ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59993— 2022

Системная инженерия

СИСТЕМНЫЙ АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ ИНФРАСТРУКТУРОЙ СИСТЕМЫ

Издание официальное

Москва
Российский институт стандартизации
2022

gost.e-ecolog.ru

Предисловие

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

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 17 августа 2022 г. № 773-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 (*gost.e-ecolog.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

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 4
4 Основные положения системной инженерии по системному анализу процесса управления инфраструктурой системы 7
5 Общие требования системной инженерии к системному анализу процесса управления инфраструктурой системы 10
6 Специальные требования к количественным показателям 11
7 Требования к методам системного анализа процесса управления инфраструктурой системы 13
Приложение А (справочное) Пример перечня решаемых задач системного анализа 17
Приложение Б (справочное) Пример перечня угроз нарушения нормальной реализации процесса управления инфраструктурой системы 18
Приложение В (справочное) Типовые модели и методы прогнозирования рисков 19
Приложение Г (справочное) Рекомендации по определению допустимых значений показателей, характеризующих риски в процессе управления инфраструктурой системы 27
Приложение Д (справочное) Примерный перечень методик системного анализа для процесса управления инфраструктурой системы 28
Библиография 29

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 инфраструктурой 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 инфраструктурой 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 инфраструктуры системы, частных и обобщенного показателей прогнозируемых рисков.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Системная инженерия

СИСТЕМНЫЙ АНАЛИЗ ПРОЦЕССА УПРАВЛЕНИЯ ИНФРАСТРКТУРОЙ СИСТЕМЫ

System engineering. System analysis of system infrastructure management process

Дата введения — 2022—11—30

1 Область применения

Настоящий стандарт устанавливает основные положения системного анализа процесса управления инфраструктурой для систем различных областей применения.

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

Требования стандарта предназначены для использования организациями, участвующими в создании (модернизации, развитии), эксплуатации систем, выведении их из эксплуатации и реализующими процесс управления инфраструктурой системы — см. примеры систем в [1]—[22].

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

ГОСТ 34.201 Информационная технология. 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 32867 Дороги автомобильные общего пользования. Организация строительства. Общие требования

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 10.0.05/ИСО 12006-2:2015 Система стандартов информационного моделирования зданий и сооружений. Строительство зданий. Структура информации об объектах строительства. Часть 2. Основные принципы классификации

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 27.102 Надежность в технике. Надежность объекта. Термины и определения

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

ГОСТ Р ИСО 9001 Системы менеджмента качества. Требования

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 Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности

ГОСТ Р ИСО/МЭК 27003 Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации

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

ГОСТ Р ИСО/МЭК 27036-2 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования

ГОСТ Р ИСО/МЭК 27036-4 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 4. Рекомендации по обеспечению безопасности облачных услуг

ГОСТ Р ИСО 31000 Менеджмент риска. Принципы и руководство

ГОСТ Р 34059 Инженерные сети зданий и сооружений внутренние. Устройство систем отопления, горячего и холодного водоснабжения. Общие технические требования

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/(ISO Guide 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 51904 Программное обеспечение встроенных систем. Общие требования к разработке и документированию

ГОСТ Р 53114 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения

ГОСТ Р 53622 Информационные технологии. Информационно-вычислительные системы. Стадии и этапы жизненного цикла, виды и комплектность документов

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 56425 Технопарки. Требования

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 58811 Центры обработки данных. Инженерная инфраструктура. Стадии создания

ГОСТ Р 58812 Центры обработки данных. Инженерная инфраструктура. Операционная модель эксплуатации. Спецификация

ГОСТ Р 59215 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий

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

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

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

ГОСТ Р 59345 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 Системная инженерия. Защита информации в процессе определения архитектуры системы

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

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

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

ГОСТ Р 59991 Системная инженерия. Системный анализ процесса управления рисками для 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 62264-1 Интеграция систем управления предприятием. Часть 1. Модели и терминология

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 27.102, ГОСТ Р ИСО 9000, ГОСТ Р ИСО/МЭК 27001, ГОСТ Р ИСО 31000, ГОСТ Р 32867, ГОСТ Р 34059, ГОСТ Р 51897, ГОСТ Р 58811, ГОСТ Р 58812, ГОСТ Р 59339, ГОСТ Р 59349, ГОСТ Р МЭК 61508-4, ГОСТ Р МЭК 62264-1, 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, статья 3.7]

3.1.2

инновационная инфраструктура: Совокупность организаций, образующих инфраструктуру поддержки субъектов малого и среднего предпринимательства в научно-технологической сфере, в том числе бизнес-инкубаторы, региональные центры инжиниринга, центры сертификации, стандартизации и испытаний и иные организации, обеспечивающие коммерциализацию результатов научно-технических исследований и разработок.

[ГОСТ Р 56425—2015, статья 3.9]

3.1.3 **обобщенный риск нарушения реализации процесса управления инфраструктурой системы с учетом дополнительных специфических системных требований:** Сочетание вероятности того, что будут нарушены надежность реализации процесса управления инфраструктурой 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 59331.

3.1.4 **инфраструктура системы:** Комплекс взаимосвязанных объектов, структур и элементов, составляющих и обеспечивающих основу создания и/или эксплуатации системы согласно ее целевому назначению и/или выведению системы из эксплуатации.

Примечание — В общем случае инфраструктуру современной системы образуют здания, сооружения, оборудование, программно-аппаратная среда и службы обеспечения, необходимые для создания (модернизации, развития) и/или эксплуатации системы и/или выведению системы из эксплуатации. Например, инфраструктура системы, представляющей собой научно-производственную организацию, может включать в себя технопарк, состоящий из технологической инфраструктуры (зданий, сооружений, строительного комплекса), инженерной инфраструктуры (сооружения связи, в том числе линейно-кабельные сооружения), коммунальной инфраструктуры (системы горячего и холодного водоснабжения, отопления, теплоснабжения, теплопотребления, теплового пункта, канализации), центра обработки данных, телекоммуникационных сетей, систем хранения и передачи данных, системы поддержки принятия решений, инновационной инфраструктуры для научно-технических исследований и разработок, транспортной инфраструктуры, системы обеспечения безопасности.

3.1.5

коммунальная инфраструктура: Система коммуникаций и объектов водоснабжения, водоотведения, теплоснабжения, электроэнергетики, электроснабжения и газоснабжения, связи, обеспечивающая функционирование технопарка.

[ГОСТ Р 56425—2015, статья 3.5]

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

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

3.1.7 **надежность реализации процесса управления инфраструктурой системы:** Свойство процесса управления инфраструктурой системы сохранять во времени в установленных пределах значения показателей процесса, характеризующих способность выполнить процесс в заданных условиях его реализации.

3.1.8

риск: Сочетание вероятности нанесения ущерба и тяжести этого ущерба.

[ГОСТ Р 51898—2002, статья 3.2]

3.1.9

система: 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 зачастую уточняется с помощью ассоциативного существительного, например система самолета. В некоторых случаях слово система может заменяться контекстно зависимым синонимом, например самолет, хотя это может впоследствии затруднить восприятие системных принципов.

[ГОСТ Р 57193—2016, статья 4.1.44]

3.1.10 **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.

3.1.11

системная инженерия: 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, статья 4.1.47]

3.1.12 **системный анализ процесса управления инфраструктурой системы:** Научный метод системного познания путем представления рассматриваемых системы и/или процесса управления инфраструктурой системы в виде приемлемой моделируемой системы, предназначенный для решения практических задач системной инженерии и включающий в себя:

- измерение и оценку специальных показателей, связанных с критичными сущностями инфраструктуры 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 инфраструктуру рассматриваемой системы;
- обоснование с использованием моделирования упреждающих мер противодействия угрозам инфраструктуре системы, 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.

