риск-ориентированного подхода (утверждены приказом Ростехнадзора от 20 июля 2020 г. № 278)

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

Ключевые слова: безопасность, качество, модель жизненного цикла системы, риск, система, стадия, системная инженерия, системный анализ, управление

Редактор *З.А. Лиманская*
Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 18.08.2022. Подписано в печать 26.08.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 3,72. Уч.-изд. л. 2,98.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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