Примечание — 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 инфраструктуре обеспечивающих систем, охватываемым по требованиям заказчика.

3.1.13

строительный комплекс: Совокупность одного или более строительных сооружений, предназначенных для обеспечения выполнения как минимум одной функции или деятельности пользователя.

Примечание — Строительный комплекс можно разделить на составляющие элементы и идентифицировать строительные сооружения, которые его образуют; например, аэропорт обычно состоит из таких строительных сооружений, как взлетно-посадочная полоса, диспетчерская башня, здание терминала, ангара для самолетов и др. Бизнес-парк обычно состоит из некоторого количества зданий, подъездных дорог и объектов ландшафтной архитектуры (каждый из которых представляет собой отдельное строительное сооружение). Автомагистраль, ведущая из точки А в точку В, состоит из сервисных станций, дорожного покрытия, мостов, насыпей, объектов ландшафтной архитектуры и др.

[ГОСТ Р 10.0.05—2019, статья 3.4.1]

3.1.14

технологическая инфраструктура: Комплекс специализированного оборудования, предназначенного для оснащения лабораторий, виварием, инновационно-технологических центров, центров промышленного дизайна, центров прототипирования, центров трансфера технологий и иных объектов, необходимых резидентам для ведения хозяйственной деятельности на территории технопарка.

[ГОСТ Р 56425—2015, статья 3.10]

3.1.15

технопарк: Управляемый управляющей компанией комплекс объектов коммунальной, транспортной и технологической инфраструктуры, обеспечивающий полный цикл услуг по размещению и развитию инновационных компаний, являющихся резидентами технопарка.

[ГОСТ Р 56425—2015, статья 3.1]

3.1.16

транспортная инфраструктура: Совокупность объектов недвижимого имущества технопарка, предназначенная для обеспечения движения транспортных средств резидентов технопарка, в том числе автомобильных дорог, железнодорожных путей, портов, тоннелей, эстакад, мостов, переездов, путепроводов.

[ГОСТ Р 56425—2015, статья 3.7]

3.1.17

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

3.2 В настоящем стандарте использовано следующее сокращение:

ТЗ — техническое задание.

4 Основные положения системной инженерии по системному анализу процесса управления инфраструктурой системы

4.1 Общие положения

4.1.1 Организации используют процесс управления инфраструктурой системы для того, чтобы преобразовать представление заинтересованных сторон о желательных возможностях системы в технические решения, соответствующие эксплуатационным потребностям пользователей. Для прогнозирования рисков, связанных с реализацией процесса управления инфраструктурой 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 инфраструктурой 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 инфраструктуре системы. В общем случае проведение системного анализа связано с решением задач эффективного функционирования, 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, обеспечения информационной безопасности;

- безопасности и защищенности 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 характеристик создаваемых объектов и конструкций;

- безопасности железнодорожного, авиационного и водного транспорта;

- 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 систем.

Решение задач системной инженерии с использованием системного анализа процесса управления инфраструктурой 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, ориентированных на 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 инфраструктурой 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 инфраструктурой системы сосредоточивают на:

- определении выходных результатов и действий, предназначенных для достижения целей процесса;

- определении потенциальных угроз и определении возможных сценариев возникновения и развития угроз для рассматриваемых инфраструктуры и процесса управления инфраструктурой системы;

- измерениях и оценках специальных показателей, связанных с критичными сущностями инфраструктуры 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 инфраструктурой системы, подлежащий системному анализу, может быть использован на любой стадии жизненного цикла системы. Стадии и этапы работ устанавливают в договорах, соглашениях и 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 53622, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58811.

Процесс управления инфраструктурой системы может входить в состав работ, выполняемых в рамках других процессов жизненного цикла системы, и при необходимости включать в себя другие процессы.

4.3 Цели системного анализа

4.3.1 Цели системного анализа процесса управления инфраструктурой системы формулируют исходя из назначения системы, решаемых задач системной инженерии и целей самого процесса. Определение целей процесса управления инфраструктурой системы осуществляют по ГОСТ Р 10.0.05, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 53114, ГОСТ Р 53647.1, ГОСТ Р 56425, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 58811, ГОСТ Р 59331, ГОСТ Р МЭК 61508-1, ГОСТ Р МЭК 62264-1 с учетом специфики системы.

В общем случае главной целью процесса управления инфраструктурой системы является поддержка таких проектных и эксплуатационных решений и действий, выполнение которых формирует функциональные возможности для создания (модернизации, развития) и/или эксплуатации системы и/или выведения системы из эксплуатации. Процесс управления инфраструктурой системы определяет, обеспечивает и поддерживает активы основных средств, инструментарии, связи и информационные технологии, необходимые для бизнеса организации.

4.3.2 В системном анализе объектами исследований являются критичные сущности инфраструктуры рассматриваемой системы, непосредственно рассматриваемый процесс управления инфраструктурой 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 системные процессы и инфраструктуру 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 системы, а также ее выведении из эксплуатации.

4.3.3 В общем случае основными целями системного анализа процесса управления инфраструктурой системы являются:

- оценка специальных показателей, связанных с критичными сущностями инфраструктуры 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 инфраструктуры рассматриваемой системы (и/или ее элементов);
- определение и обоснование с использованием моделирования в жизненном цикле системы упреждающих мер противодействия угрозам и условиям, 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 инфраструктурой системы.

5 Общие требования системной инженерии к системному анализу процесса управления инфраструктурой системы

5.1 Общие требования системной инженерии к системному анализу процесса управления инфраструктурой 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 инфраструктурой системы должны обеспечивать:

- решение основных задач системного анализа, главными из которых являются:
  - задачи оценки специальных показателей, связанных с критичными сущностями инфраструктуры рассматриваемой системы;
  - задачи прогнозирования рисков, свойственных процессу управления инфраструктурой системы;
  - задачи обоснования допустимых значений специальных показателей, связанных с критичными сущностями инфраструктуры рассматриваемой системы, и допустимых рисков;
  - задачи определения существенных угроз и условий для инфраструктуры рассматриваемой системы и процесса управления инфраструктурой системы с использованием специальных показателей и прогнозируемых рисков;
  - комплекс задач поддержки принятия решений по обеспечению качества, безопасности и/или эффективности рассматриваемой системы в ее жизненном цикле;
- решение вспомогательных задач совершенствования непосредственно самого системного анализа процесса управления инфраструктурой 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 инфраструктурой 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 Р ИСО/МЭК 27036-2, ГОСТ Р ИСО/МЭК 27036-4, ГОСТ Р 59331, ГОСТ Р 59337, ГОСТ Р 59339, ГОСТ Р 59346, ГОСТ Р 59355, [1]—[22]).

Поскольку элементы процесса управления инфраструктурой 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 инфраструктурой системы призваны обеспечивать управление техническими и организационными усилиями по планированию и реализации этого процесса.

5.5 Область применения системного анализа процесса управления инфраструктурой системы должна охватывать:

- специальные критичные сущности, контролируемые организацией применительно к инфраструктуре 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 инфраструктурой системы (например требований по защите информации, — см. ГОСТ Р 59331);

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

Пример перечня возможных угроз нарушения нормальной реализации процесса управления инфраструктурой системы приведен в приложении Б.

5.6 Системный анализ процесса управления инфраструктурой системы осуществляют с использованием количественных показателей, моделей и методов (см. приложение В) с учетом специфики системы и рекомендаций ГОСТ Р ИСО 9001, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО/МЭК 15026, ГОСТ Р ИСО/МЭК 15026-4, ГОСТ Р ИСО/МЭК 16085, ГОСТ Р ИСО 17359, ГОСТ Р ИСО/МЭК 27002, ГОСТ Р 51901.1, ГОСТ Р 51901.5, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 54145, ГОСТ Р 58771, ГОСТ Р 59331, ГОСТ Р 59339, 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, ГОСТ Р МЭК 62264-1, ГОСТ Р МЭК 62508.

6 Специальные требования к количественным показателям

6.1 Общие положения

6.1.1 Для обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах используют устанавливаемые качественные и количественные показатели рисков. 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 инфраструктурой системы должны учитывать:

- критичные сущности системы (и/или ее элементов), связанные с ее инфраструктурой, включая критичные сущности, связанные с достижением целей системной инженерии;
- требования заинтересованных сторон, имеющих интерес к рассматриваемой системе, выходные результаты и выполняемые действия процесса управления инфраструктурой системы;
- потенциальные угрозы инфраструктуре системы (включая угрозы для выходных результатов и выполняемых действий процесса управления инфраструктурой 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 инфраструктурой 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 инфраструктурой системы, подлежащие учету при решении задач системного анализа, определяют по ГОСТ 2.102, ГОСТ 2.114, ГОСТ 15.016, ГОСТ 34.201, ГОСТ 34.602, ГОСТ 32867, ГОСТ IEC 61508-3, ГОСТ Р 10.0.05, ГОСТ Р 15.101, ГОСТ Р ИСО 9001, ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО 15704, ГОСТ Р 34059, ГОСТ Р 51583, ГОСТ Р 51904, ГОСТ Р 53114, ГОСТ Р 53647.1, ГОСТ Р 56425, ГОСТ Р 56939, ГОСТ Р 57102, ГОСТ Р 57193, ГОСТ Р 57839, ГОСТ Р 58494, ГОСТ Р 58811, ГОСТ Р 59215, ГОСТ Р 59331, ГОСТ Р 59339, ГОСТ Р МЭК 62264-1. При этом учитывают специфику рассматриваемой системы (см., например [1]—[22]).

6.1.4 Основными выходными результатами процесса управления инфраструктурой системы являются:

- описание системы и применяемой инфраструктуры, включая взаимодействия системы и инфраструктурных подсистем (в том числе обеспечивающих), их функции и границы;
- системные требования и проектные ограничения, включая функциональные, эксплуатационные, процессные требования и требования по взаимодействию системы и инфраструктурных подсистем (в том числе обеспечивающих);

- материалы эскизного и/или технического проектирования системы;
- отчеты по анализу системных требований;
- требования к применяемой инфраструктуре системы и обеспечивающим системам или системным элементам, необходимым для выполнения действий процесса;
- элементы инфраструктуры системы, соответствующие требованиям, предъявляемым к системе;
- описание комплексов программных, программно-аппаратных и технических средств, определяющих инфраструктуру системы и ее применение;
- акты, протоколы, предписания с результатами контроля состояния инфраструктуры системы;
- график технического обслуживания (сопровождения) инфраструктуры системы;
- план мероприятий по охране труда (в части, качающейся инфраструктуры системы);
- инструкции по монтажу, пуску и регулированию элементов инфраструктуры системы;
- паспорт на инфраструктуру системы в целом и на отдельные инфраструктурные элементы (при необходимости);
- ведомость комплекта запасных частей, инструментов и принадлежностей;
- эксплуатационные и специальные инструкции;
- технические условия и требования на ремонт элементов инфраструктуры системы.

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

- определение проектных требований к инфраструктуре системы;
- выработку стратегии по созданию (модернизации) и развитию инфраструктуры системы;
- разработку ТЗ на создание (модернизацию) или развитие инфраструктуры системы;
- разработку рабочей документации на инфраструктуру системы;
- определение элементов инфраструктуры системы, включая инструментарии, программные средства, программно-аппаратные и технические средства;
- отбор элементов инфраструктуры системы, удовлетворяющих требованиям конкретного проекта;
- анализ соответствия отобранных элементов инфраструктуры системы требованиям конкретного проекта;
- приобретение необходимых элементов инфраструктуры системы;
- проведение сертификационных и аттестационных испытаний элементов инфраструктуры системы (при необходимости);
- техническое обслуживание (сопровождение) и необходимую поддержку инфраструктуры системы, включая:
  - выполнение работ для поддержания инфраструктуры системы в работоспособном состоянии,
  - оценку степени, до которой элементы инфраструктуры системы и поставленные инфраструктурные ресурсы удовлетворяют требованиям проекта,
  - определение и обеспечение улучшений или изменений по инфраструктурным ресурсам, включая при необходимости изменения требований проекта;
- оценку рисков нарушения надежности реализации процесса управления инфраструктурой системы;
- оценку эффективности функционирования системы с использованием процесса управления инфраструктурой системы.

6.2 Требования к составу показателей

Используемые показатели должны обеспечивать решение основных и вспомогательных задач системного анализа процесса управления инфраструктурой 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 инфраструктурой системы.

6.3 Требования к количественным показателям

6.3.1 Для решения задач системного анализа используют:

- специальные показатели, связанные с критичными сущностями инфраструктуры рассматриваемой системы (например, физические показатели функционирования инфраструктурного оборудования, оцениваемые с использованием измерения);
- прогнозируемый риск нарушения надежности реализации процесса управления инфраструктурой системы;
- прогнозируемый обобщенный риск нарушения реализации процесса управления инфраструктурой 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 исходных данных

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

- источники, позволяющие сформировать данные, обеспечивающие оценку специальных показателей, связанных с критичными сущностями инфраструктуры рассматриваемой системы;
- временны́е данные применения технологий противодействия угрозам и/или функционирования вспомогательных систем управления инфраструктурой, планируемых к использованию или используемых в рамках инфраструктуры рассматриваемой системы (в том числе данные о срабатывании исполнительных механизмов этих систем);
- текущие и статистические данные о состоянии параметров контролируемых критичных сущностей инфраструктуры 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 инфраструктуре системы (привязанные к временам и условиям наступления событий, характеризующих соответствующие нарушения и предпосылки к нарушениям);
- текущие и статистические данные результатов технического диагностирования инфраструктуры рассматриваемой системы и вспомогательных систем управления инфраструктурой системы;
- 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 их инфраструктуры;
- 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 инфраструктуры системы.

Типовые исходные данные для моделирования приведены в приложении В.

7 Требования к методам системного анализа процесса управления инфраструктурой 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 инфраструктурой системы.

7.1.2 Требования к формализованным методам системного анализа процесса управления инфраструктурой 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 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 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 59331, 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 инфраструктуры 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 (см. 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 инфраструктурой 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 инфраструктуру системы (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 инфраструктурой системы.

7.4 Требования к методам обоснования допустимых рисков

7.4.1 При выполнении процесса управления инфраструктурой рассматриваемой системы допустимые риски выступают в качестве количественных норм эффективности мер противодействия угрозам. Значения допустимых рисков определяют применительно к риску нарушения надежности реализации процесса 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, которую выбирают в качестве аналога для моделируемой системы. Общее описание методов обоснования допустимых рисков, применимых для процесса управления инфраструктурой 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 инфраструктурой системы и 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 инфраструктуры рассматриваемой системы, а также с использованием прогнозирования рисков. Общий алгоритм определения существенных угроз и условий, применимый для процесса управления инфраструктурой системы, приведен в ГОСТ Р 59991 (см. также ГОСТ Р 59331, 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, обоснования эффективных предупреждающих мер по снижению рисков или их удержанию в допустимых пределах, определения существенных угроз и условий применительно к процессу управления инфраструктурой системы. Применение методов должно быть ориентировано на:

- обеспечение надежности реализации процесса управления инфраструктурой 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 инфраструктуры системы);
- обоснование предложений по повышению качества, безопасности и/или эффективности системы и совершенствование системного анализа и методов решения задач системного анализа процесса управления инфраструктурой 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 инфраструктурой системы основана на оценках специальных показателей, связанных с критичными сущностями инфраструктуры 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 инфраструктурой системы (см. 7.4, 7.5).

7.6.3 Поддержка принятия решений по обоснованию мер, направленных на достижение целей процесса управления инфраструктурой 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 инфраструктурой системы в случае определения предпосылок к нарушению или непосредственно следов произошедших нарушений из-за реализации угроз. Определение мер по обеспечению надежности реализации процесса управления инфраструктурой 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 инфраструктурой 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 в части инфраструктуры системы при среднесрочном планировании 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 инфраструктурой 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 инфраструктуры 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 процесса управления инфраструктурой системы 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 инфраструктурой 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 инфраструктурой 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 инфраструктуры рассматриваемой системы, для предотвращения ущерба и уменьшения размеров возможных негативных последствий. К таким задачам относят:

- задачи обработки и контроля данных о состоянии инфраструктуры системы;
- построение деревьев отказов в инфраструктуре системы, ведущих к возникновению аварии, и деревьев событий, связанных с развитием аварий (например, с разливами вредных веществ и жидкостей, испарениями, воспламенениями, взрывами, интоксикацией, поражениями, загрязнениями окружающей среды);
- задачи оценки возможных прямых и косвенных экономических, экологических и социальных ущербов из-за нарушения реализации процесса управления инфраструктурой системы.

А.1.2 Задачи обоснования допустимых значений специальных показателей, связанных с критичными сущностями инфраструктуры рассматриваемой системы, и допустимых рисков. Например, для моделируемой системы, представляющей собой промышленный и топливно-энергетический комплекс региона, задают допустимые значения специальных показателей и допустимых рисков для таких формализованных сущностей, как имеющиеся атомные реакторы и объекты ядерного цикла, объекты гражданского и промышленного строительства, электросети, гидро- и теплоэнергетические комплексы, металлургические и транспортные комплексы, магистральные газо- и нефтепродуктоводы, уникальные инженерные сооружения, системы связи и управления.

А.1.3 Задачи определения существенных угроз и условий для инфраструктуры 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 информационную, коммунальную, технологическую, транспортную инфраструктуру, технопарки;
- задачи анализа рисков для инфраструктуры сложных конструкций, включая декомпозицию конструкции на составляющие элементы, детализацию и обобщение информации с учетом ее неполноты и недостоверности, выбор критериев риска, диагностику и моделирование применения конструкции во времени с учетом случайных факторов в среде эксплуатации (в нагрузках, механических воздействиях, прочности и дефектности материалов, напряженности, деформируемости и трещиностойкости как для отдельных элементов, так и для конструкции в целом), а также интерпретацию получаемых результатов диагностики и моделирования;
- задачи системной инженерии при проектировании, испытаниях и эксплуатации системы по показателям «эффективность — стоимость» (в части, связанной с инфраструктурой системы).

А.1.4 Комплекс задач поддержки принятия решений в системной инженерии (в части инфраструктуры рассматриваемой системы), связанных с обеспечением качества, безопасности и эффективности в жизненном цикле системы. К таким задачам относят задачи обоснования требований к приемлемым условиям и мерам противодействия угрозам инфраструктуре 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 года 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 инфраструктурой системы, а также при иных корректных ограничениях;
- комбинации перечисленных выше или иных оптимизационных задач применительно к инфраструктуре системы или ее отдельным элементам.

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

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

Приложение Б
(справочное)

Пример перечня угроз нарушения нормальной реализации процесса управления инфраструктурой системы

Перечень угроз нарушения нормальной реализации процесса управления инфраструктурой 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 коммунальной, технологической, транспортной инфраструктуре, инфраструктуре технопарков — по ГОСТ Р 56425;
- 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 критической информационной инфраструктуры, 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 59331, ГОСТ Р 59339, ГОСТ Р 59341;
- 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, инфраструктура систем которого была скомпрометирована;
- прочие соответствующие угрозы качеству, безопасности и эффективности системы, связанные с процессом управления инфраструктурой системы.

Приложение В
(справочное)

Типовые модели и методы прогнозирования рисков

В.1 Основные положения

В.1.1 Для прогнозирования рисков в процессе управления инфраструктурой системы применяют любые возможные методы, обеспечивающие приемлемое достижение поставленных целей. С учетом набираемой статистики приводимые типовые модели и методы обеспечивают согласно 6.3:

- прогнозирование риска нарушения надежности реализации процесса управления инфраструктурой системы — см. В.1.2—В.1.9, В.2;

- прогнозирование обобщенного риска нарушения реализации процесса управления инфраструктурой системы с учетом дополнительных специфических системных требований — см. В.3;

В.1.2 Для расчета типовых показателей рисков исследуемые сущности рассматривают в виде моделируемой системы простой или сложной структуры. Под моделируемой системой понимают систему, для которой решение задач системного анализа осуществляется с использованием формализованной модели системы, включающей при необходимости формализованные модели учитываемых сущностей в условиях их применения. Модели и методы прогнозирования рисков в таких системах используют данные, получаемые по факту наступления событий, по выявленным предпосылкам к наступлению событий, и данные собираемой и накапливаемой статистики по системным процессам и возможным условиям их реализации, а также возможные гипотетичные данные.

Моделируемая система простой структуры представляет собой систему из единственного элемента или множества элементов, логически объединенных для анализа как один элемент. Анализ системы простой структуры осуществляют по принципу «черного ящика», когда известны входы и выходы, но неизвестны внутренние детали функционирования системы. Моделируемая система сложной структуры представляется как совокупность взаимодействующих элементов, каждый из которых рассматривается как «черный ящик», функционирующий в условиях неопределенности.

В.1.3 При анализе «черного ящика» для вероятностного прогнозирования рисков осуществляют формальное определение пространства элементарных состояний. Это пространство элементарных состояний формируют в результате статистического анализа произошедших событий с их привязкой к временной оси. Предполагается повторяемость событий. Чтобы провести системный анализ для ответа на условный вопрос «Что будет, если…», при формировании сценариев возможных нарушений статистика реальных событий по желанию исследователя процессов может быть дополнена гипотетичными событиями, характеризующими ожидаемые и/или прогнозируемые условия функционирования системы. Применительно к анализируемому сценарию осуществляют расчет вероятности пребывания элементов моделируемой системы в определенном элементарном состоянии в течение задаваемого периода прогноза. Для негативных последствий при оценке рисков этой расчетной вероятности сопоставляют возможный ущерб.

В.1.4 Для математической формализации используют следующие основные положения:

- к началу периода прогноза предполагается, что целостность моделируемой системы обеспечена, включая изначальное выполнение требований к нормальной реализации системных процессов;

- в условиях неопределенностей возникновение и разрастание различных угроз описывают в терминах случайных событий;

- для различных вариантов развития угроз средства, технологии и меры противодействия угрозам с формальной точки зрения представляют собой совокупность мер и/или защитных преград, предназначенных для воспрепятствования реализации угроз.

Обоснованное использование выбранных мер и защитных преград является предупреждающими контрмерами, нацеленными на обеспечение нормальной реализации процесса управления инфраструктурой системы.

В.1.5 Ниже — в В.2.2, В.2.3 — приведены математические модели для прогнозирования рисков в системе, представляемой в виде «черного ящика». Модель В.2.2 для прогнозирования рисков при отсутствии какого-либо контроля (диагностики) целостности системы является частным случаем модели В.2.3 при реализации технологии периодического системного контроля. Модель В.2.2 применима на практике лишь для оценки и сравнения случая полностью бесконтрольного функционирования моделируемой системы, например там, где контроль невозможен или нецелесообразен по функциональным, экономическим или временны́м соображениям, или когда ответственные лица пренебрегают функциями контроля или не реагируют должным образом на результаты системного анализа.

В.1.6 Для моделируемой системы сложной структуры применимы методы, изложенные в В.2.4, включая методы комбинации и повышения адекватности моделей.

В.1.7 При проведении оценок расчетных показателей на заданный период прогноза предполагают усредненное повторение количественных исходных данных, свойственных прошедшему аналогичному периоду для моделируемой системы. Для исследования запроектных сценариев при моделировании могут быть использованы гипотетичные исходные данные.

В.1.8 Изложение моделей в В.2 дано в контексте нарушения надежности реализации процесса без учета дополнительных специфических системных требований (например, требований по защите информации), в В.3 приведены способы прогнозирования риска нарушения дополнительных специфических системных требований в процессе управления инфраструктурой системы (в том числе с использованием моделей В.2). Методы прогнозирования риска нарушения реализации процесса управления инфраструктурой системы с учетом дополнительных специфических системных требований представлены в В.4. Этот риск характеризуют сочетанием риска нарушения надежности реализации процесса управления инфраструктурой системы (без учета дополнительных специфических системных требований) и риска нарушения риска дополнительных специфических системных требований в этом процессе.

В.1.9 Другие возможные подходы к оценке рисков описаны в ГОСТ IEC 61508-3, ГОСТ Р ИСО 13379-1, ГОСТ Р ИСО 13381-1, ГОСТ Р ИСО 17359, ГОСТ Р 51901.1, ГОСТ Р 51901.7, ГОСТ Р 51901.16, ГОСТ Р 54124, ГОСТ Р 58494, ГОСТ Р 58771, ГОСТ Р 59339, 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.1 Математические модели для прогнозирования риска нарушения надежности реализации процесса управления инфраструктурой системы

В.2.1 Общие положения

В.2.1.1 В моделях для анализа надежности реализации процесса под системой понимают отдельное действие или множество действий процесса, получаемый выходной результат или множество выходных результатов (или иные критичные сущности инфраструктуры системы, подлежащие учету в моделируемой системе).

Примечание — Выполнение дополнительных специфических системных требований в В.2 не рассматривается (учет этих требований см. в В.3 и В.4).

В.2.1.2 Для каждого элемента моделируемой системы возможны отсутствие какого-либо контроля либо периодический системный контроль (диагностика) его целостности с необходимым восстановлением по результатам контроля.

В.2.1.3 В терминах системы, состоящей из элементов, отождествляемых с выполняемыми действиями или получаемыми выходными результатами (или иными рассматриваемыми сущностями), под целостностью моделируемой системы понимают такое состояние элементов системы, которое в течение задаваемого периода прогноза отвечает требованию обеспечения надежной реализации процесса управления инфраструктурой системы. С точки зрения вероятностного прогнозирования риска нарушения надежности реализации процесса управления инфраструктурой системы пространство элементарных состояний отдельного элемента моделируемой системы на временной оси образуют следующие состояния:

- «Целостность элемента моделируемой системы сохранена», если в течение всего периода прогноза обеспечена надежная реализация анализируемого действия или получение определенного выходного результата процесса или обеспечено нормальное состояние иной критичной сущности инфраструктуры системы (подлежащее учету и анализу в моделируемой системе как отдельный элемент);
- «Целостность элемента моделируемой системы нарушена» — в противном случае.

В результате моделирования получают расчетные значения вероятностных показателей нахождения элементов моделируемой системы в определенном элементарном состоянии. В сопоставлении с возможным ущербом вероятность нахождения в состоянии «Целостность элемента моделируемой системы нарушена» характеризует риск нарушения надежности выполнения соответствующего действия или получения соответствующего выходного результата реализуемого процесса или функционирования критичной сущности инфраструктуры системы.

В.2.2 Математическая модель «черного ящика» при отсутствии какого-либо контроля

Моделируемая система представлена в виде «черного ящика», функционирование которого не контролируется. Восстановление возможностей по обеспечению выполнения действий процесса осуществляется лишь после обнаружения наступившего нарушения. В результате возникновения угроз и их развития может произойти нарушение надежности реализации процесса. С формальной точки зрения модель позволяет оценить вероятностное значение риска нарушения надежности реализации процесса в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетная вероятность нарушения надежности реализации процесса управления инфраструктурой системы в течение заданного периода прогноза при отсутствии какого-либо контроля.

Модель представляет собой частный случай модели В.2.3, если период между диагностиками состояния моделируемой системы больше периода прогноза. Учитывая это, используют формулы (В.1)—(В.3).

В.2.3 Математическая модель «черного ящика» при реализации технологии периодического системного контроля

В моделируемой системе, представленной в виде «черного ящика», осуществляется периодический контроль состояния системы с точки зрения надежности реализации процесса управления инфраструктурой.

Из-за случайного характера угроз, различных организационных, программно-технических и технологических причин, различного уровня квалификации специалистов, привлекаемых для контроля, неэффективных мер поддержания или восстановления приемлемых условий, а также в силу иных причин надежность реализации процесса управления инфраструктурой системы может быть нарушена. Такое нарушение способно повлечь за собой негативные последствия.

В рамках модели развитие событий в моделируемой системе считается не нарушающим надежность реализации процесса управления инфраструктурой в течение заданного периода прогноза (см. также В.2.4), если в течение всего периода прогноза источники угроз отсутствуют либо за время между соседними диагностиками возникшие источники угроз не успевают активизироваться. При этом в модели предполагается, что при очередном контроле (диагностике) происходит своевременное определение каждого источника угроз и принятие адекватных защитных мер и действий против активизации выявленных угроз.

Примечание — С точки зрения надежности реализации процесса управления инфраструктурой системы примером источников угроз могут служить природные и техногенные угрозы для конкретного инфраструктурного оборудования, когда значения отслеживаемого параметра функционирования оборудования (например, температуры, давления) выходят за установленные для него допустимые пределы рабочего или нормативного диапазона значений. Активизация такого источника угроз на практике начинается с момента нарушения допустимого диапазона и завершается реальным отказом или сбоем в работе оборудования, способным привести к ущербу, см., например ГОСТ Р 58494, ГОСТ Р 59331.

В целях моделирования предполагают, что существуют не только средства контроля (диагностики) состояния моделируемой системы (позволяющие выявить источники угроз и следы их активизации), но и способы поддержания и/или восстановления нарушаемых возможностей системы. Восстановление осуществляется лишь в период системного контроля (диагностики) или сразу после него при определении источников угроз или следов их активизации. Соответственно, чем чаще осуществляют системный контроль с должной реакцией на выявляемые нарушения или предпосылки к нарушениям, тем выше гарантии обеспечения надежности реализации рассматриваемого процесса в период прогноза (так как в принятой модели за счет предупреждающих действий по результатам диагностики нейтрализуются появившиеся и/или активизируемые угрозы, тем самым отдаляется во времени момент завершения активизации какой-либо угрозы).

В модели рассмотрен последовательный алгоритм возникновения и развития потенциальной угрозы: сначала возникает источник угрозы, после чего он начинает активизироваться. По прошествии времени активизации, свойственного этому источнику угрозы (в общем случае это время активизации представляет собой случайную величину), наступает виртуальный момент нарушения целостности моделируемой системы, интерпретируемый как момент нарушения надежности реализации рассматриваемого процесса с возможными ущербами. Если после виртуального начала активизации угрозы на временной оси наступает очередная диагностика, то дальнейшая активизация угрозы полагается предотвращенной до нанесения недопустимого ущерба, а источник угроз — нейтрализованным (до возможного нового появления какой-либо угрозы после прошедшей диагностики).

Примечание — Если активизация мгновенная, это считают эквивалентным внезапному отказу. Усилия системной инженерии как раз и направлены на использование времени постепенной активизации угроз для своевременного определения, распознавания и противодействия им.

С точки зрения системной инженерии результатом применения модели является расчетная вероятность нарушения надежности реализации процесса управления инфраструктурой системы в течение заданного периода прогноза при реализации технологии периодического системного контроля (диагностики) целостности системы.

Для моделируемой системы, представленной в виде «черного ящика», применительно к выполняемым действиям, выходным результатам и иным критичным сущностям для процесса управления инфраструктурой системы формально определяют следующие исходные данные:

σ — частота возникновения источников угроз с точки зрения нарушения надежности реализации процесса;

β — среднее время развития угроз (активизации источников угроз) с момента их возникновения до нарушения целостности с точки зрения нарушения надежности реализации процесса;

$T_{меж}$ — среднее время между окончанием предыдущей и началом очередной диагностики целостности моделируемой системы;

$T_{диаг}$ — среднее время системной диагностики целостности моделируемой системы (без использования метода повышения адекватности модели по В.2.4 действует ограничительное предположение, что среднее время восстановления нарушаемой целостности системы, выявляемой при диагностике, включено в среднее время системной диагностики, т. е. средние времена диагностики без и с восстановлением целостности моделируемой системы приблизительно одинаковы, различиями при моделировании можно пренебречь);

$T_{восст}$ — среднее время восстановления нарушаемой целостности моделируемой системы (используется в случае применения метода повышения адекватности модели по В.2.4);

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

Примечание — Примеры переопределения этих исходных данных (согласно В.2.4), конкретизированные в приложении к дополнительным специфическим требованиям, приведены в В.3.

Вероятность нарушения надежности реализации процесса $R_{надежн}(T_{зад})$ в течение заданного периода прогноза $T_{зад}$ вычисляют по формуле

$$R_{надежн}(T_{зад}) = R_{надежн}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}) = 1 - P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад}), \quad (В.1)$$

где $P_{возд}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ — вероятность надежной реализации процесса в течение периода $T_{зад}$.

Возможны два варианта:

- вариант 1 — заданный период прогноза $T_{зад}$ меньше периода между окончаниями соседних контролей целостности моделируемой системы ($T_{зад} < T_{меж} + T_{диаг}$);
- вариант 2 — заданный период прогноза $T_{зад}$ больше или равен периоду между окончаниями соседних контролей целостности ($T_{зад} \geq T_{меж} + T_{диаг}$), т. е. за это время заведомо произойдет один или более контролей целостности моделируемой системы с восстановлением возможностей нарушенного выполнения процесса (если нарушения имели место).

Для варианта 1 при условии независимости исходных характеристик вероятность $P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{зад})$ надежной реализации процесса управления инфраструктурой системы в течение периода прогноза $T_{зад}$ вычисляют по формуле

$$P_{возд(1)} = \begin{cases} \left(\sigma - \beta^{-1}\right)^{-1}\left\{\sigma e^{-T_{зад}/\beta} - \beta^{-1} e^{-\sigma T_{зад}}\right\}, \text{если } \sigma \neq \beta^{-1}, \\ e^{-\sigma T_{зад}}\left[1 + \sigma T_{зад}\right], \text{если } \sigma = \beta^{-1}. \end{cases} \quad (В.2)$$

Примечание — Формулу (В.2) используют также для оценки вероятности надежной реализации процесса управления инфраструктурой системы при отсутствии какого-либо контроля в предположении, что к началу периода прогноза целостность моделируемой системы обеспечена, т. е. для расчетов по модели В.2.2.

Для варианта 2 при условии независимости исходных характеристик вероятность надежной реализации процесса управления инфраструктурой системы в течение периода прогноза $T_{зад}$ вычисляют по формуле

$$P_{возд(2)} = P_{серед} \cdot P_{кон}, \quad (В.3)$$

где $P_{серед}$ — вероятность надежной реализации процесса управления инфраструктурой системы в течение всех периодов между системными контролями, целиком вошедшими в границы времени $T_{зад}$, вычисляемая по формуле

$$P_{серед} = P^{N}_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{меж} + T_{диаг}), \quad (В.4)$$

где N — число периодов между диагностиками, которые целиком вошли в границы времени $T_{зад}$, с округлением до целого числа, $N = [T_{зад}/(T_{меж} + T_{диаг})]$ — целая часть;

$P_{кон}$ — вероятность надежной реализации процесса управления инфраструктурой системы после последнего системного контроля, вычисляемая по формуле (В.2), т. е.

$$P_{кон} = P_{возд(1)}(\sigma, \beta, T_{меж}, T_{диаг}, T_{ост}),$$

где $T_{ост}$ — остаток времени в общем заданном периоде $T_{зад}$ по завершении полных периодов, вычисляемый по формуле

$$T_{ост} = T_{зад} - N(T_{меж} + T_{диаг}). \quad (В.5)$$

Формула (В.3) логически интерпретируется так: для обеспечения выполнения требований надежной реализации процесса управления инфраструктурой системы за весь период прогноза требуется обеспечение надежности на каждом из участков — будь то середина или конец задаваемого периода прогноза $T_{зад}$.

Примечание — Для расчетов $P_{возд(2)}$ возможны иные вероятностные меры, например, когда N — действительное число, учитывающее не только целую, но и дробную часть.

В итоге вероятность надежной реализации процесса управления инфраструктурой моделируемой системы, представляемой в виде «черного ящика», в течение периода прогноза $T_{зад}$ определяется аналитическими выражениями (В.2)—(В.5) в зависимости от варианта соотношений между исходными данными. Это позволяет вычислить по формуле (В.1) вероятность нарушения надежности реализации процесса управления инфраструктурой моделируемой системы $R_{надежн}$ (σ, β, $T_{меж}$, $T_{диаг}$, $T_{зад}$) в течение заданного периода прогноза $T_{зад}$ с учетом предпринимаемых технологических мер периодического системного контроля и восстановления возможностей по обеспечению выполнения процесса. С учетом возможного ущерба эта вероятность характеризует прогнозируемый риск нарушения надежности реализации процесса управления инфраструктурой системы в течение заданного периода прогноза при реализации технологии периодического системного контроля.

Примечание — В частном случае, когда период между диагностиками больше периода прогноза $T_{меж} > T_{зад}$, модель В.2.3 превращается в модель В.2.2 для прогноза риска нарушения надежности реализации процесса управления инфраструктурой системы при отсутствии какого-либо контроля.

В.2.4 Расчет риска для моделируемой системы сложной структуры, комбинация и повышение адекватности

Описанные в В.2.2 и В.2.3 модели применимы для проведения оценок, когда система представлена в виде «черного ящика» и когда значения времен системной диагностики и восстановления нарушенной целостности системы совпадают. В развитие моделей В.2.2 и В.2.3 в настоящем подразделе приведены способы, позволяющие с использованием В.2.2 и В.2.3 создание моделей для моделируемой систем сложной структуры и более общего случая, когда значения времен системной диагностики и восстановления нарушенных возможностей системы различны.

Расчет основан на применении следующих инженерных способов.

1-й способ позволяет использовать одни и те же модели для расчетов различных показателей по области их приложения. Поскольку модели математические, то путем смыслового переопределения исходных данных возможно использование одних и тех же моделей для оценки показателей, различающихся по смыслу, но идентичных по методу их расчета. Применение этого способа позволяет соизмерять прогнозируемые риски для разнородных угроз по единой вероятностной шкале от 0 до 1.

2-й способ позволяет переходить от оценок моделируемой системы или отдельных элементов, представляемых в виде «черного ящика», к оценкам моделируемой системы сложной структуры с параллельно-последовательным логическим соединением составных элементов. В формируемой структуре, исходя из реализуемых технологий для системы, состоящей из двух элементов, взаимовлияющих на выполнение процесса, указывается характер их логического соединения. Если два элемента соединяются последовательно, что означает логическое соединение «И», то в контексте надежности реализации процесса это интерпретируется так: «в системе обеспечена надежность реализации процесса в течение времени t, если 1-й элемент «И» 2-й элемент сохраняют свои возможности по надежной реализации процесса в течение этого времени». Если два элемента соединяются параллельно, что означает логическое соединение «ИЛИ», это интерпретируется так: «система сохраняет возможности по надежной реализации процесса в течение времени t, если 1-й элемент «ИЛИ» 2-й элемент сохраняют свои возможности по надежной реализации процесса в течение этого времени».

Для комплексной оценки в приложении к сложной моделируемой системе используются рассчитанные на моделях вероятности нарушения надежности реализации процесса для каждого из составных элементов за заданное время t. Тогда для простейшей структуры из двух независимых элементов вероятность нарушения надежности реализации процесса за время t определяют по формулам:

- для системы из двух последовательно соединенных элементов

$$P(t) = 1 - [1 - P_1(t)] \cdot [1 - P_2(t)]; \quad (В.6)$$

- для системы из двух параллельно соединенных элементов

$$P(t) = P_1(t) \cdot P_2(t), \quad (В.7)$$

где $P_1(t)$ и $P_2(t)$ — вероятности нарушения надежности реализации процесса соответственно для 1-го и 2-го элементов за заданное время t.

Рекурсивное применение соотношений (В.6), (В.7) снизу-вверх предоставляет возможности получения соответствующих вероятностных оценок для сложной логической структуры с параллельно-последовательным логическим соединением элементов.

Примечание — Способ рекурсивного применения процессов рекомендован ГОСТ Р 57102. Рекурсивное применение снизу-вверх означает первичное применение моделей В.2.2 или В.2.3 сначала для отдельных системных элементов, представляемых в виде «черного ящика» в принятой сложной логической структуре системы, затем, учитывая характер логического объединения («И» или «ИЛИ») в принятой структуре, по фор-

мулам (В.6) или (В.7) проводят расчет вероятности нарушения надежности реализации процесса за время t для объединяемых элементов (в принятых условиях независимости распределений их временных характеристик). И так — до объединения элементов на уровне системы в целом. При этом сохраняется возможность аналитического прослеживания зависимости результатов расчетов по формулам (В.6) или (В.7) от исходных параметров моделей В.2.1 и В.2.2.

3-й способ в развитие 2-го способа позволяет использовать результаты моделирования для формирования заранее неизвестных (или сложно измеряемых) исходных данных в интересах последующего моделирования. На выходе моделирования по моделям В.2.2 и В.2.3 и применения 2-го способа получается вероятность нарушения надежности функционирования моделируемой системы в течение заданного периода времени t. Если для каждого элемента просчитать эту вероятность для всех точек t от нуля до бесконечности, получится траектория функции распределения времени нарушения надежности функционирования моделируемой системы вплоть до каждого из элементов в зависимости от реализуемых мер контроля и восстановления целостности, т. е. то, что используется в формулах (В.6) и (В.7). Полученный вид этой функции распределения, построенной по точкам (например, с использованием программных комплексов), позволяет традиционными методами математической статистики определить такой показатель, как среднее время до нарушения надежности функционирования каждого из элементов и моделируемой системы в целом. С точки зрения системной инженерии в приложении к рассматриваемому процессу, представляемому в виде моделируемой системы простой или сложной структуры, это среднее время может быть интерпретировано как виртуальная средняя наработка на нарушение надежности реализации процесса при прогнозировании риска по моделям В.2.2 и В.2.3. Обратная величина этого среднего времени является частотой нарушений надежности реализации процесса в условиях разнородных угроз и применяемых методов контроля и восстановления возможностей по обеспечению выполнения процесса для составных элементов. Именно это — необходимые исходные данные для последующего применения моделей «черного ящика» В.2.2 и В.2.3. Этот способ используют, когда изначальная статистика для определения частотных характеристик отсутствует или ее недостаточно.

4-й способ в дополнение к возможностям 2-го и 3-го способов позволяет повысить адекватность моделирования за счет развития моделей В.2.2 и В.2.3 в части отдельного учета времени на контроль (диагностику) состояния и восстановление после нарушения целостности моделируемой системы. В моделях В.2.2 и В.2.3 время системного контроля по составному элементу одинаково и равно в среднем $T_{диаг}$. Вместе с тем, если по результатам контроля для восстановления нарушенных возможностей по выполнению процесса на практике требуется дополнительное время ($T_{восст}$), то для моделирования, учитывающего лишь один параметр ($T_{диаг}$), это дополнительное время должно быть также учтено. При этом усредненное время диагностики с учетом дополнительного времени на восстановление вычисляют итеративно с заданной точностью:

- 1-я итерация определяет $T^{(1)}_{диаг} = T_{диаг}$, задаваемое на входе модели. Для 1-й итерации при обнаружении нарушений полагается мгновенное восстановление нарушаемых возможностей по обеспечению выполнения процесса;
- 2-я итерация осуществляется после расчета риска $R^{(1)}$ по исходным данным после 1-й итерации

$$T^{(2)}_{диаг} = T^{(1)}_{диаг} \cdot (1 - R^{(1)}) + R^{(1)} \cdot T_{восст}, \quad (В.8)$$

где $R^{(1)}$ — риск нарушения надежности реализации процесса с исходным значением $T^{(1)}_{диаг}$, вычисляемый с использованием модели В.2.3. Здесь, поскольку на 1-й итерации $T^{(1)}_{диаг}$ не учитывает времени восстановления, риск $R^{(1)}$, рассчитываемый с использованием модели В.2.3, ожидается оптимистичным, т. е. меньше реального;

- r-я итерация осуществляется после расчета риска $R^{(r-1)}$ по исходным данным после $(r-1)$-й итерации

$$T^{(r)}_{диаг} = T^{(r-1)}_{диаг} \cdot (1 - R^{(r-1)} + R^{(r-1)} \cdot T_{восст}, \quad (В.9)$$

где $R^{(r-1)}$ вычисляют по моделям В.2.2, В.2.3, но в качестве исходного уже выступает $T^{(r-1)}_{диаг}$, рассчитанное на предыдущем шаге итерации. Здесь в большей степени учитывается время восстановления с частотой, стремящейся к реальной. Соответственно риск $R^{(r-1)}$ также приближается к реальному, $r \geq 2$.

С увеличением r указанная последовательность $T^{(r)}_{диаг}$ сходится, и для дальнейших расчетов используют значение, отличающееся от точного предела $T^{(\infty)}_{диаг}$ на величину, пренебрежимо малую по сравнению с задаваемой изначально точностью итерации ε:

$$|R^{(r)} - R^{(r-1)}| \leq \varepsilon.$$

Таким образом, 4-й способ позволяет вместо одного исходного данного (среднего времени системной диагностики, включая восстановление нарушенной целостности моделируемой системы) учитывать два, которые могут быть различны по своему значению:

- $T_{диаг}$ — среднее время системной диагностики целостности моделируемой системы;

- $T_{восст}$ — среднее время восстановления нарушенной целостности моделируемой системы.

При этом для расчетов применяется одна и те же модель В.2.3.

Примечание — Способ итеративного применения процессов рекомендован ГОСТ Р 57102, ГОСТ Р 58494, ГОСТ Р 59331.

Применение инженерных способов 1—4 обеспечивает более точный прогноз для системы сложной структуры с учетом различий во временах диагностики и восстановления целостности моделируемой системы.

В.3 Математические модели для прогнозирования 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. Примером могут служить модели и методы прогнозирования риска нарушения требований по защите информации — см. ГОСТ Р 59341—2021 (В.2 приложения В).

Примечание — Модели, приведенные в ГОСТ Р 59341 для процесса управления информацией, в полной мере применимы для прогнозирования риска нарушения некоторых из дополнительных специфических системных требований в процессе управления инфраструктурой системы (в частности, дополнительные специфические требования к своевременности представления информации, к контролю безошибочности и обеспечению достоверности циркулирующей информации о состоянии инфраструктуры системы, требования по защите циркулирующей и хранимой информации).

В моделях простой структуры под анализируемой системой понимают определенный выходной результат или действие или совокупность задействованных активов (или иные критичные сущности инфраструктуры системы, подлежащие учету в моделируемой системе при анализе выполнения дополнительных специфических системных требований). В моделях сложной структуры под анализируемой системой понимают определенную упорядоченную совокупность составных элементов, каждый из которых логически представляет собой выходной результат или действие, или совокупность задействованных активов (или иные критичные сущности инфраструктуры системы, подлежащие учету в моделируемой системе сложной структуры при анализе выполнения дополнительных специфических системных требований). В общем случае для системы сложной структуры для различных элементов могут быть применены различные модели угроз или различные технологии системного контроля выполнения дополнительных специфических системных требований и восстановления элементов системы. Отдельный элемент рассматривают как «черный ящик».

Под целостностью моделируемой системы согласно определению 3.1.18 понимают такое ее состояние, которое в течение задаваемого периода прогноза отвечает целевому назначению системы (см. также В.2.1.3). При моделировании, направленном на прогнозирование риска нарушения дополнительных специфических системных требований, целевое назначение моделируемой системы проявляется в выполнении дополнительных специфических системных требований. В этом случае для каждого из элементов и моделируемой системы в целом пространство элементарных состояний на временной оси образуют два основных состояния:

- «Выполнение дополнительных специфических системных требований в моделируемой системе обеспечено», если в течение всего периода прогноза обеспечено выполнение дополнительных специфических системных требований;
- «Выполнение дополнительных специфических системных требований в моделируемой системе нарушено» — в противном случае.

В результате математического моделирования рассчитывают вероятность приемлемого выполнения дополнительных специфических системных требований (т. е. пребывания в состоянии «Выполнение дополнительных специфических системных требований в моделируемой системе обеспечено») в течение всего периода прогноза и ее дополнение до единицы, представляющее собой вероятность нарушения дополнительных специфических системных требований (т. е. пребывания в состоянии «Выполнение дополнительных специфических системных требований в моделируемой системе нарушено»). В свою очередь вероятность нарушения дополнительных специфических системных требований в течение всего периода прогноза в сопоставлении с возможным ущербом определяет риск нарушения дополнительных специфических системных требований.

Аналогично В.2 применяют математическую модель «черного ящика» при отсутствии какого-либо контроля или математическую модель «черного ящика» при реализации технологии периодического системного контроля, каждая из которых адаптирована к контексту выполнения дополнительных специфических системных требований. С формальной точки зрения при сопоставлении с возможным ущербом модель позволяет оценить вероятностное значение риска нарушения дополнительных специфических системных требований в моделируемой системе в течение заданного периода прогноза. С точки зрения системной инженерии этот результат интерпретируют следующим образом: результатом применения модели является расчетная вероятность нарушения дополнительных специфических системных требований в процессе управления инфраструктурой системы в течение заданного пе-

риода прогноза при реализации технологии периодического системного контроля (диагностики). При этом учитывают предпринимаемые меры периодической диагностики и восстановления возможностей по обеспечению выполнения дополнительных специфических системных требований.

В.3.2 Исходные данные и расчетные показатели

Для расчета вероятностных показателей применительно к моделируемой системе, где анализируемые сущности могут быть представлены в виде «черного ящика», используют исходные данные, формально определяемые в общем случае 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 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 инфраструктурой системы для моделируемой системы простой и сложной структуры осуществляют по тем же формулам (В.1)—(В.9), в частности для дополнительных специфических системных требований по защите информации — по ГОСТ Р 59341—2021 (В.2 приложение В).

Расчет вероятности нарушения дополнительных специфических системных требований для процесса управления инфраструктурой 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 риска нарушения реализации процесса с учетом дополнительных специфических системных требований

В сопоставлении с возможным ущербом обобщенный риск нарушения реализации процесса управления инфраструктурой системы с учетом дополнительных специфических системных требований $R_{обобщ}(T_{зад})$ для периода прогноза $T_{зад}$ определяют по формуле

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

где $R_{надежн}(T_{зад})$ — вероятность нарушения надежности реализации процесса управления инфраструктурой системы в течение периода прогноза $T_{зад}$ без учета дополнительных специфических системных требований, рассчитывают по моделям и рекомендациям В.2;

$R_{надежн}(T_{зад})$ — вероятность нарушения дополнительных специфических системных требований в системе для процесса управления инфраструктурой системы в течение периода прогноза $T_{зад}$, рассчитывают по моделям и рекомендациям В.3.

Приложение Г
(справочное)

Рекомендации по определению допустимых значений показателей, характеризующих риски в процессе управления инфраструктурой 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 59339, ГОСТ Р 59349, 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 инфраструктуры 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 подлежит 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, характеризуются 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 надежности реализации процесса управления инфраструктурой системы является выполнение требований системной инженерии при допустимом риске заказчика, обосновываемом по прецедентному принципу.

Типовые допустимые значения количественных показателей рисков для процесса управления инфраструктурой 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 Г.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 инфраструктурой системы (без учета дополнительных специфических системных требований)	Не выше 0,05	Не выше 0,01
Обобщенный риск нарушения реализации процесса управления инфраструктурой системы с учетом дополнительных специфических системных требований	Не выше 0,10	Не выше 0,05

Приложение Д
(справочное)

Примерный перечень методик системного анализа для процесса управления инфраструктурой системы

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

Д.2 Методика прогнозирования риска нарушения дополнительных специфических системных требований в процессе управления инфраструктурой системы.

Д.3 Методика прогнозирования обобщенного риска нарушения реализации процесса управления инфраструктурой 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 инфраструктурой системы с учетом дополнительных специфических системных требований).

Д.5 Методики определения существенных недостатков процесса управления инфраструктурой системы с использованием прогнозирования рисков.

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

Д.7 Методики обоснования предложений по совершенствованию непосредственно самого системного анализа процесса управления инфраструктурой системы.

Примечания

1 Системной основой для создания методик служат положения разделов 5—7, 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)

[22] Основы государственной политики Российской Федерации в Арктике на период до 2035 года (утверждены указом Президента Российской Федерации от 5 марта 2020 г. № 164)

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

Ключевые слова: безопасность, процесс управления инфраструктурой системы, модель, риск, система, системная инженерия, системный анализ, управление

Редактор *Н.А. Аргунова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *А.Н. Золотаревой*

Сдано в набор 18.08.2022. Подписано в печать 01.09.2022. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,18. Уч.-изд. л. 3,35.

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